CYBER CERCLE

10 DÉCEMBRE 2019

NANTES

RENCONTRES CYBERSÉCURITÉ PAYS DE LA LOIRE

#RCYBERPAYSDELALOIRE
#TDFCYBER2019

Région PAYS DE LA LOIRE

TOUR DE FRANCE DE LA CYBERSÉCURITÉ

#TDFCYBER

@CyberCercle
@CyberTerritoire

ESPACES DÉMOS
TABLES RONDES
FORMATION
NETWORKING
RECRUTEMENT
ATELIERS

DOSSIER PARTICIPANT

RCyberPaysdelaLoire
NANTES
10 DÉCEMBRE 2019

Edito

Christelle MORANÇAIS
Présidente de la Région des Pays de la Loire

Notre monde se numérise à vitesse grand V. Rares sont désormais les domaines de la vie quotidienne qui échappent au numérique. Pour le meilleur et pour le pire. Et le pire est encore trop souvent ignoré du grand public et des entreprises. Peu d'entre nous mesurent concrètement les dangers qui planent au-dessus de nos données personnelles, et qui constituent autant de menaces pour notre intimité : nos comptes bancaires, nos bulletins de santé..., mais aussi nos brevets industriels ou de recherche et, plus fondamentalement, nos démocraties qui sont l'objet de cyberattaques toujours plus difficiles à déjouer.

Toute la société est concernée, et c'est toute la société qui doit collectivement tendre vers le « principe de vigilance », encore très absent de nos usages numériques.

Mais pour mesurer les risques encourus, encore faut-il mieux identifier les menaces et la façon de s'en prémunir efficacement. L'enjeu est de taille, car il en va en matière de cybercriminalité comme de dopage : les délinquants ont toujours un coup d'avance sur les autorités. Et ceux qui s'y prêtent sont d'autant plus dangereux qu'ils ne connaissent ni limites technologiques ni frontières géographiques, recourent à leur propre système monétaire et de transaction ; quand ils ne bénéficient pas de l'appui de certains Etats corrompus...

La Région des Pays de la Loire a de formidables atouts à faire valoir en matière de cybersécurité, et des places fortes à valoriser : Nantes, Angers, Cholet ou Laval abritent des fleurons industriels et des start-up spécialisées qui nous positionnent parmi les régions les plus avancées sur ce sujet. L'ancrage territorial de cet écosystème unique est pour nous une priorité, et un gage de réussite pour l'avenir.

Au cours de l'année 2020, la Région prendra d'ailleurs des initiatives fortes, à travers notamment le déploiement du nouveau programme « Initiative Cyber Région », pour consolider et amplifier la dynamique de cette « industrie du futur » qui concourt à l'intérêt général et à la vitalité économique de nos territoires.

La cybersécurité procède d'une logique simple et commune à l'ensemble des espaces privés et publics qui composent nos sociétés : c'est parce que la sécurité y est garantie qu'au-lieu de constituer une menace et un risque, l'espace numérique demeure un formidable lieu d'opportunités et de développement. C'est cette conviction qui anime « Nos Rencontres de la cybersécurité », organisées avec le Cercle de la Cybersécurité, et que la Région est très fière d'accueillir.

DOSSIER PARTICIPANT

RCyberPaysdelaLoire
NANTES
10 DÉCEMBRE 2019

Edito

Crédit photo Alain Zimeray

Bénédicte PILLET
Présidente du CyberCercle

Après Bourges, Pau, Toulon, Lannion et Lyon, le Tour de France de la Cybersécurité s'arrête pour sa dernière étape de l'année 2019 à l'Hôtel de la Région des Pays de la Loire à Nantes.

Je remercie très sincèrement la Présidente de la Région des Pays de la Loire, Christelle Morançais, d'avoir accepté de soutenir et d'accueillir cette journée des Rencontres de la Cybersécurité Pays de la Loire.

