CYBER CERCLE

EN DISTANCIEL

RENCONTRES CYBERSÉCURITÉ NOUVELLE-AQUITAINE

#RCYBERNOUVELLEAQUITAINE
#TDFCYBER

RCyberNouvelle-Aquitaine en distanciel 24 NOVEMBRE 2022

Crédit photo Alain Zimeray

Bénédicte PILLIET
Présidente du CyberCercle

Edito

Le CyberCercle a fait de la sécurité et la confiance numériques des territoires un des axes forts de son action depuis 2014, encore renforcée en cette fin d'année 2022 par la création de l'Observatoire des Territoires de Confiance Numérique.

Etre au contact des acteurs locaux pour promouvoir la sécurité et la confiance numériques afin d'en faire un axe stratégique de développement et d'attractivité, engager des synergies au sein des écosystèmes, des territoires et entre les territoires, susciter des projets fédérateurs, être force de propositions pour les élus sont notamment les moteurs de notre action et de notre motivation en région depuis plus de huit ans.

La Nouvelle-Aquitaine est une des régions sur laquelle nous avons mis en place une dynamique tout au long de l'année avec la création du CyberCercle Nouvelle-Aquitaine et ses matinales bimestrielles et développé des partenariats de confiance avec un certain nombre d'acteurs majeurs de ce territoire.

« Dans « confiance et sécurité numériques », il y a le mot confiance et celle-ci s'applique aussi dans les relations professionnelles et humaines » : sur les sujets qui sont les nôtres, l'humain et la confiance doivent être au cœur des actions menées.

Et la confiance est un maitre-mot pour le CyberCercle.

Permettre dans un contexte de numérisation accrue de notre société et d'augmentation exponentielle des cyberattaques d'avoir accès à une parole de confiance sur la sécurité numérique, développer des réseaux de confiance pour favoriser les échanges constructifs et le développement d'une culture commune sur ces sujets, agir collectivement au service de l'intérêt général sont trois axes majeurs de notre action sur les territoires.

Et je tiens ici à remercier très sincèrement les organisations néo-aquitaines avec lesquelles nous travaillons sur ces sujets dans ce même état d'esprit tout au long de l'année : Digital Aquitaine, la French Tech Bordeaux, Aéronautique Valley, Niort Tech, sans compter les institutions que sont la DCPJ Sud Ouest, la DREETS, la Région de Gendarmerie Nouvelle-Aquitaine, et également les organisateurs de HACK-IT-N 2022, Tehtris et ENSEIRB-MATMECA, avec lesquels cette année nous avons créé une dynamique entre nos deux événements.

Je remercie tout particulièrement Madame Fabienne Buccio, Préfète de Nouvelle-Aquitaine, Préfète de Gironde, d'avoir accepté d'ouvrir les travaux de cette quatrième édition, ainsi que le général de division Samuel Bubuis, commandant de la Région de Gendarmerie Nouvelle-Aquitaine de se faire représenter par le général de brigade Christophe Buisson, commandant en second de la Gendarmerie dans le cyberespace, pour l'intervention de clôture.

Je tiens aussi à remercier nos partenaires qui nous accompagnent en région, partageant leur expertise avec pédagogie : le Groupe La Poste, Cybermalveillance.gouv.fr, proofpoint, CERTitude NUMERIQUE, Dicé, Avant de Cliquer, CSB School, ENEDIS, le cabinet S.B. & B.D, la Banque des Territoires. Je remercie enfin nos soutiens, collectivités, ministères, associations, écoles, qui s'associent à notre action dans cet esprit fédérateur qui est le nôtre.

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

« *Seul on va plus vite. Ensemble on va plus loin.* »
« *Construire ensemble des territoires de confiance et de sécurité numériques.* »
« *Agir efficacement ensemble pour construire une culture de sécurité numérique partagée au service des acteurs présents sur les territoires.* »

Cette quatrième édition des Rencontres de la Cybersécurité Nouvelle-Aquitaine et plus largement notre action sur ce territoire néo-aquitaine s'inscrivent pleinement dans ce triptyque dynamique qui est le nôtre depuis 2014, de plus en plus fondamental pour faire face collectivement aux enjeux actuels, qu'ils soient économiques, sécuritaires ou sociétaux.

