CYBER CERCLE

EN DISTANCIEL

28 SEPTEMBRE 2021
MERIGNAC
RENCONTRES CYBERSÉCURITÉ
NOUVELLE-AQUITAINE

#RCYBERNOUVELLEAQUITAINE
#TDFCYBER

TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCYBER

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS

@CyberCercle
@CyberTerritoire

DOSSIER PARTICIPANT

Crédit photo Alain Zimeray

Bénédicte PILLIET
Présidente du CyberCercle

Edito

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

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

Avec la crise sanitaire, le Tour de France de la Cybersécurité s'est réinventé en distanciel quand cela était nécessaire, en maintenant deux objectifs majeurs : permettre dans le contexte actuel d'avoir accès à une parole de confiance sur la sécurité numérique et favoriser les échanges constructifs pour avancer ensemble vers des territoires de confiance numérique, alors même que le recours au numérique est devenu encore plus essentiel dans la crise que nous traversons, avec des usages qui ne reviendront pas en arrière.

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

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

En effet, si tout le monde (ou presque), entend le message sur le risque cyber et la nécessité de le traiter, la sécurité numérique reste cependant un axe insuffisamment pris en compte par les collectivités, PME-PMI, organismes de recherche et de formation… faute de temps, de moyens ou de solutions simples à mettre en œuvre, et de partages d'informations. Pourtant ces acteurs, maillons essentiels des écosystèmes, et ils sont nombreux dans la région, sont au cœur du sujet.

Le territoire dans lequel nous sommes s'est résolument engagé dans la construction de territoires de confiance numérique, sous l'impulsion de la Région Nouvelle-Aquitaine et de son Président, Alain ROUSSET, avec la feuille de route cybersécurité engagée à l'été 2020 par la Région. Nous sommes heureux au CyberCercle de contribuer à cette dynamique, avec cette journée des Rencontres de la Cybersécurité Nouvelle-Aquitaine et les matinales bimestrielles que nous avons mises en place avec la ville de Mérignac depuis mars 2021 afin d'animer une communauté de confiance autour de ces sujets.

Je tiens à remercier nos partenaires, qui pour certains nous suivent sur l'ensemble du TDFCyber depuis sa création comme le Groupe La Poste, Cybermalveillance.gouv.fr et CERTitude NUMERIQUE, des entreprises et organisations comme ENEDIS, Avant de Cliquer et la Banque des Territoires qui s'y sont associées cette année, et pour cette étape la ville de Mérignac. Je remercie également nos soutiens, ministères, représentants de l'Etat, écoles, associations, avec ici sur ce territoire particulier, la Préfecture de Région, la Région Nouvelle-Aquitaine, la Police Judiciaire de Bordeaux, la Région de Gendarmerie Nouvelle-Aquitaine, l'ADI-Nouvelle-Aquitaine, la French Tech Bordeaux, le CLUSIR Aquitaine et Bordeaux Technowest, qui s'associent à cet événement dans cet esprit fédérateur qui est le nôtre.
Je remercie enfin notre ambassadrice en région Nouvelle-Aquitaine, Cécile DESMOND, dont la connaissance des acteurs locaux, associée aux valeurs de partage au service de l'intérêt général qui sont au cœur du CyberCercle, est une vraie force pour notre action.

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

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

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

9h00 ■›› **OUVERTURE DES TRAVAUX**

➤ Mot de bienvenue de **Bénédicte PILLIET**, présidente du CyberCercle

➤ Interventions

➢ **Marie RECALDE**, adjointe au Maire de Mérignac, déléguée au développement économique, à l'emploi, à l'innovation, à la formation et à l'égalité femmes/hommes, conseillère métropolitaine en charge de l'économie de Bordeaux Métropole, représentante d'**Alain ANZIANI**, maire de Mérignac, président de Bordeaux Métropole

➢ **Andréa BROUILLE**, 1ère vice-présidente de la Région Nouvelle-Aquitaine, en charge du développement économique, représentant d'**Alain ROUSSET**, président de la Région Nouvelle-Aquitaine

➢ **Martin GUESPEREAU**, préfet délégué pour la défense et la sécurité, représentant **Fabienne BUCCIO**, préfète de la Région Nouvelle-Aquitaine, préfète de la zone de défense et de sécurité Sud-ouest, préfète de la Gironde

9h40 ■›› **TABLE RONDE**

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

➤ Animateur : **Bénédicte PILLIET**, présidente, CyberCercle

➢ **Marie RECALDE**, adjointe au Maire de Mérignac, déléguée au développement économique, à l'emploi, à l'innovation, à la formation et à l'égalité femmes/hommes, conseillère métropolitaine en charge de l'économie, Bordeaux Métropole

➢ **Jérôme NOTIN**, directeur général, Cybermalveillance.gouv.fr

➢ **Hélène DESLIENS**, vice-présidente, French Tech Bordeaux

➢ **Commissaire Divisionnaire Paul BOUSQUET**, Chef de la division des affaires économiques et financières, Direction Territoriale de la Police Judiciaire de Bordeaux - DZPJ Sud Ouest

➢ **Guy FLAMENT**, chargé de mission Campus Cyber, Agence de Développement et d'Innovation, Région Nouvelle-Aquitaine

11h00 ■›› **KEYNOTES**

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

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

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

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

➤ **L'opération EMERAUDE d'ENEDIS : comment sensibiliser ses collaborateurs à la cybersécurité**

Laurent BOURREAU, chef d'agence EASI, direction régionale Aquitaine, ENEDIS

➤ **La dimension cyber dans le domaine de l'aéronautique de Défense**

Général Jean-Marc LAURENT, responsable exécutif de la Chaire « Défense et Aérospatial », Sciences Po Bordeaux

13h00 ■›› **FIN DE LA MATINÉE**

14h30 ■›› **ATELIERS**

Les ateliers durent deux heures et ont pour objectif de permettre aux participants d'échanger, de façon très pratique et opérationnelle, dans un cadre de confiance - ils sont placés sous les règles de Chatham House.

➤ ATELIER 1

Quels enjeux de cybersécurité pour la filière Aéronautique, de la security by design à la supply chain ?

Animateur : **Eric VAUTIER**, RSSI, ADP - senior advisor, CyberCercle
Karine AMIEVA-CAMOS, délégué à l'information stratégique et à la sécurité économiques pour la région Nouvelle-Aquitaine, direction régionale de l'économie, de l'emploi, du travail et des solidarités, Secrétariat général pour les affaires régionales, Préfecture de la région Nouvelle-Aquitaine
Romain BOTTAN, chief information security officer, directeur programme AirCyber, BoostAeroSpace
Gurvan QUENET, RSSI, Aéroport de Mérignac - président, CLUSIR Nouvelle Aquitaine

➤ ATELIER 2

Comment favoriser l'innovation en cybersécurité ?