Nous vivons aujourd'hui une véritable transformation numérique qui impacte l'ensemble des acteurs, publics et privés, quelle que soit leur taille, et que ce soit au niveau national, international et bien évidemment territorial.
Mais force est de constater que le travail à accomplir pour que nos territoires deviennent des territoire de confiance numérique, favorisant ainsi 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.

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

Le territoire dans lequel nous sommes s'est résolument engagé dans la construction de territoires de confiance numérique.

Sous l'impulsion de sa présidente, la Région des Pays de la Loire a en effet mis le numérique et la sécurité numérique au cœur de ses politiques publiques, soutenues par un écosystème dynamique.

Le CyberCercle a fait de la sécurité et la confiance numériques des territoires un axe majeur de son action. Raison pour laquelle il a lancé l'année dernière le Tour de France de la Cybersécurité
Aller au contact des acteurs locaux, quels qu'ils soient, 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.
Et je tiens à remercier nos partenaires, de plus en plus nombreux, qui pour certains nous suivent depuis le début et sur l'ensemble du TDFCyber.

Rappelons-nous que la sécurité numérique demande un effort individuel mais surtout collectif, allant bien au-delà de la sphère des experts dans laquelle elle est encore trop souvent enfermée. Et que le rôle des élus au niveau des territoires est fondamental.

« *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 première édition des Rencontres de la Cybersécurité Pays de la Loire veut s'inscrire pleinement dans cette dynamique constructive.

RENCONTRES
CYBERSÉCURITÉ
PAYS DE LA LOIRE

LE PROGRAMME

Programme

Hôtel de la Région des Pays de la Loire, Nantes

RENCONTRES CYBERSÉCURITÉ PAYS DE LA LOIRE

8h15 **Ouverture de l'accueil** autour d'un buffet petit-déjeuner dans l'espace de rencontres

9h00 **Ouverture de la journée**

- Mot de bienvenue de **Bénédicte PILLIET**, Présidente du CyberCercle
- Ouverture par **Christelle MORANÇAIS**, Présidente de la Région des Pays de la Loire

9h30 **Table ronde**

Territoires numériques de confiance : quelles actions mener pour développer l'équité des territoires ?

Thèmes abordés :
Enjeux – développement économique, sécurité, mobilité, transports, formation... coordination entre acteurs nationaux et acteurs locaux
Rôle des politiques publiques locales
Quelles responsabilités pour quelles entités (rôle du conseil régional, du département, des communauté de communes, des métropoles...)

- **Paul JEANNETEAU**, Vice-président de la Région des Pays de la Loire, Président de la Commission entreprise, développement international, tourisme, innovation, enseignement supérieur et recherche
- **Jeanne BEHRE-ROBINSON**, adjointe au maire en charge de la sécurité, ville d'Angers
- **Gabriel de BROSSES**, Directeur de la Cybersécurité, Groupe La Poste
- **Philippe LOUDENOT**, Fonctionnaire de la Sécurité des Systèmes d'Information, ministères sociaux – membre du conseil d'administration, CESIN
- **Colonel Richard PEGOURIE**, conseiller affaires métropolitaines, Région de Gendarmerie des Pays de la Loire
- **Alexandre de CENIVAL**, membre du réseau des référents cybermenaces, sous-direction de la lutte contre la cybercriminalité, Direction Centrale de la Police Judiciaire

11h00 **Pause café**

11h30 **Key notes**

- « Services numériques aux citoyens : où en sont les collectivités territoriales ? », présentation de l'étude du GROUPE LA POSTE

Gabriel de BROSSES, Directeur de la Cybersécurité, Groupe La Poste

- La stratégie et les moyens de lutte contre la cybercriminalité de la Police Nationale

Naïké FREMIN du SARTEL, responsable communication, sous-direction de la lutte contre la cybercriminalité, Direction Centrale de la Police Judiciaire

- La stratégie et les moyens de lutte contre la cybercriminalité de la Gendarmerie Nationale

Capitaine Alban DELAUNAY, chargé de projets, Région de Gendarmerie des Pays de la Loire

- Cybersécurité : comment retrouver la confiance ?