DOSSIER PARTICIPANT

RCyberNouvelle-Aquitaine en distanciel 24 NOVEMBRE 2022

Cécile DESMOND
Ambassadrice Nouvelle-Aquitaine

Edito

Je suis ravie d'accompagner la dynamique et les valeurs du CyberCercle sur notre région depuis 2021, avec la création du CyberCercle Nouvelle-Aquitaine.

Ces 4èmes Rencontres complètent un ensemble d'actions que nous menons tout au long de l'année sur notre territoire, que ce soit les Matinales bimestrielles ou des interventions des senior advisors du CyberCercle dans le cadre de plusieurs évènements de l'écosystème néo-aquitain : le soutien à la filière cybersécurité à la Maison de la Nouvelle Aquitaine à Paris, la table ronde d'ouverture sur la cyber-résilience du salon INNN qui s'est déroulé à Niort.

Ressources au coeur de notre action : l'expertise à vocation pédagogique, le partage et les échanges, en s'appuyant sur les femmes et les hommes, professionnels et acteurs engagés sur le terrain, mais aussi étudiants, réservistes ou bénévoles citoyens qui s'impliquent pour participer de cette clairvoyance. Et parce que l'Humain est la clé, comme nous le rappelle la 1ere thématique de ces Rencontres, je tiens à remercier chacune et chacun pour vos interventions et vos actions.

Dans cette très grande région Nouvelle Aquitaine qui compte douze départements et dont l'ensemble des filières contribue fortement à l'économie de notre pays, les enjeux liés à la cybersécurité sont évidemment majeurs.
Les collectivités, les acteurs publics ou privés du territoire sont aujourd'hui impliqués sur ces sujets, dans le cadre du déploiement de politiques nationales, de feuilles de routes régionales ou locales, d'investissement de filières ou d'écosystèmes pour accroître la résilience, maintenir la confiance et contribuer aux enjeux de souveraineté. Notre volonté de contribuer par nos actions à mieux faire comprendre les déploiements des politiques publiques de sécurité et de confiance numériques s'inscrit également dans la démarche nationale du CyberCercle qui renforce cette année son action avec la création de l'Observatoire des Territoires de Confiance Numérique. Mais nous aurons l'occasion d'en reparler...

Le CyberCercle Nouvelle-Aquitaine à travers les différentes keynotes de cette matinée de Rencontres, vise ainsi à mettre en lumière la trame de certaines actions conduites sur notre territoire, comme la stratégie de déploiement menée par Enedis, ou des projets et synergies d'actions en cours sur la région, tels que le Centre de Ressources Cyber Nord Nouvelle-Aquitaine porté par Niort.

Rappelons aussi que ces Rencontres du 24 novembre 2022 sont couplées avec l'évènement Hack-It-N qui se déroulera le 25 novembre, et ceci à la faveur d'une dynamique commune pour à la fois promouvoir le développement des compétences nécessaires à la croissance de nos filières techniques et d'excellences en matière de cybersécurité, mais aussi, pour ouvrir plus largement à la compréhension des enjeux de transformation numérique au service des acteurs publics et privés du territoire néo-aquitain.

Cet objectif du CyberCercle Nouvelle-Aquitaine de diffuser une culture pluridisciplinaire et élargie de sécurité et confiance numériques d'un numérique au service de la société de demain, dans le sens de l'intérêt général et de co-construction avec les acteurs locaux et nationaux, se poursuivra tout au long de l'année 2023.

Et nous serons heureux de vous y associer et de vous y retrouver.

■›› OUVERTURE DES TRAVAUX

➤ **Fabienne BUCCIO**, préfète de la Région Nouvelle-Aquitaine, préfète de la zone de défense et de sécurité Sud-Ouest, préfète de la Gironde

➤ **Bénédicte PILLIET**, présidente du CyberCercle, et **Cécile DESMOND**, ambassadrice du CyberCercle Nouvelle-Aquitaine, animeront les travaux de cette matinée.