Animateur : **Dr Michel DUBOIS**, chef du bureau Expertise, direction de la cybersécurité, Groupe La Poste
Nicolas MARTIN, directeur du développement, Bordeaux Technowest
François CHARBONNIER, investisseur confiance numérique, Banque des Territoires
Christine SAMANDEL, Chief of Staff & Project Owner Ecosystem, TEHTRIS
Toufik AHMED, titulaire, Chaire Cyber Résilience des Infrastructures Numériques, Bordeaux INP

➤ ATELIER 3

Collectivités : de la sécurité numérique au quotidien à son insertion dans les projets de développement des territoires

Animatrice : **Bénédicte PILLIET**, présidente, CyberCercle
Amandine DEL-AMO, chargée de mission partenariats, Cybermalveillance.gouv.fr
Olivier GRALL, délégué régional Nouvelle-Aquitaine, ANSSI
Lieutenant-colonel Ludovic BONCOMPAIN, chef du bureau appui numérique, officier référent en sécurité économique, et **Adjudante Christelle BOISSIMON**, référente sécurité économique, Région de Gendarmerie Nouvelle-Aquitaine
Philippe STEUER, RSSI, Bordeaux Métropole
Astrid FROIDURE, chargée de mission, Avant de Cliquer

➤ ATELIER 4

Les ressources humaines en cybersécurité : métiers et formation, des métiers d'avenir

Animatrice : **Baya LONQUEUX**, membre, Cercle des Femmes de la Cybersécurité (CEFCYS)
David OFER, président, Fédération Française de Cybersécurité
Alexandre DUBOIS, directeur adjoint - référent national filière informatique, YNOV Bordeaux
Benoît de SAINT-SERNIN, président, Ecole Européenne de la Cybersécurité
Marc-André BEAUDET, RSSI, membre, CESIN

16h30 ■›› **FIN DES TRAVAUX**

Les intervenants

Marie RECALDE

Adjointe déléguée au développement économique, à l'emploi, à l'innovation, à la formation et à l'égalité femmes/hommes
Mérignac

Marie RECALDE est depuis 2008 Adjointe au Maire de Mérignac, déléguée au développement économique, à l'emploi, à l'innovation, à la formation et à l'égalité femmes/hommes. Elle est également avocat associé chez Fontaine Avocats.
Elle a été Députée de la Gironde, membre de la Commission de la Défense de 2012 à 2017, conseillère générale de la Gironde à partir de 2008, occupant le poste de Vice-Présidente en charge des Transports et de la Mobilité de 2010 à 2011. Elle a dirigé un Etablissement Public d'Aménagement et d'Urbanisme et dirigé les affaires juridiques et foncières de diverses collectivités publiques. Elle a en outre exercé comme urbaniste conseil dans un cabinet d'architecte.
Marie RECALDE est titulaire d'un DEA de Droit de l'Urbanisme, de l'Environnement et Economie de l'Environnement de l'Université de Bordeaux et diplômée de Sciences Po Bordeaux. Elle est auditeur de la 66ème session nationale de l'Institut des Hautes Etudes de la Défense Nationale, Colonel de la Réserve citoyenne de l'Armée de l'Air.

Martin GUESPEREAU

Préfet délégué pour la défense et la sécurité
Préfecture de la Région Nouvelle-Aquitaine

Préfet délégué pour la défense et la sécurité auprès de la préfète de la région Nouvelle-Aquitaine, préfète de la zone de défense et de sécurité Sud-Ouest, préfète de la Gironde.
Directeur de cabinet de Sébastien LECORNU, secrétaire d'Etat à la transi#on écologique (2017-2018) puis directeur adjoint de cabinet du ministre chargé des collectivités territoriales (2018- 2020).
Métropole du Grand Paris, directeur de projet d'une consultation urbaine de 7Mds€ d'investissements (2016-2017).
Agence de l'eau Rhône Méditerranée Corse, directeur général (2011-2015).
Agence française de sécurité sanitaire de l'environnement et du travail (auj ANSES), directeur général (2009-2011).
Matignon, conseiller technique de François FILLON, premier ministre, sur l'écologie et l'urbanisme (2007-08).
Ministère de la santé, conseiller technique de Xavier BERTRAND sur les crises sanitaires et la santé environnement (2004-07).
Direction du Trésor (ministère des finances) : adjoint du chef de bureau, pilotage de la politique financière française en Afrique du Nord et au Moyen-Orient (2003-04).
DRIRE de Picardie (auj DREAL), chef du service régional des installations classées (2000-2003).
COGEMA, chargé de mission auprès du directeur commercial, étude sur les USA (mi-temps ; 1998-99).

Bénédicte PILLIET

Présidente
CyberCercle

Crédit photo Alain

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.

Andréa BROUILLE

1ère vice-présidente de la Région Nouvelle-Aquitaine, en charge du développement économique

Jérôme NOTIN

Directeur Général
Cybermalveillance.gouv.fr

Jérôme NOTIN travaille depuis vingt ans dans le domaine de la sécurité numérique.
Après un début de carrière dans des entreprises privées liées à la cyber sécurité et au logiciel libre, il rejoint l'ANSSI en 2016 comme préfigurateur du dispositif national d'assistance aux victimes de cybermalveillance. Il devient directeur général du groupement d'intérêt public qui porte ce dispositif à sa création en mars 2017.

Commissaire divisionnaire Paul BOUSQUET

Chef de la division des affaires économiques et financières
Direction Territoriale de la Police Judiciaire de Bordeaux
DZPJ Sud Ouest

D'août 2003 à octobre 2014, Paul BOUSQUET occupe plusieurs fonctions de chef de service dans différentes directions territoriales de Sécurité Publique. En octobre 2014, il devient chef du Groupe Interministériel de recherche (GIR) de Bordeaux, unité inter-services (Police judiciaire, Sécurité Publique, Douane, Finances Publiques), spécialisée dans la lutte contre l'économie souterraine et l'identification des avoirs criminels, poste qu'il occupera jusqu'en novembre 2017.
En novembre 2017 le commissaire divisionnaire Paul BOUSQUET est nommé chef de la division de lutte contre la criminalité financière à la Direction Territoriale de Police Judiciaire de Bordeaux.

Dr Michel DUBOIS

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

Michel DUBOIS est chef du pôle expertise cybersécurité au sein de la direction de la cybersécurité du Groupe La Poste. Ingénieur en informatique, titulaire d'un 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).

Hélène DESLIENS

Vice-présidente
French Tech Bordeaux

Hélène DESLIENS est co-fondatrice de deux entreprises : Experteez, organisme de formation sur les méthodes de travail collaboratif (Design thinking / Design Sprint, Agiles et Lean) pour accompagner les entreprises dans leur transformation digitale et Markopolo, cabinet dédié à l'innovation. Hélène est également vice-présidente de FrenchTech Bordeaux, membre de l'association de financement de l'innovation Finaqui, co-présidente de l'association des Bruits de la Rue qui a pour vocation de "penser pour agir autrement contre les précarités » et vice-présidente du Conseil des IUT à l'université Bordeaux Montaigne.
Fréquemment mentor de startup, tant dans le cadre des réseaux impulsant les femmes entrepreneures (Women Tech Makers, les Premières...) que dans le cadre du réseau international des Experts Google (GDE), et "Sprint Master" certifiée Google » sur la méthodologie du Design Sprint.
20 années d'expérience dans le marketing et le numérique au sein d'entreprises tant nationales qu'internationales : Hélène DESLIENS a travaillé sur le marketing distributeur au sein de Toshiba Syst. France, puis sur le lancement d'une offre dédiée aux PME-PMI, fruit d'un partenariat entre SAP et Origin (devenue ATOS Origin). En 2000, elle prend en charge l'animation de la clientèle de Banque Directe (devenue AXA Banque) par le contenu multimédia, puis rejoint la direction marketing et internet de Meilleurtaux.com.