Michel VAN DEN BERGHE, chargé de mission par le Premier ministre, CyberCampus

13h00 **Cocktail déjeunatoire**

14h30 **Ateliers**

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

Programme

Hôtel de la Région des Pays de la Loire, Nantes

RENCONTRES CYBERSÉCURITÉ PAYS DE LA LOIRE

➤ De la smart city aux **territoires intelligents** : quels enjeux de sécurité numérique pour **le développement des collectivités territoriales** (dématérialisation, réglementation, e-citoyen, mobilité...) ?
Maurice PERRION, Vice-président de la Région des Pays de la Loire, Président de la Commission territoires, ruralité, santé, environnement, transition énergétique, croissance verte et logement
Bénédicte PILLIET, Présidente, CyberCercle
Capitaine Alban DELAUNAY, chargé de projets, Région de Gendarmerie des Pays de la Loire

➤ Du tracteur connecté à la sécurité des infrastructures de l'industrie agro-alimentaire, quels enjeux de sécurité numérique et quelles solutions pour les **acteurs de la filière agricole et agro-alimentaire** ?
Lydie BERNARD, Vice-présidente de la Région des Pays de la Loire, Présidente de la Commission agriculture, agroalimentaire, forêt et pêche
Groupement de Gendarmerie du Maine-et-Loire

➤ De la sécurisation des infrastructures à l'industrie 4.0, comment insérer de la cybersécurité dans les **sites industriels** ?
Stéphane MEYNET, Président-fondateur CERTitude Numérique – senior advisor, CyberCercle
Ludovic de CARCOUET, Président, et **Pierre DEBARY**, manager SSI, Digitemis
Olivier LE TYNEVEZ, ingénieur commercial cybersécurité, Schneider Electric

➤ A l'heure de la e-santé et d'une numérisation accrue des infrastructures médicales, quels enjeux de sécurité numérique et quelles perspectives pour le **secteur de la santé** ?
Philippe LOUDENOT, Fonctionnaire de la Sécurité des Systèmes d'Information, ministères sociaux – membre du conseil d'administration du CESIN
Pierre-Antoine GOURRAUD, Professeur des universités, CHU de Nantes
Cédric CARTAU, RSSI et DPO, CHU de Nantes, GHT44
Auriane LEMESLE, référente régionale de la Sécurité des SI, GCS e-santé Pays de la Loire – secrétaire générale, APSSIS
Antoine PIAZZA, IT Infrastructure Operation Manager, EUROFINS

➤ **Innovation et cybersécurité** : enjeux et influences croisées pour les objets connectés et l'IA
Jean-Pierre LEBEE, responsable Métier SSI, DGA Maîtrise de l'Information
Mathieu MOREUX, Product Marketing Manager, Microsoft
Eric AUGE, responsable systèmes et sécurité, THALES
Lionel GILLES, consultant en sécurité offensive, SOGETI
Frédéric SERRAND, IT infrastructure Manager, EUROFINS

➤ Les enjeux de la cybersécurité dans le secteur maritime : de la terre à la mer, du civil au militaire
Jean-Marie DUMON, délégué Défense et Sécurité, GICAN
Bruno BENDER, chargé de mission cybersécurité, Comité France Maritime
Marie-Thérèse ANDRE, ingénieur cybersécurité, DGA Maîtrise de l'Information
Tanguy JACOB, Chef de service, Service Systèmes d'Information, Port de Nantes-Saint-Nazaire

➤ **Comment sensibiliser en interne** ses collaborateurs aux bonnes pratiques de la sécurité numérique ?
Jérôme MASSEAU, Directeur de la Filière Sûreté et Sécurité, implid
Nora MANSOURI, consultante manager, implid
Géraldine PERONNE, avocate à la Cour, docteur en droit, implid Legal