■›› FAIRE FACE A LA MENACE CYBER EN S'APPUYANT SUR LE FACTEUR HUMAIN

Etat actualisé de la menace et perspectives judiciaires

Commissaire Divisionnaire Paul BOUSQUET, chef de la division de lutte contre la criminalité financière, direction zonale de Police Judiciaire Sud-Ouest

Ransomware : anticiper pour ne pas subir : l'humain au coeur du dispositif

Loïc GUEZO, directeur Stratégie Cybersécurité, Proofpoint

La formation pour développer la cybersécurité face au phishing

Astrid FROIDURE, responsable des Affaires Publiques, Avant de Cliquer

Mise en œuvre en entreprise d'une filière cybersécurité dans les régions, de la stratégie initiale à la réalisation

Sébastien POCHON, référent cyber, directions régionales Limousin et Auvergne, Enedis
Charlotte VIALAT, référente cyber, directions régionales Aquitaine Nord et Pyrénées Landes, Enedis

■›› LES COLLECTIVITES AU COEUR DES ENJEUX DE CYBERSECURITE

➤ « Data, intelligence artificielle et cybersécurité dans les territoires », note de conjoncture du Groupe La Poste et de la Banque des Territoires – Caisse des Dépôts

Dr Michel DUBOIS, directeur technique, direction de la Cybersécurité, Groupe la Poste

➤ La stratégie de territoire développée à Niort autour de la cybersécurité

Marc PARENTHOEN, enseignant-chercheur, Institut des risques, Niort

■›› RENFORCER LA FILIERE CYBERSECURITE : UN ENJEU DE SOUVERAINETE

➤ **Plan de relance & investissement pour la cybersécurité sur les territoires**
François CHARBONNIER, investisseur Confiance numérique, Banque des Territoires – Caisse des Dépôts

➤ **Comment des organisations phares de la filière numérique en Nouvelle-Aquitaine intègrent-elles la cybersécurité dans leurs actions**
Antoine LAMARCHE, directeur, Digital Aquitaine
Philippe METAYER, directeur général délégué, French Tech Bordeaux

➤ **Label Expert Cyber et Référentiel de compétences : construire sur les territoires un réseau de prestataires de confiance en matière de cybersécurité**
Franck GICQUEL, responsable des partenariats, Cybermalveillance.gouv.fr

■›› INTERVENTION DE CLOTURE

➤ **Général de brigade Christophe HUSSON**, commandant en second, commandement de la Gendarmerie dans le cyberespace, Gendarmerie nationale

Les intervenants

Fabienne BUCCIO

Préfète de la région Nouvelle-Aquitaine
Préfète de la zone de défense et de sécurité Sud-Ouest
Préfète de la Gironde

Après avoir fait une carrière de plus de 20 ans dans différentes préfectures, Fabienne BUCCIO est titularisée préfète en 2007, où elle est nommée dans 4 départements, en Mayenne, dans l'Eure, dans la Loire, puis dans le Pas-de-Calais.
En mars 2017, elle devient préfète de région, où elle est nommée préfète de la région Normandie, préfète de Seine-Maritime ; puis en mars 2019, elle devient préfète de la région Nouvelle-Aquitaine, préfète de la zone de défense et de sécurité Sud-Ouest et préfète de la Gironde.

Cécile DESMOND

Ambassadrice Nouvelle-Aquitaine
CyberCercle

Dans le cadre de ses activités d'assureur, l'arrivée d'offres de cyber-assurance pour les PME-ETI a conduit Cécile DESMOND dès 2015 à explorer la cybersécurité de manière transverse et à rencontrer des experts pluridisciplinaires liés à ce domaine afin de mieux l'appréhender dans le cadre de son métier d'assureur.
Passionnée par ces sujets, elle est devenue membre du Clusir Nouvelle Aquitaine. A ce titre, elle a organisé plusieurs évènements autour de la sécurité numérique et de ses enjeux business, et participé à des ateliers sur la cyber-assurance, en synergie avec des acteurs locaux (clubs d'entreprises, clusters, technopoles..)
Rattachée au réseau de la Réserve Citoyenne Cyberdéfense (armée de l'air) depuis 2017, elle contribue également à la sensibilisation de la société civile aux enjeux de cyberdéfense.
Issue d'un parcours professionnel initial en Ressources Humaines, Cécile DESMOND est particulièrement sensible aux questions de formations, développement des compétences et reconversions, points d'intérêts majeurs aujourd'hui dans le secteur de la cybersécurité.
Elle est depuis 2021 ambassadrice régionale Nouvelle-Aquitaine du CyberCercle.