Guy FLAMENT

Chargé de mission Campus Cyber
Agence de Développement et d'Innovation
Région Nouvelle-Aquitaine

Guy FLAMENT a récemment été chargé, au sein de l'Agence de développement et d'innovation (ADI) de Nouvelle-Aquitaine, de piloter la phase d'incubation du projet de Cybercampus régional et la mise en place du centre régional de réponse à incident (CSIRT) qui constitue la première brique opérationnelle du campus. Ce projet représente le pilier central de l'ambition régionale en matière de cybersécurité et de confiance numérique.
Il intervient régulièrement dans des conférences sur la cybersécurité et conseille également les entreprises locales dans leurs stratégies de développement.
Hautement spécialisé en cybersécurité, il a précédemment travaillé chez Tecnalia France pour y mener des projets de R&D et d'innovation numériques et pour l'agence nationale de cybersécurité (ANSSI). Il a occupé pendant 3 ans le poste de délégué régional pour la Nouvelle-Aquitaine.

Les intervenants

Franck GICQUEL

Responsable des Partenariats
Cybermalveillance.gouv.fr

Franck GICQUEL est Responsable des partenariats de Cybermalveillance.gouv.fr.
Il intègre l'équipe dès la phase de préfiguration du dispositif au sein de l'ANSSI en 2016.
Il officiait alors depuis plus de 10 ans dans l'écosystème de la sécurité et des systèmes d'informations. Il a notamment été Directeur Commercial chez DG Consultants, Groupe Comexposium, où il a contribué à développer leur événement phare, les Assises de la Sécurité à Monaco, et à fédérer la communauté des professionnels du secteur.

Olivier GRALL

Délégué à la sécurité numérique
ANSSI

Olivier GRALL est le délégué à la sécurité numérique de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour la région Nouvelle Aquitaine. Il a intégré en Septembre 2018 le dispositif d'action territoriale qui permet à l'Agence d'agir au plus près des acteurs économiques et des collectivités locales.
Il était auparavant Ingénieur en investigation numérique au sein de la division réponse de l'ANSSI. Il est également membre du commité Directeur de l'AFSIN (Association Francophone des spécialistes de l'investigation numérique) et a dirigé pendant 7 ans la Branche Francaise de la Société MSAB qui équipe les forces de l'ordre en solutions d'analyse de téléphones Mobiles.

Eric VAUTIER

RSSI Groupe
Groupe ADP

Après des études en informatique à l'Ecole Nationale de l'Aviation Civile et quatre ans dans des entreprises de services du numérique, Eric VAUTIER a rejoint le Groupe ADP en 1996 en tant que chef de projet en Systèmes d'Informations Aéroportuaires. Simultanément, il participe à des projets pour le Groupe à l'international dont le Terminal 3 de l'aéroport de Dubai. En 2008, il quitte l'aéroportuaire pour prendre la responsabilité de la sécurité informatique sur le périmètre de la DSI. Depuis, ses missions ont évolué en même temps que la cybersécurité apparaissait et prenait toute son importance. Il est aujourd'hui le RSSI Groupe, en charge du pilotage de la cybersécurité sur les aéroports parisiens, mais aussi des principales filiales du Groupe, en France et à l'étranger.
Eric VAUTIER est senior advisor du CyberCercle.

Laurent BOURREAU

Chef d'agence EASI
Direction régionale Aquitaine Nord, ENEDIS

Titulaire d'un DESS en « sureté de mission des organisations », Laurent BOURREAU a effectué une grande partie de sa carrière au sein du Groupe EDF, puis d'ENEDIS à partir de 2011. Après un parcours dans les domaine de la Qualité, le contrôle interne et le pilotage de la performance, il est devenu en mai 2020 chef de projet senior, animateur Risques Contrôle Interne, Référent Sûreté, Développeur Data visualisation chez ENEDIS Direction Régionale Aquitaine Nord. Il est depuis mai 2021 responsable des fonctions supports, Logistique, Système d'information, Cybersécurité dans cette même direction avec différentes missions : manager une équipe de 16 experts dans des domaines variés comme l'immobilier, le suivi de la flotte véhicules et engins, les achats tertiaires et facturation, les approvisionnements, les déchets environnementaux, SI et cybersécurité ; Référent Sûreté ; responsable Mobilité Electrique Interne ; animateur Risques Contrôle Interne, mandataire de site et appui auprès du Directeur Régional Délégué.

Général Jean-Marc LAURENT

Responsable exécutif de la Chaire « Défense et Aérospatial »
Sciences Po Bordeaux

Le général de corps aérien (2S) Jean-Marc LAURENT fut pilote de chasse dans l'armée de l'Air. Ingénieur de l'Ecole de l'Air (promotion 1979), diplômé de l'Ecole de Guerre, il a été auditeur de l'Institut des Hautes Etudes de Défense Nationale (IHEDN), du Centre des Hautes Etudes Militaires (CHEM) et du European Center for Security Studies.
Après un parcours opérationnel et de commandement qui lui a permis de participer à de nombreux engagements internationaux, il est promu au grade de général en 2006 et est alors chargé des Opérations à la Délégation des Affaires stratégiques de la Défense. Il dirigera ensuite le Centre d'études stratégiques aérospatiales. Il achève sa carrière militaire comme commandeur de l'armée de l'Air chargé de son pôle technico-opérationnel et, simultanément, comme responsable ministériel de la zone de défense et de sécurité Sud-Ouest. En 2014, il fonde la chaire « Défense & Aérospatial » à Sciences Po Bordeaux.

Karine AMIEVA-CAMOS

Déléguée à l'information stratégique
et à la sécurité économiques
DREETS Nouvelle Aquitaine

Après une expérience dans le domaine humanitaire (Haut-Commissariat aux Réfugiés des Nations Unies) en Fédération de Russie, puis dans une multinationale pétrolière (REPSOL), Karine AMIEVA-CAMOS est entrée au ministère de l'Economie pour effectuer des missions de soutien à l'export. Pendant une douzaine d'années elle a été en poste à l'ambassade de France en Fédération de Russie, puis aux Etats-Unis en tant que conseillère internationale. De retour en France en 2009, elle a travaillé à la DGCCRF sur des missions de surveillance du marché des produits cosmétiques, une mission à caractère régalien qui l'a amenée à représenter la France à la Commission européenne. Depuis 2014 elle anime la politique d'intelligence économique en région Nouvelle Aquitaine, sous l'autorité de la Préfète.

Gurvan QUENET

RSSI
Aéroport de Bordeaux Mérignac

Gurvan QUENET a commencé sa carrière à la Direction Générale de l'Armement, puis au sein de différentes sociétés de service en tant que Consultant et responsable d'offres Cyber. En 2020 il rejoint l'Agence de la Sécurité des Système d'Information (ANSSI), avant d'occuper pendant 10 ans le poste de RSSI et de chef de service Sécurité opérationnelle, à Bordeaux Métropole. En 2019, il rejoint l'Aéroport de Bordeaux Mérignac comme Responsable Sécurité des Systèmes d'Information.
A titre individuel, Gurvan QUENET est président du CLUSIR Aquitaine (Club Français de la Sécurité de l'Information en Nouvelle Aquitaine), membre du club Ebios, et de la réserve Cyberdefense.