➤ **Démonstrations du Hacking Lab** de **FORTINET** à 13 heures et à 14 heures 40 (durée : 40mn) avec
Nicolas HERREYRE, System Engineer
Aurélien PINON, System Engineer
Alain MORAIS, Channel Systems Engineer
Ludovic PENY, System Engineer

16h30 ■›› **Retex des ateliers par les animateurs en plénière**

17h00 ■›› **Verre de clôture** dans l'espace de rencontres-démonstrations

RENCONTRES
CYBERSÉCURITÉ
PAYS DE LA LOIRE

LES INTERVENANTS

Les intervenants

Christelle MORANÇAIS

Présidente de la région des Pays de la Loire

Née le 28 janvier 1975. Elle vit au Mans avec son mari et ses 2 enfants.
De formation commerciale, elle a travaillé pendant 20 ans dans l'immobilier ; elle a débuté sa carrière en tant que négociatrice, puis responsable développement Grand Ouest pour un grand réseau immobilier.
Après s'être consacrée à sa famille et ses enfants, elle lance avec son mari sa propre société : MegAgence où elle occupait le poste de Directeur Général.
Parallèlement à son activité professionnelle, elle est élue conseillère municipale du Mans et conseillère communautaire de « Le Mans Métropole », le 30 mars 2014. Elle s'est notamment investie sur les thématiques économiques, de commerce et d'attractivité.
Tête de liste pour la Sarthe sur la liste d'union de la Droite et du Centre conduite par Bruno Retailleau, elle est élue Conseillère régionale, le 13 décembre 2015.
Elle devient Vice-présidente du Conseil régional et Présidente de la commission Emploi, apprentissage, formation professionnelle, insertion. Elle a porté le Grenelle de l'apprentissage, qui à partir d'une concertation avec tous les acteurs concernés a permis de relancer une dynamique pour cette voie d'excellence vers l'insertion professionnelle durable. La Région devient ainsi la 1ère Région de France pour l'apprentissage.
En octobre 2017, elle devient Présidente de la Région Pays de la Loire. Faisant de la lutte contre le chômage sa priorité, elle met rapidement en œuvre un Plan de Bataille pour l'Emploi permettant de faire se rencontrer les entreprises ligériennes et les demandeurs d'emploi.
Après l'abandon du projet d'aéroport du Grand Ouest à Notre-Dame-des-Landes, elle fédère l'ensemble des acteurs politiques, économiques et universitaires des Pays de la Loire afin de porter un Contrat d'Avenir visant à permettre le développement et l'attractivité de la région.
Convaincue de l'urgence à agir et de l'importance stratégique de positionner l'écologie au cœur de l'avenir des Pays de la Loire, elle a également fait adopter un plan d'actions ambitieux de 353M€ sur la transition écologique permettant de poser les bases d'une véritable croissance verte.
Elle est élue Présidente du Conseil de surveillance du Grand Port Nantes – Saint Nazaire le 22 novembre 2019. L'élection du président d'une collectivité territoriale à la tête d'un Grand Port maritime – sur le modèle de certains ports nord-européens - est une première en France.

Autres fonctions :

- Présidente de Solutions&Co, agence de développement économique de la Région
- Présidente de la Mission Val de Loire, patrimoine mondial
- Vice-présidente du parti Les Républicains (depuis octobre 2019)

Maurice PERRION

Vice-président, Région des Pays de la Loire

Voilà plus de 20 ans que Maurice Perrion s'engage dans la vie publique. Conseiller municipal de Ligné à partir de 1992, il est devenu le premier magistrat de la ville en 1995. Il a été conseiller général du canton de Ligné de 2004 à 2015 et 2e vice-président de la Communauté de communes du Pays d'Ancenis (COMPA), en charge de la commission développement et aménagement de 2008 à 2015. En 2001, l'élu est nommé Président de l'association des maires du Pays d'Ancenis puis, en 2014, de l'association des maires de Loire-Atlantique. Professionnellement, Maurice Perrion a été le gérant du bureau d'études BEP ingénierie (topographie, cartographie) qui emploie une cinquantaine de salariés. Elu aux régionales de 2015, il est nommé 7e vice-président du conseil régional des Pays de la Loire, en charge des territoires, de la ruralité, la santé, l'environnement, la transition énergétique, la croissance verte et le logement. En avril 2016, il prend la présidence de la Fédération régionale des maires des Pays de la Loire, nouvellement créée. Il devient 3e vice-président du Conseil régional en octobre 2017.