Commissaire divisionnaire Paul BOUSQUET

Chef de la division de lutte contre la criminalité financière
Direction zonale de Police Judiciaire 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.

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.

Loïc GUEZO

Directeur Senior, Stratégie Cybersécurité, SEMEA
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.

Astrid FROIDURE

Chargée de Relations Publiques
Avant de Cliquer

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

Charlotte VIALAT

Référente Cybersécurité DR AQN et PYL
Direction Régionale Aquitaine Nord
Enedis

Responsable des enjeux de cybersécurité sur les régions Aquitaine Nord et Pyrénées-Landes chez Enedis depuis novembre 2021.
Juriste en droit de l'environnement de formation. J'ai intégré le groupe EDF en 2004 et exercé plusieurs missions : juriste-conseil, chargé de portefeuille de concessions, appui prévention-sécurité, PMO au sein du domaine Clients, pilote de la transformation des centres d'appels dépannage et consultante interne.

Dr Michel DUBOIS

Directeur 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).

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.

Marc PARENTHOËN

Enseignant-chercheur en informatique
Université de Poitiers, IRIAF, XLIM équipe ASALI-IG, UMR CNRS 7252

Marc Parenthoën est enseignant-chercheur en informatique à l'université de Poitiers, XLim UMR CNRS 7252, responsable du master Risques et environnement, dont le parcours Risques des systèmes d'information est labellisé SecNumedu. À l'Institut des Risques Industriels, Assurantiels et Financiers (IRIAF), composante niortaise de l'université de Poitiers, le cyber range FRUIT by IRIAF fédère ses activités de recherche autour de la formation aux bons réflexes dans les usages de la cybersécurité principalement à destination des collectivités, des administrations et des petites entités privées dans un objectif de résilience cyber des territoires, dispositif de formation-recherche clé de voûte du Centre de Ressources Cyber Nord Nouvelle-Aquitaine.

Les intervenants

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.

Antoine LAMARCHE

Directeur
Digital Aquitaine

Né à Bordeaux, j'ai une double formation scientifique (DEA Physique/chimie) et marketing (DESS IAE).
Passionné par la création et la technologie j'ai longtemps travaillé dans les médias et les industries culturelles à Paris avant de rejoindre Cdiscount et de retrouver ma région d'origine. Dans ces nouvelles fonctions j'ai pu accompagner l'hyper croissance d'une startup devenue licorne et son engagement dans une politique RSE pragmatique.
Je suis naturellement très intéressé par le digital et sa capacité de transformation et particulièrement attentif au développement durable et à la notion d'impact.
Mais aussi...
Passionné de pop culture, de littérature, de rugby, je suis aussi gamer et apprenti apiculteur.

Philippe MÉTAYER

Directeur Général
La French Tech Bordeaux

Philippe Métayer est le Directeur Général de La French Tech Bordeaux, qui fédère désormais plus de 1500 entreprises technologiques et innovantes et représente plus de 32 000 emplois, hors ETI et grands groupes.
Electronicien de formation, Philippe Métayer a travaillé dans des startups industrielles et des grands groupes au début de sa carrière professionnelle. Il a ensuite choisi d'enseigner puis a pris la direction adjointe de l'IUT Bordeaux Montaigne en 2008. Il rejoint ensuite Bordeaux Métropole en 2015 avec comme mission de structurer l'écosystème technologique et innovant du territoire. En 2018, il prend la Direction générale de La French Tech Bordeaux. Expert en innovation, technologies et écosystèmes numériques, Philippe Métayer est également Maitre de Conférences Associé à l'Université Bordeaux Montaigne.

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.