Romain BOTTAN

Chief Information Security Officer
Directeur programme AirCyber
BoostAeroSpace

C'est via l'obtention d'un Master professionnel en "Informatique, Réseaux & Systèmes de Télécommunications" à l'Université de Toulouse (IUP STRI) chez Alcatel-Lucent que Romain BOTTAN se spécialisa très tôt dans le domaine de la sécurité informatique. Romain débutât ensuite sa carrière d'ingénieur chez CapGemini Sogeti en tant qu'ingénieur sécurité pour le département sécurité informatique d'Airbus. Il passa 5 ans à travailler pour Airbus avant de se faire proposer de rejoindre Airbus Defense and Space CyberSecurity en tant qu'officier de sécurité de BoostAeroSpace.
Depuis 2011, il est responsable de la bonne coordination des activités sécurités de BoostAeroSpace et de ses fournisseurs de services où il officialisa ses compétences sécurité au travers des certifications internationales CISSP et ISO 27001 Lead Implementer.
Puis, en 2014, il assista Airbus Group en tant que Group CyberSecurity Program Manager pendant une année avant d'intégrer officiellement l'entreprise BoostAeroSpace en tant que Chief Information Security Officer.
Il est depuis 2018 également directeur du programme d'amélioration du niveau de cybersécurité de la SupplyChain Aéronautique Européenne AirCyber.

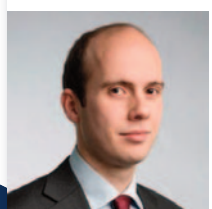
Nicolas MARTIN

Chef du développement
Spatial Défense et Drones
Bordeaux Technowest

Nicolas MARTIN est chef du développement de la technopole Bordeaux Technowest, association parapublique dédiée à l'accompagnement d'entreprises innovantes via ses incubateurs & pépinières et au développement économique local via notamment ses centres d'affaires sur les parcs d'activités Aéroparc et Ecoparc sur la métropole de Bordeaux. Ingénieur aéronautique, il a complété son cursus par un master à l'IAE de Poitiers. Il effectué une première partie de carrière au sein du ministère de la Défense et en interministériel. Devenu consultant en 2015, il est un des artisans à l'origine du prochain centre de ressources cybersécurité de Mont-de-Marsan. Au sein de Technowest depuis 2017, il a permis l'accueil des premières entreprises cyber et a co-organisé plusieurs évènements de sensibilisation sur les enjeux de cybersécurité auprès des entreprises du territoires avec le soutien des instances régionales (Anssi, Clusir, collectivités, clubs des entreprises, autres services de l'Etat) dont il est le correspondant.

Francois CHARBONNIER

Investisseur Confiance Numérique
Banque des Territoires - Caisse des Dépôts



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.

Christine SAMANDEL

Chief of Staff & Project Owner Ecosystem
TEHTRIS

Diplômée en Sécurité Internationale et spécialisée en renseignement et cybersécurité de l'Ecole d'Affaires Internationales de Sciences Po Paris, Christine SAMANDEL a rejoint TEHTRIS au poste de Chief of Staff de Laurent OUDOT, co-CEO et CTO. Elle est notamment en charge des partenariats technologiques dans le cadre du projet TEHTRIS Ecosystem, un réseau de solutions de cybersécurité de confiance favorisant les co-innovations les plus performantes du marché.

Les intervenants

Toufik AHMED

Titulaire
Chaire Cyber Résilience des Infrastructures Numériques

Toufik AHMED est professeur des universités en Informatique à Bordeaux INP. Il exerce ses activités d'enseignement à l'ENSEIB-MATMECA (Ecole Nationale Supérieure d'Électronique, Informatique, Télécommunications, Mathématique et Mécanique de Bordeaux) et ses activités de recherche au laboratoire le LaBRI (Laboratoire Bordelais de Recherche en Informatique). Il est directeur de la recherche de l'innovation et du transfert de l'ENSEIRB-MATMECA et porteur de la chaire « Cyber résilience des infrastructures numériques », qui est consacrée au développement des recherches permettant d'atteindre la cyber résilience et des offres de formation diplômante en lien avec la cyber sécurité à l'image du Diplôme d'établissement « Expert Cybersécurité des Infrastructures Numériques ».

Lieutenant-Colonel Ludovic BONCOMPAIN

Chef du bureau appui numérique
Région de Gendarmerie Nouvelle-Aquitaine
Gendarmerie Nationale

Le Lieutenant-Colonel Ludovic BONCOMPAIN est entré en gendarmerie en 1997.

- 1998 : Gendarmerie Mobile Escadron de Mirande (32)
- 2001-2003 : École des officiers Melun (77)
- 2003-2007 : escadron de GM Versailles Satory : commandant de peloton blindé, missions de maintien de l'ordre en Métropole et OM, 2 missions de maintien de la paix au Kosovo
- 2007-2010 : cycle d'étude INFO 1 DGA Bourges/ENSI Bourges, chef de projet informatique dont :
- juillet 2009 : affectation au data center de la gendarmerie en région parisienne
- 2009-2010 : responsable de la cellule PCA-PRA, gestionnaire d'application métier judiciaire : mise en production et suivi, mémoire de validation de diplôme sur le PCA/PRA d'une application métier commune entre la GN et la PN
- 2010-2014 : chef du bureau télécommunication sécurité : accès centraux, réseau filaire du data center, réseau opérationnel hertzien national.
- 2014 – 2017 : commandant de la compagnie des Iles du vent à Tahiti (200 gendarmes, 170 000 habitants).
- 2017 – 2020 : chef du bureau de la coordination des opérations Région Picardie, conseiller technique SIC et cybersécurité, gestionnaire de flotte GSM, RSSI régional, coordination des SIC départementaux
- 2020 : chef du bureau appui numérique Région Nouvelle-Aquitaine, officier référent en sécurité économique, conseiller technique SIC et cybersécurité, gestionnaire de flotte GSM, RSSI régional, coordination des SIC départementaux (12 départements).

Amandine DEL-AMO

Chargée de mission partenariats
Cybermalveillance.gouv.fr

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

Adjudante Christelle BOISSIMON

Référente Sécurité Economique et Protection des Entreprises (SEcoPE)
Région de Gendarmerie Nouvelle-Aquitaine
Gendarmerie Nationale

Formée par l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ), l'adjudante Christelle BOISSIMON est référente Sécurité Economique et Protection des Entreprises (SEcoPE) à l'état-major de la région de gendarmerie de Nouvelle-Aquitaine.
Elle réalise diverses actions de prévention (diagnostic et sensibilisations) au profit des entreprises et des administrations, en abordant l'ensemble des risques et menaces susceptibles de les atteindre (fragilités humaines, sûreté, risques financiers, intrusions consenties, cybersécurité...)