Paul JEANNETEAU

Vice-président, Région des Pays de la Loire

Docteur en pharmacie diplômé de l'Université d'Angers Paul Jeanneteau est pharmacien installé à Champigné en Maine-et-Loire. Il fait son entrée en politique en devenant maire de cette commune en 1995. Il est réélu pour un deuxième mandat en mars 2001. C'est aussi à cette date qu'il fait son entrée au conseil général de Maine-et-Loire en étant élu dans le canton de Châteauneuf-sur-Sarthe. Il en devient vice-président en 2004 jusqu'en 2015. Il est en parallèle Vice-Président de la Communauté de communes du Haut Anjou. Il préside le Comité d'Expansion Economique de Maine et Loire pendant 11 ans et la Fédération Nationale des agences de développement économique entre 2009 et 2011. Député de la 1ère circonscription de Maine et Loire entre 2007 et 2012, il siège au sein de la commission des Affaires sociales et se consacre notamment aux questions du handicap et de la dépendance. Depuis décembre 2015, il est Vice-président du Conseil régional des Pays de la Loire et Président de la commission entreprise, développement international, tourisme, innovation, enseignement supérieur et recherche.

Lydie BERNARD

Vice-présidente, Région des Pays de la Loire

Lydie BERNARD est agricultrice vendéenne à Saint-André-Treize-Voies. Elle s'est installée avec sa sœur en 1984 via le GAEC La Relance, qui compte aujourd'hui trois associés. Vice-présidente de la Région des Pays de la Loire, elle est en charge de l'agriculture, l'agroalimentaire, de la forêt et de la pêche. Elle est notamment très investie sur les dossiers de la politique agricole commune, de l'alimentation, du numérique et du développement des start-ups agricoles. Dans le monde du basket vendéen, Lydie BERNARD est aussi entraineuse du SMASH.

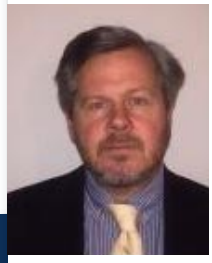
Gabriel DE BROSSES

Directeur de la Cybersécurité, GROUPE LA POSTE

Gabriel de Brosses est le Directeur de la cybersécurité du Groupe La Poste depuis le 1er novembre 2017.
Il a, auparavant, servi son pays en tant qu'officier pendant vingt-sept ans. Avant de rejoindre le Groupe La Poste il était coordinateur sectoriel ministériel au sein de l'ANSSI, où il était en charge du suivi de la sécurité des systèmes d'information des services du Premier ministre et de plusieurs ministères.
De 2013 à 2015, il a été chef de la cellule de planification des opérations cyber de l'état-major stratégique du commandement des opérations de l'OTAN, de 2011 à 2013 il a tenu les fonctions de conseiller militaire du sous-chef d'état-major en charge de la planification stratégique. Il a servi plus de vingt ans dans les transmissions de l'Armée de Terre et a été engagé en opérations en ex-Yougoslavie et en République démocratique du Congo en tant que porte-parole militaire des Nations unies.

Alexandre DE CENIVAL

Membre du réseau des référents Cybermenaces, Sous-direction à la lutte contre la cybercriminalité, DCPJ



Ingénieur de formation, Alexandre de CENIVAL démarre sa carrière dans le secteur bancaire, en gestion des risques, puis entame une reconversion et créé une entreprise d'étanchéité dans le bâtiment avant de rejoindre le réseau des référents Cybermenace de la Police nationale.