Général de brigade Christophe HUSSON

Commandant en second
Commandement de la gendarmerie dans le Cyberespace

Le Général de brigade Christophe HUSSON est Commandant en second de la gendarmerie dans le Cyberespace – Administration centrale.
Il fût Commandant du groupement de gendarmerie départementale du Nord (Commandement territorial) : Responsable de la sécurité publique sur 75% du territoire. À la tête de 1 360 personnels d'active répartis sur 54 points de présence et de 530 réservistes – 2018.
Chargé de mission, Cabinet du directeur général de la gendarmerie nationale, administration centrale : préparation et suivi des grands dossiers liés aux systèmes d'information impliquant la gendarmerie – 2017.
Chargé de mission Service des technologies et des systèmes d'information de la sécurité intérieure ST(SI)2, administration centrale : préparation et suivi des grands dossiers transverses du service – 2015...
Le Général de brigade Christophe HUSSON est Chevalier de la légion d'honneur (2018) et Officier Ordre national du Mérite (2022).

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

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

MINISTÈRE DES ARMÉES

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

proofpoint®

Protégez les personnes. Défendez les données.

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

En savoir plus :
Proofpoint.com/fr

proofpoint®

Protect people. Defend data.

Sensibilisation à la sécurité

Instaurez une culture de sensibilisation à la sécurité informatique

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

En savoir plus :
Proofpoint.com/fr

LES JEUNES IHEDN

ENGAGEMENT

De la jeunesse

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

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

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

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

Propulser l'en

Passerelle entre les
l'association offre
transformer vos idé

Développer l

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

Que vous souhaitiez pro
développement, tout est

NOS ACTIONS

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

ngagement !

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

Promouvoir l'expertise innovante

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

a connaissance

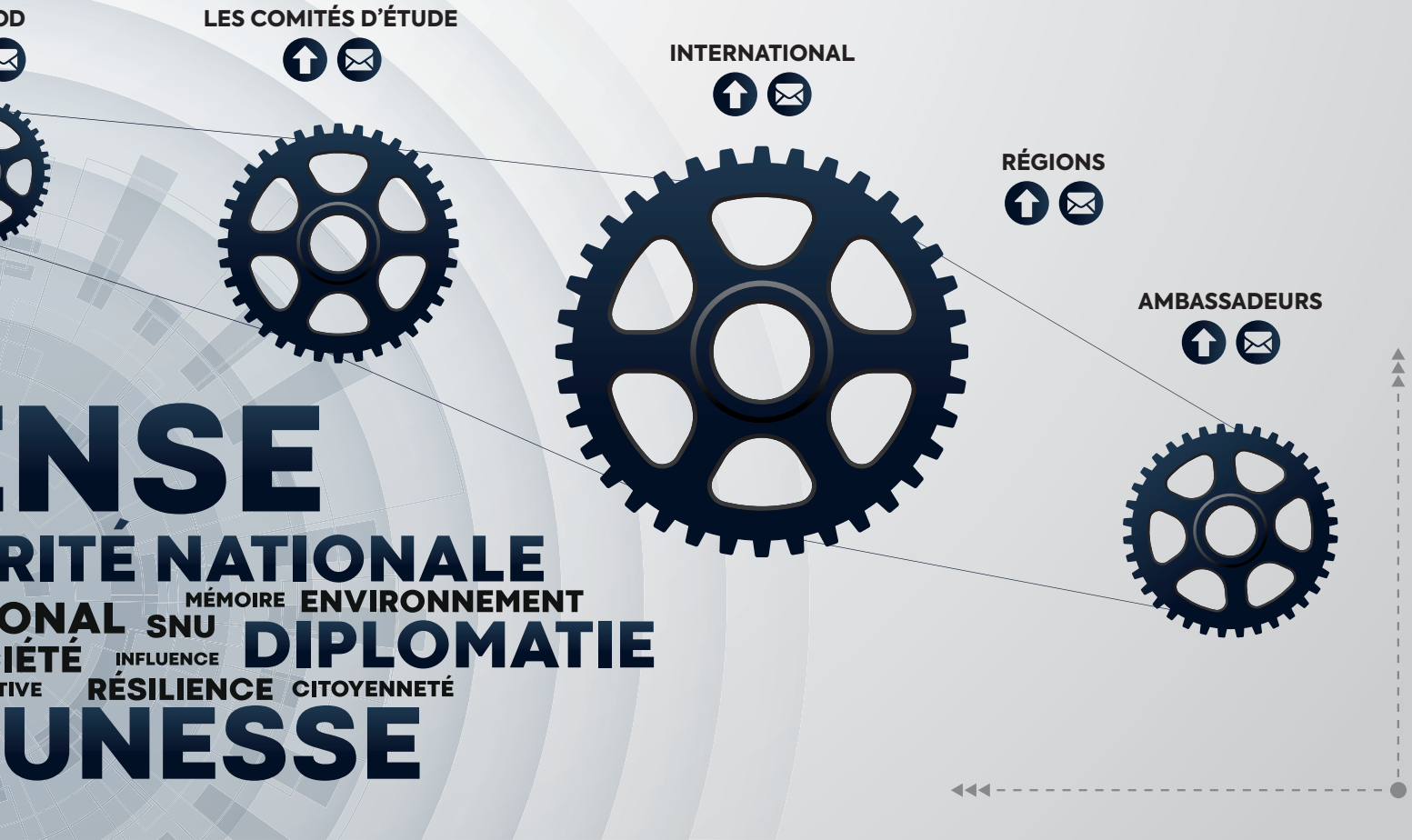
association organise une centaine de rs et visites sur des sujets généralistes ou e avec l'actualité.