Philippe STEUER

RSSI
Bordeaux Métropole

Avec plus de 30 années d'expérience dans le domaine des nouvelles technologies de l'information dont plus de la moitié dans la sécurité de l'information, Philippe STEUER est aujourd'hui Responsable de la Sécurité du Système d'Information commun à Bordeaux Métropole.
Par le passé, il a notamment été responsable d'une équipe d'intelligence économique au sein d'une banque française puis a été à l'initiative de la création d'un centre de lutte contre la cybercriminalité et en charge d'un centre de réponses aux attaques informatiques (CERT) au sein du grand groupe.
Après une année d'étude passée chez Audencia, il crée sa société de conseil en cyber. Il accompagne alors des startups et sociétés françaises et luxembourgeoises pour développer leurs services cyber, les adapter à leur cible en prenant en compte le pays et le domaine d'activité.
Fin 2018, nouveau défi professionnel sur Bordeaux. Il effectue un audit de maturité sécurité au sein de la DSI de Bordeaux Métropole après lequel il est intégré comme RSSI pour accompagner la transformation numérique de la Métropole.
En veille permanente sur les enjeux de sécurité, Il a participé à différents groupes de travail, anime des conférences et des tables rondes sur les menaces, vulnérabilités et contre-mesures dans le cyberespace.
Il est également actif dans le rayonnement de l'esprit de défense et dans le renforcement du lien armées-Nation en tant qu'auditeur IHEDN et réserviste auprès de la Direction Zonale de la Police Judiciaire de Bordeaux.

Baya LONQUEUX

Membre
Cercle des Femmes de la Cybersécurité

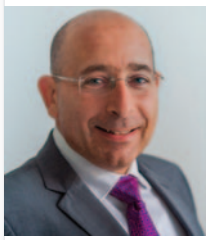
Baya LONQUEUX est un membre actif du CEFCYS, le Cercle des femmes de la Cybersécurité.
Après plus de 15 ans d'expériences dans la commercialisation de services informatiques, conciliant les exigences de pilotage commercial de Comptes Client, de construction ad'hoc et de développement de Centres de profits, et de management opérationnel d'équipes de delivery, elle a développé une expertise avancée dans le domaine de la sécurité des systèmes d'informations en prenant la responsabilité de la branche consulting d'un acteur clé du secteur.
L'esprit d'entreprendre, le goût de l'innovation, et la volonté d'animer l'écosystème de partenaires, prescripteurs, et d'industriels qui lui ont toujours fait confiance, ont fini de la convaincre de créer sa propre entreprise, la société Reciproc-it, une ESN spécialisée en sécurité des systèmes d'information.

Astrid FROIDURE

Chargée de Relations Publiques
Avant de Cliquer

David OFER

Président
Fédération Française de la Cybersécurité



Spécialiste des nouvelles technologies, de l'IA et de la cybersécurité, David OFER est président de la Fédération Française de la Cybersécurité.
Dirigeant d'entreprises de technologies, entrepreneur et investisseur depuis 25 ans, il est spécialiste de la croissance des entreprises et de l'internationalisation. Fervent défenseur de l'entreprenariat et des startups, il est actuellement Vice-président d'Itrust, société spécialisée en technologie de cybersécurité. Il est aussi en charge de la relation entre les investisseurs et les startups de cybersécurité à l'European Cybersecurity Organisation où il a créé les cyber investor days au niveau européen.
Avec un parcours très international, David OFER a lancé des startups qui anticipaient les marchés avec par exemple, l'invention des systèmes de cookies, l'introduction en France des QR-code, le développement de la publicité contextuelle sur mobile, ou l'Utilisation de l'IA en cybersécurité.
Il est titulaire d'un doctorat en administration des affaires et ingénieur en systèmes d'information, il est également passé par HEC où il est également membre référencé du Club Finances HEC.
Fréquemment consulté pour son anticipation des marchés technologiques, il a participé aux groupes de travail du comité sénatorial français sur les start-ups

Les intervenants

Alexandre DUBOIS

Directeur adjoint - référent national filière informatique
YNOV Bordeaux

Après 10 ans à oeuvrer dans le monde du développement web et principalement e-commerce, il a rejoint la direction du campus Ynov de Bordeaux.
Responsable national informatique pour ce groupe d'éducation, il dirige l'offre des programmes dans ce domaine dont une spécialité et un mastère en cybersécurité.

Marc-André BEAUDET

RSSI, membre
CESIN

Marc-André BEAUDET est membre du CESIN.
Titulaire d'un diplôme d'ingénieur du CNAM Paris, il évolue depuis plus de 15 ans dans le domaine de la sécurité des systèmes d'information, tout d'abord en tant que militaire d'active au sein d'une unité opérationnelle de l'Armée de Terre. Il a ensuite occupé différents postes d'ingénieur cybersécurité au sein de plusieurs institutions publiques (ANSSI, CNIL puis Ministère de l'Intérieur). avant d'évoluer vers des fonctions de RSSI, notamment au sein de l'aéroport de Bordeaux. Marc-André BEAUDET occupe depuis janvier 2021 la fonction de RSSI groupe au sein de Filhet-Allard, dont le siège est implanté dans la région bordelaise, société spécialisée dans le domaine du courtage d'assurance.

Benoît de SAINT-SERNIN

Président
Ecole Européenne de Cybersécurité

Benoît de SAINT-SERNIN a co-fondé et dirigé l'Ecole Européenne d'Intelligence Européenne depuis 2005. Ce groupe comprend aujourd'hui 3 écoles :
- EEIE : l'Ecole Européenne d'Intelligence Européenne
- EESP : l'Ecole Européenne de Sécurité Privée
- EECS : l'Ecole Européenne de Cyber Sécurité.

Diplômé de l'ESLSCA, il a précédemment crée en 1997 avec le Général Pichot-Duclos, l'Ecole de Guerre Economique (EGE), puis travaillé dans la communication chez Angie, Groupe ING Bank, Disneyland Resort Paris.
Lieutenant-colonel de la Réserve Citoyenne de la Gendarmerie Nationale, il est référent sur les questions d'IE.

RENCONTRES
CYBERSÉCURITÉ
NOUVELLE-AQUITAINE

MERCI À NOS PARTENAIRES & SOUTIENS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

PARTICULIERS, ENTREPRISES, COLLECTIVITÉS TERRITORIALES :

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

PIRATAGE

ARNAQUE

CHANTAGE

VIRUS

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

MISSIONS
DU DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

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

MEMBRES

PREMIER MINISTRE

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

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

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

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

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

LES JEUNES IHEDN

ENGAGEMENT

De la jeunesse

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

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

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

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

Propulser l'en

Passerelle entre les
l'association offre
transformer vos idé

Développer l

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

Que vous souhaitiez pro
développement, tout est

DIRECTION

LA PRO

DÉFE

RÉFLEXIONS SÉCU

SERVICE INTERNATI

INNOVATION CULTURE SOC

UNION EUROPÉENNE 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, de nombreuses opportunités de ées en engagement concret.