Les intervenants

Bénédicte PILLIET

Présidente fondatrice du CyberCercle

Crédit photo Alain Zimeray

Bénédicte Pilliet est depuis 2011 la Présidente fondatrice du CyberCercle, cercle de réflexion, d'expertise et d'échanges placé sous la dynamique des élus, parlementaires et locaux, qui traite des questions de confiance et de sécurité numériques, sous l'angle de la gouvernance, de la stratégie, des politiques publiques, de l'organisation et de la formation. Dans ce cadre, elle organise des événements fédérateurs réunissant l'ensemble des acteurs concernés, avec pour objectif de faire progresser les sujets de sécurité numérique en créant des cadres de confiance pour échanger expertises et expériences, favoriser le dialogue entre les organisations, entreprises, collectivités territoriales, engagées dans des process de transformation numérique et les acteurs publics et privés de la cybersécurité. Elle édite également une lettre d'information trimestrielle "Cybersécurité & Politiques Publiques".
Bénédicte Pilliet est responsable du séminaire "Politiques publiques de cybersécurité et Relations internationales" au sein du M2 "Politiques de Défense-Sécurité et Relations internationales" à l'Université de Toulouse Capitole 1, et Directeur pédagogique du Certificat Sécurité Numérique de l'Université Paris-Dauphine. Elle est chargée de cours à l'Université Catholique de Lyon et à l'Institut Léonard de Vinci. Elle est également amenée à intervenir comme experte sur les sujets de sécurité numérique au sein de nombreuses organisations, colloques, congrès et salons.
Diplômée de Sciences Po Paris en 1990, Bénédicte Pilliet bénéficie d'une expertise dans la communication institutionnelle qu'elle a exercée dans plusieurs agences de communication au profit de collectivités, d'entreprises, de groupes industriels ou d'associations professionnelles dans différents secteurs. En 2001 elle s'oriente vers les Affaires Publiques sur les questions de Défense et de Sécurité Nationale, avant de se spécialiser sur la cybersécurité à partir de 2011.

Bénédicte Pilliet est, depuis 2007, Lieutenant-colonel de réserve (Citoyenne) de 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 auprès du Coordonnateur National.
Elle est Vice-présidente de l'association Les Amis de la RCC, membre d'honneur du CefCys (Club des Femmes de la Cybersécurité), membre fondateur du Cercle K2 et membre du CESIN (Club des Experts de la sécurité de l'information et du numérique).
Bénédicte Pilliet est titulaire de la Médaille de la Défense nationale, échelon or, agrafe cyber, et de la Médaille des Services Militaires Volontaires, échelon bronze.

Philippe LOUDENOT

FSSI, Ministères sociaux

Après une carrière au sein du ministère de la défense à différents postes Philippe LOUDENOT devient responsable national de la sécurité des systèmes d'information du service de santé des armées. Puis FSSI adjoint dans le service du Haut fonctionnaire de défense et de sécurité pour les ministères chargés des affaires sociales, il rejoint les services du Premier ministre en 2011, ou il participe à la création et met en place un service du haut fonctionnaire de défense et de sécurité. Il en est nommé fonctionnaire de sécurité des systèmes d'information et conseille les autorités des services du Premier ministre, juridictions autorités administratives indépendantes en matière de cybersécurité.
Il vient de rejoindre à nouveau le service du Haut fonctionnaire de défense et de sécurité des ministères chargés des affaires sociales comme FSSI.
Chargé de cours SSI au profit de différentes universités et écoles d'Ingénieurs, Philippe LOUDENOT est également présent dans la vie associative des experts en Sécurité du Système d'Information, il est membre du conseil d'administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information et du CESIN, membre du club EBIOS.