Fédérer un réseau international

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

NOTRE ORGANISATION

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



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

LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

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

UN CONSTAT

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

3 AXES OPÉRATIONNELS STRATÉGIQUES

AXE 1

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

AXE 2

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

AXE 3

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

LA MISE EN ŒUVRE DU RÉSEAU

Par qui ?

Le réseau est constitué :

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

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

Pour qui ?

Le réseau s'adresse principalement :

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

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

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

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

VOUS ÊTES VICTIME D'UNE CYBERATTAQUE ?

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

LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

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

CONTACTS

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

CSB.SCHOOL

N'étudiez pas la cybersécurité, vivez-la !

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

Bachelor Spécialiste en cybersécurité

Mastère Manager en cybersécurité

Formation Intra-Entreprise

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

CYBERSECURITY BUSINESS.SCHOOL

39 rue de la Cité - 69003 LYON

N'étudiez pas la cybersécurité, vivez-la

Plus qu'un slogan, une réalité à la CSB

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

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

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

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

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

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

Patrice Chelim.
Directeur de la CSB

ZOOM SUR :

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

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

Avantde Cliquer .com

L'humain au cœur de la cybersécurité

Vous êtes décideur…

Divisez /10
le risque de cyberattaques.

Développez la vigilance de vos utilisateurs et gagnez en sérénité

STOP

Pour en finir avec le phishing !