Promouvoir l'expertise innovante

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

a connaissance

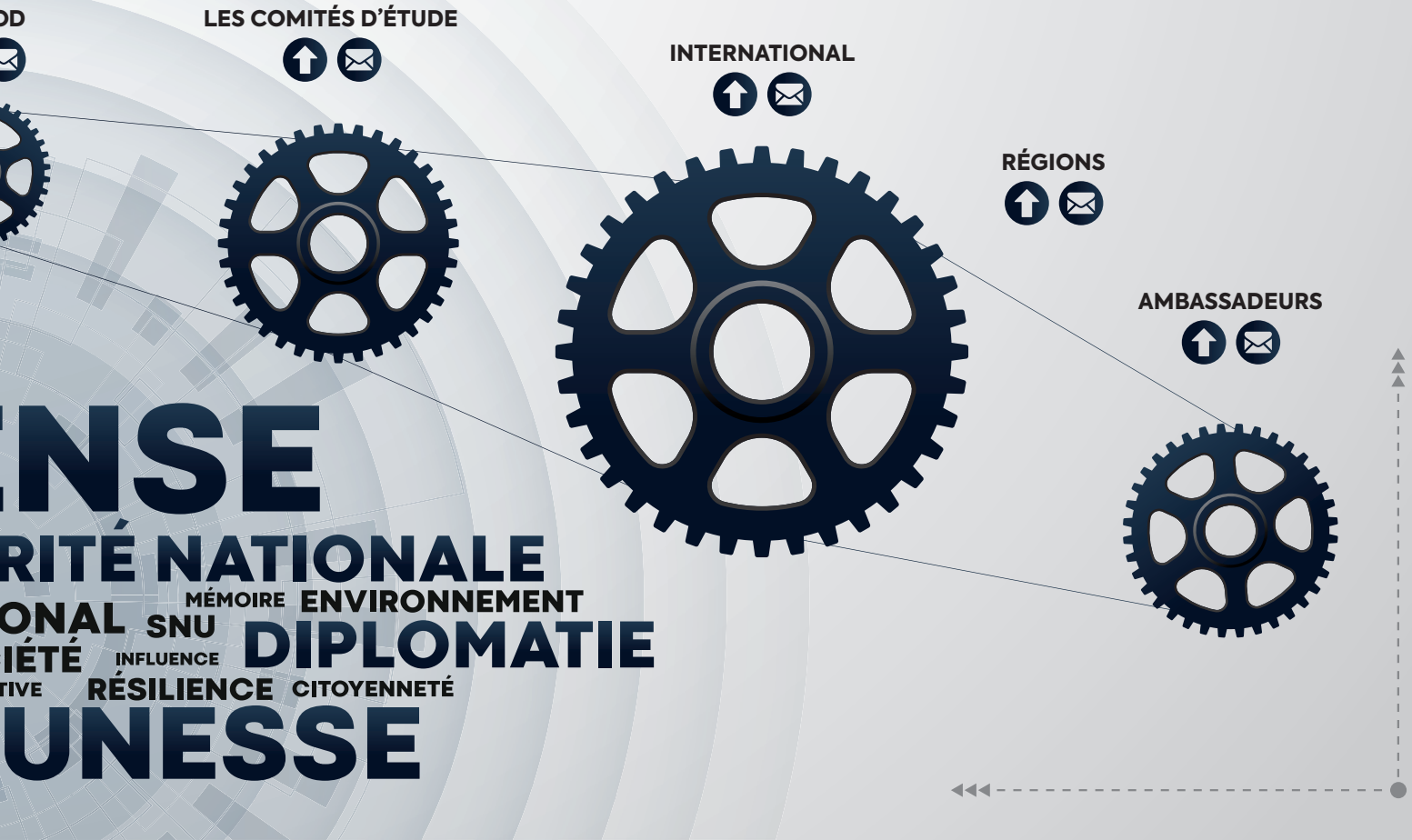
association organise une centaine de rs et visites sur des sujets généralistes ou e avec l'actualité.

Fédérer un réseau international

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

NOTRE ORGANISATION

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



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

CONFIANCE, QUALITÉ, EXPERTISE : LE LABEL EXPERTCYBER

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

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

1 QU'EST-CE QUE LE LABEL EXPERTCYBER ?

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

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

2 QUI SONT LES PRESTATAIRES LABELLISÉS ?

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

3 QUI PEUT FAIRE APPEL À UN PRESTATAIRE LABELLISÉ EXPERTCYBER ?

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

4 POURQUOI FAIRE APPEL À UN PRESTATAIRE LABELLISÉ ?

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

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

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

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

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

PLUS D'INFORMATIONS SUR
WWW.EXPERTCYBER.FR

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FICHE DE CONTACT
RÉSEAU DES RÉFÉRENTS CYBERMENACES DE LA POLICE NATIONALE

Vous êtes une société ?

Entreprise unipersonnelle, artisan, profession libérale, TPE/PME ?

Vous êtes victime d'une cyberattaque, d'une escroquerie utilisant Internet ou les réseaux sociaux ?

La Police judiciaire vous propose un point de contact unique pour le territoire : **Nouvelle-Aquitaine**

cybermenaces-bordeaux@interieur.gouv.fr

POLICE NATIONALE

Le réseau des référents cybermenaces de la Police nationale est une structure innovante composée de :

- **Réservistes** issus du monde de l'entreprise engagés dans la lutte contre la cybercriminalité
- **Policiers spécialisés**
- **Investigateurs en cybercriminalité**
- **Professionnels et Institutions partenaires**

POLICE NATIONALE

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

LES ACTEURS

VOUS SOUHAITEZ SÉCURISER VOS MARCHÉS ET VOTRE SAVOIR-FAIRE EN FRANCE ET À L'INTERNATIONAL ?

LA DIRECTION GÉNÉRALE DES DOUANES

- prévient les pratiques agressives et déloyales ;
- préserve les intérêts français à l'étranger via son réseau international d'attachés douaniers ;
- participe au contrôle des investissements étrangers en France ;
- promeut l'agrément Opérateur Economique Agréé (OEA), label de confiance douanier européen.

Contact

+33 (0) 9 70 27 55 80
pae-bordeaux@douane.finances.gouv.fr

Outil

www.douane.gouv.fr

L'ASSOCIATION FRANÇAISE DE NORMALISATION (AFNOR)

- propose des solutions fondées sur les normes volontaires, documents consensuels reflétant les bonnes pratiques les plus reconnues au niveau européen et international.

Contact

+33 (0) 5 57 29 14 33
delegation.bordeaux@afnor.org

Outil

https://normalisation.afnor.org/thematiques/numerique/

L'INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE (INPI)

- accompagne les entreprises, sur le territoire et à l'export, en matière de propriété industrielle pour protéger le savoir-faire des acteurs économiques en France.

Contact

0820 210 211
nouvelleaquitaine@inpi.fr

Outil

www.inpi.fr

VOUS SOUHAITEZ PROTÉGER VOS INFORMATIONS STRATÉGIQUES, VOS LOCAUX, SENSIBILISER VOS SALARIÉS, FAIRE UN DIAGNOSTIC ?

LA DIRECTION ZONALE DE SÉCURITÉ INTÉRIEURE (DZSI)

- participe à la protection du patrimoine scientifique et technique de la nation (PPST) ;
- apporte son expertise en matière de sécurité économique ;
- accompagne les entreprises dans leurs démarches de protection des informations stratégiques et sensibles.

Contact

securite-economique-bordeaux@interieur.gouv.fr

Outil

La lettre d'information « Flash Ingérence » disponible sur abonnement, à solliciter par écrit à l'adresse ci-dessus.

L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

- apporte son expertise et son assistance technique aux administrations et aux entreprises dans leur développement numérique ;
- assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

Contact

nouvelle-aquitaine@ssi.gouv.fr

Outils

www.ssi.gouv.fr
https://secnumacademie.gouv.fr/ (formation à distance)

LES DÉLÉGUÉS À L'INFORMATION STRATÉGIQUE ET À LA SÉCURITÉ ÉCONOMIQUES (DISSE)

- informent, orientent et conseillent les acteurs économiques en matière de sécurité économique.

Contact

na.disse@direccte.gouv.fr

Outils

Guide des 26 fiches de sécurité économique et DIESE (diagnostic d'intelligence économique et de sécurité économique) sur : https://sisse.entreprises.gouv.fr

GENDARMERIE : LES RÉFÉRENTS SÉCURITÉ ÉCONOMIQUE ET PROTECTION DES ENTREPRISES (SÉcoPE)

- aident à l'identification des risques et à l'adaption des dispositifs de protection ;
- organisent des actions de sensibilisation et de prévention au profit de différents acteurs (entreprises, associations, facultés...).

Contact

securite-economique-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

Outil

Jeu des 8 familles d'atteintes à la sécurité économique sur **www.gendarmerie.interieur.gouv.fr**

LE SERVICE ZONAL DU RENSEIGNEMENT TERRITORIAL (SZRT 33)

- assure le suivi économique et social des entreprises dans les départements ;
- exerce des fonctions de capteur dans la mise en œuvre globale de la politique publique d'intelligence économique ;
- détecte les vulnérabilités et les atteintes aux entreprises.

LA DÉLÉGATION RÉGIONALE À LA RECHERCHE ET À LA TECHNOLOGIE (DRRT)

- participe à la sensibilisation des établissements d'enseignement supérieur, des organismes publics et privés de recherche, des centres de ressources technologiques (CRT) ainsi que des jeunes entreprises innovantes (JEI), en matière de sécurité économique.

Contact

drrt.nouvelle-aquitaine@recherche.gouv.fr

VOUS ÊTES UNE ENTREPRISE ACTIVE SUR LES MARCHÉS DÉFENSE, OU INTÉRESSÉE PAR CES OPPORTUNITÉS ?

LA DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE (DRSD)

- décèle et neutralise toute menace contre les intérêts nationaux et la souveraineté nationale, touchant la sphère défense ;
- assure le suivi, la sensibilisation, le conseil des industries et instituts de formation ou de recherche en lien avec la défense dans sa mission de contre-ingérence économique (incluant la cyber défense).

Contact

+33 (0) 5 57 85 10 22

drsd-bordeaux-cie.contact.fct@intradef.gouv.fr

Outils

www.drsd.defense.gouv.fr

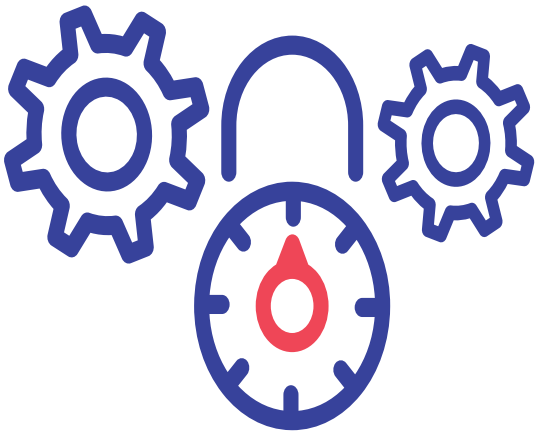
LA DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA)

- accompagne les PME de la base industrielle et technologique de défense (BITD) dans leur projet de développement (innovation, exportation, accès au marché) ;
- contribue à la sensibilisation des PME et ETI à la sécurité économique et à la cybersécurité.

Outils

www.achats.defense.gouv.fr (espace PME)

www.ixarm.com



PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE

SISSE Commissaire et Service de l'Information Stratégique et de la Sécurité Économiques

www.prefectures-regions.gouv.fr/nouvelle-aquitaine

@PrefAquitaine33 @PrefetNouvelleAquitaine33

ENTREPRISES ET LABORATOIRES
EN NOUVELLE-AQUITAINE

PROTÉGEZ VOS INFORMATIONS STRATÉGIQUES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFÈTE
DE LA RÉGION
NOUVELLE-AQUITAINE

SÉCURISEZ L'AVENIR DE VOTRE ENTREPRISE !

Chaque année, un nombre croissant d'entreprises et de laboratoires de recherche sont victimes de captations d'informations stratégiques ou sensibles.

Ces actes ciblés peuvent entraîner une perte de compétitivité importante pour l'établissement et altérer son image, voire mettre en péril son existence.

Certains savoir-faire peuvent également être détournés à des fins malveillantes.

Dans un monde où la concurrence est exacerbée, la compétitivité conditionne la survie de l'entreprise.

La protection des savoir-faire et des informations devient alors un enjeu vital pour sa pérennité.

Du chef d'entreprise à l'ouvrier, du cadre supérieur au chargé de communication, du directeur de laboratoire au chercheur, chacun est concerné par la sécurité économique.

LES RISQUES DE SÉCURITÉ

LES ATTEINTES PHYSIQUES SUR SITE

Intrusions dans un bâtiment (public ou privé) pour dérober des informations stratégiques non-protégées.

LA FRAGILISATION, LA DÉSORGANISATION D'ENTREPRISES

Manœuvres pour déstabiliser un établissement sous plusieurs formes : parasitisme, dénigrement, débauchage de personnel, détournement de clientèle, etc.

LES ATTEINTES AU SAVOIR-FAIRE

Perte de compétence clé, captation de brevet, contrefaçon de produits, concurrence déloyale, espionnage.

LES INTRUSIONS CONSENTIES

Captations d'informations stratégiques via les conférences, séminaires, visites de délégations étrangères, entrisme, stagiaires, intérimaires, etc.

LES RISQUES FINANCIERS

Dépendance vis-à-vis d'un client,d'un fournisseur prédominant, injection, de

LES ATTEINTES À LA RÉPUTATION

Attaque informationnelle sur l'identité et la situation de l'entreprise, qui porte préjudice à son image et à sa réputation.

LES FRAGILITÉS HUMAINES

Vol à distance d'informations stratégiques dans l'entreprise par des personnes extérieures via l'ingénierie sociale, par exemple en usurpant l'identité d'un salarié, d'un client ou d'un fournisseur.

LES RISQUES INFORMATIQUES

Destruction ou chiffrement de données, vols d'ordinateurs et de supports de stockage, atteintes aux traitements et systèmes automatisés de données, attaques par déni de service distribué.

capitaux par fonds activiste, escroquerie financière, sanctions de partenaires étrangers.

CONSEILS POUR VOTRE STRATÉGIE D'ENTREPRISE

Identifier son information stratégique

- réaliser un classement des informations détenues par votre entreprise ;
- se questionner sur l'impact qu'engendrerait la perte, la destruction ou la divulgation de ces informations ;
- identifier les informations sensibles, stratégiques et les lieux sensibles de votre entreprise.

Identifier les risques, menaces et vulnérabilités

- réaliser un diagnostic ;
- évaluer les forces et faiblesses de votre entreprise et sa progression dans le temps à l'aide d'outils informatiques (ex : logiciel DIESE via le site du SISSE).