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

3 outils complémentaires

en live

UN AUDIT DE VULNERABILITÉ

L'APPRENTISSAGE PAR L'ACTION

UN BOUTON ALERTE CYBER

conçus / hébergés / développés en FRANCE

Les outils
Avant de Cliquer

UN AUDIT DE VULNERABILITÉ

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

UN BOUTON ALERTE CYBER

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

L'APPRENTISSAGE PAR L'ACTION

Un algorithme intelligent

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

Notre solution EN VIDEO

SENSIBILISATION SUR POSTE DE TRAVAIL

Envoi d'e-mails de faux phishing

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

Une sensibilisation immédiate

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

Montée en compétences personnalisée

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

Ecrans de veille éducatifs

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

Plateforme de e-learning

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

Test de la clé USB

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

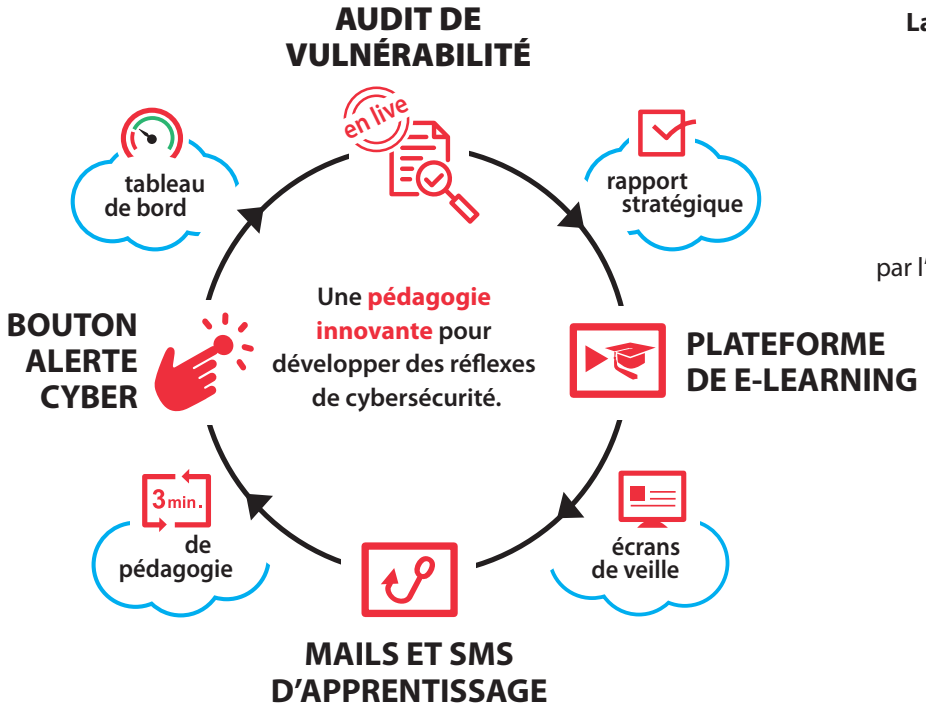
SOLAINN ACHATS INNOVANTS · bpifrance UNIVERSITE · C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière · Éditeur référencé UGAP-SCC · UGAP · The 2021 French CYBER-SECURITY STARTUPS radar WAVESTONE

Les formules
Avant de Cliquer

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

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

LA SOLUTION COMPLETE : des réflexes acquis



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

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

Solution SaaS

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

2 MOIS EN TASK FORCE : parer à l'urgence

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

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

Vous êtes décideur…

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

RGPD

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

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

Avant de Cliquer en 2021 c'est :

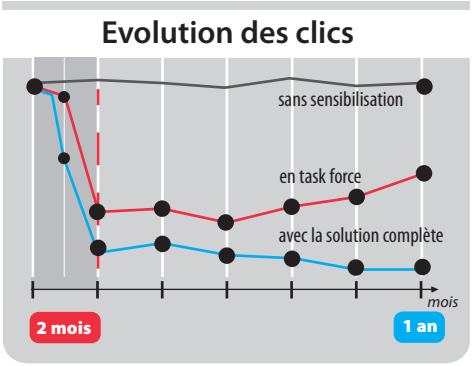
« 23 collaborateurs installés en Normandie.
La jeune entreprise créée en 2017 sensibilise **plus de 250 000 utilisateurs** et se développe aujourd'hui **à l'international. »**

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

Niveau de risque

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

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



Avantde Cliquer .com
L'humain au cœur de la cybersécurité

www.avantdecliquer.com

Coordination technique et commerciale
Carl : 06 31 37 41 50

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

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

Référencé CAIH
Centrale d'Achat de l'Informatique Hospitalière

Bpi France
Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité

Référencé UGAP
L'achat public responsable

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

conçus / hébergés / développés en FRANCE

Conception Limage : 09/2021

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

NOTRE CABINET VOUS ACCOMPAGNE

PAR UN PILOTAGE ANTICIPÉ, GLOBAL & TRANVERSAL

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

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

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

Les objectifs de cette démarche innovante :

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

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

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

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

TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCYBER

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS

@CyberCercle
@CyberTerritoire

PRÉSENTATION DU CYBERCERCLE

Missions / Vocation

Le CyberCercle est un cercle de réflexion créé en 2011 lorsque la sécurité numérique – la cybersécurité - n'était encore trop souvent qu'à ses débuts pour de nombreuses organisations et l'apanage des experts techniques.

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

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

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

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

PRÉSENTATION DU CYBERCERCLE

Valeurs

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

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

Les activités

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

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

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

Positionnement

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

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

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

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

CYBER CERCLE PAROLE D'EXPERT

Affronter la tempête cyber

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

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

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

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

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

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

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

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

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

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

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

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

[1] https://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/jet2020-cyber-espionage-ebook-en-fr.pdf

Quelques chiffres

Le CyberCercle en quelques chiffres, depuis 2012 :

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

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

MERCI À NOS PARTENAIRES & SOUTIENS

CYBER CERCLE

CYBER CERCLE

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