Prendre des mesures de protection

- sensibiliser vos salariés aux risques ;
- encadrer l'accueil des personnes externes à votre entreprise ;
- protéger votre savoir-faire ;
- savoir bien communiquer sans divulguer vos informations stratégiques ;
- élaborer un plan de continuité et de reprise d'activité en cas de crise.

Assurer une veille

- surveiller l'évolution des réglementations qui affectent l'activité de votre établissement ;
- identifier les innovations ;
- surveiller la concurrence, votre image et son impact.

Mener des actions d'influence

- participer à l'élaboration des normes ;
- valoriser votre réseau, votre image.

Avantde Cliquer .com

L'humain au cœur de la cybersécurité

Vous êtes décideur…

Divisez /10
le risque de cyberattaques.

Développez la vigilance de vos utilisateurs et gagnez en sérénité

STOP

Pour en finir avec le phishing !

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

3 outils complémentaires

en live

UN AUDIT DE VULNERABILITÉ

L'APPRENTISSAGE PAR L'ACTION

UN BOUTON ALERTE CYBER

conçus / hébergés / développés en FRANCE

Les outils
Avant de Cliquer

UN AUDIT DE VULNERABILITÉ

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

UN BOUTON ALERTE CYBER

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

L'APPRENTISSAGE PAR L'ACTION

Un algorithme intelligent

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

Notre solution EN VIDEO

SENSIBILISATION SUR POSTE DE TRAVAIL

Envoi d'e-mails de faux phishing

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

Une sensibilisation immédiate

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

Montée en compétences personnalisée

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

Ecrans de veille éducatifs

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

Plateforme de e-learning

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

Test de la clé USB

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

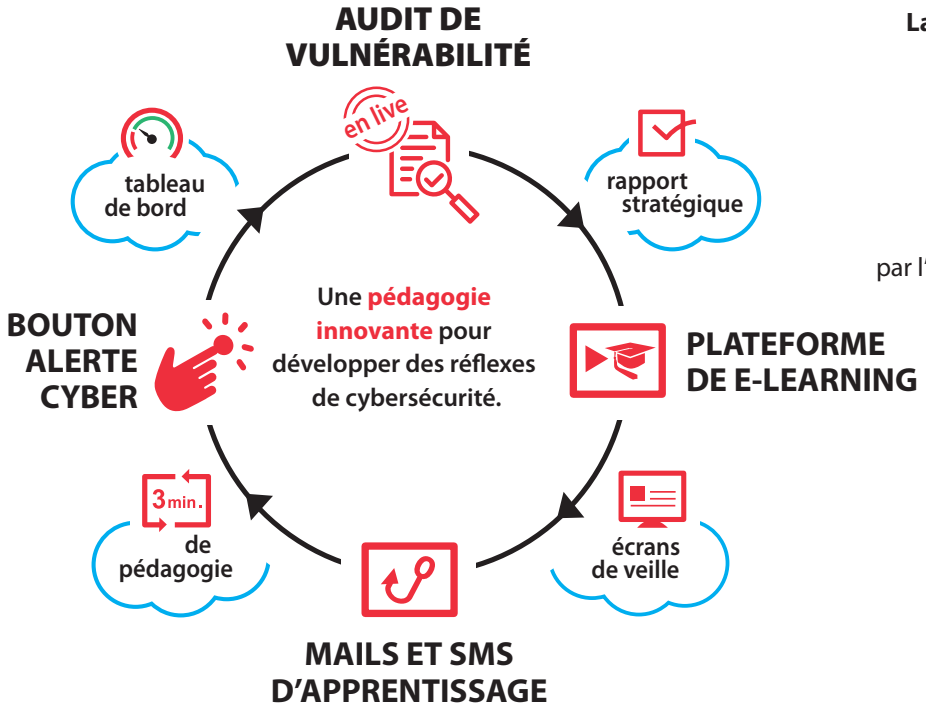
SOLAINN ACHATS INNOVANTS · bpifrance UNIVERSITE · C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière · Éditeur référencé UGAP-SCC · UGAP · The 2021 French CYBER-SECURITY STARTUPS radar · WAVESTONE

Les formules
Avant de Cliquer

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

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

LA SOLUTION COMPLETE : des réflexes acquis



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

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

Solution SaaS

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

2 MOIS EN TASK FORCE : parer à l'urgence

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

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

Vous êtes décideur…

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

RGPD

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

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

Avant de Cliquer en 2021 c'est :

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

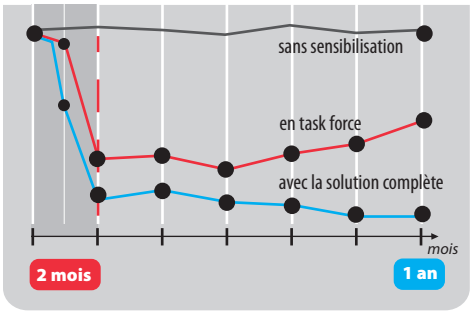
13 langues sous-titrées Français/anglais
Allemand, Anglais, Bulgare, Espagnol, Hongrois, Italien, Mandarin, Polonais, Portugais, Roumain, Russe, Turque, Ukrainien.

Niveau de risque

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

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

Evolution des clics



Avantde Cliquer .com

L'humain au cœur de la cybersécurité

www.avantdecliquer.com

Coordination technique et commerciale
Carl : 06 31 37 41 50

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

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

Référencé CAIH
Centrale d'Achat de l'Informatique Hospitalière

Bpi France
Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité

Référencé UGAP
L'achat public responsable

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

conçus / hébergés / développés en FRANCE

Conception Limage : 09/2021

PRÉSENTATION DU CYBERCERCLE

Missions / Vocation

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

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

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

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

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

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

PRÉSENTATION DU CYBERCERCLE

Valeurs

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

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

Positionnement

Le CyberCercle a un positionnement unique.

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

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

Activités

Les activités du Cybercercle s'articulent autour :

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

Ces événements sont plus ou moins ouverts.

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

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

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

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

Quelques chiffres

Le CyberCercle c'est :

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

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

MERCI À NOS PARTENAIRES & SOUTIENS

PARTENAIRES

BANQUE des TERRITOIRES
GROUPE CAISSE DES DÉPÔTS

Mérignac

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LE GROUPE LA POSTE

DIRECTION CYBERSÉCURITÉ GROUPE

AvantdeCliquer.com
L'humain au cœur de la cybersécurité

ENEDIS
L'ELECTRICITE EN RESEAU

CERTitude NUMERIQUE

SOUTIENS

PRÉFET DE LA RÉGION NOUVELLE-AQUITAINE
Liberté
Égalité
Fraternité

Direction régionale de l'économie, de l'emploi, du travail et des solidarités (DREETS)

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Gendarmerie nationale

POLICE NATIONALE
DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

RCM
OCLCPI • RÉFÉRENT CYBER MENACE

cpme
CONFÉDÉRATION DES PME

ADI
Nouvelle-Aquitaine
Agence de Développement et d'Innovation

BORDEAUX TECHNOWEST

CHAIRE DÉFENSE & AÉROSPATIAL

CLUSIR
Aquitaine

CERCS

APSSIS

ANPP

CESIN

LES JEUNES IHEDN

CYBER CERCLE

CYBER CERCLE

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