Naïke FREMIN DU SARTEL

Responsable communication, Sous-direction de la lutte contre la cybercriminalité, Direction Centrale de la Police Judiciaire

Stéphane Meynet, ingénieur de l'École des Mines d'Alès, a démarré sa carrière dans l'industrie de la micro-électronique. Après avoir été en charge pendant 10 ans de systèmes automatisés de contrôle de procédés industriels dans un contexte opérationnel, il a rejoint l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dans un premier temps, il a conduit le projet sécurité des systèmes industriels en traitant les aspects de cybersécurité des infrastructures critiques de la nation. Puis, dans le cadre du déploiement de l'ANSSI au niveau territorial, il a été le délégué à la sécurité numérique pour la région Auvergne-Rhône-Alpes.
Il est aujourd'hui le président de CERTitude NUMERIQUE, entreprise dédiée à la sécurité numérique, et plus particulièrement appliquée aux systèmes industriels, qu'il a fondé en janvier 2018.

Jeanne BEHRE-ROBINSON

Adjointe au maire, en charge de la sécurité, Mairie d'ANGERS

Adjointe au Maire d'Angers en charge de la Sécurité et tranquillité publique Juriste publiciste Déléguée départementale de la Chambre de Métiers et de l'Artisanat – Maine et Loire Directrice régionale de la Communication et des relations publiques de la CMA Pays de la Loire

Ludovic DE CARCOUËT

Président, DIGITEMIS

Ludovic de Carcouët est ingénieur des Ponts & Chaussées et de l'Institut Mines-Télécom.
Après avoir travaillé pendant 7 années en Asie, il a fondé l'entreprise Digitemis, qui réunit des experts de haut niveau, ingénieurs en cybersécurité et juristes spécialisés dans la protection des données personnelles.
Entreprise en hyper-croissance, Digitemis a reçu 7 labels d'audit et de formation de la CNIL, est qualifiée comme prestataire de services de confiance PASSI par l'ANSSI, est lauréate du Pass French Tech, précieuse récompense reçue des mains du Premier Ministre. Depuis 2015, Digitemis est devenu le leader européen de l'audit et du pilotage de la cybersécurité des fournisseurs, grâce à sa solution innovante PERIDIAG. Développée dans le cadre des Investissements d'Avenir, elle a déjà permis l'évaluation de plus de mille PME. Digitemis apporte ainsi aux donneurs d'ordre des indicateurs de confiance, face aux enjeux de cybersécurité et de conformité, dans l'organisation étendue. Digitemis est référencé à l'UGAP depuis 2018 et travaille avec de nombreuses administrations et collectivités territoriales.

Michel VAN DEN BERGHE

Chargé de mission, CyberCampus

Michel VAN DEN BERGHE a été nommée en juillet 2019 en charge de la réflexion sur le CyberCampus français, par le premier ministre Edouard PHILIPPE. Né en 1960, diplômé de la Faculté polytechnique de Mons, Michel VAN DEN BERGHE est Directeur général d'Orange Cyberdefense depuis le 1er juillet 2014, suite au rachat par le Groupe Orange d'Atheos, dont il était le Président Fondateur depuis 2002. Il est également le fondateur des Rencontres de l'Identité, de l'Audit et du Management de la Sécurité (RIAMS).

Pierre-Antoine GOURRAUD

Professeur des universités, CHU de Nantes

Pierre-Antoine Gourraud est professeur des universités, praticien-hospitalier de la faculté de médecine de l'université de Nantes (France). C'est un ancien élève de l'école Normale Supérieure de Lyon (France) du département de biologie. Après un master de santé publique obtenu à l'université-Paris XI en 2002, il a obtenu un doctorat en épidémiologie immunogénétique et en santé publique à l'université de Toulouse-III en 2005. Il a séjourné à San Francisco de 2009 à 2016. Arrivé comme chercheur post-doctorant du département de neurologie à l'université de Californie (UCSF, Etats-Unis), il le quitte en tant que professeur associé en 2018. Auteur de plus de 130 publications, ses activités de recherche se positionnent au carrefour de l'immunologie, de la génétique et du traitement informatique des données de santé. En 2006, PA Gourraud a reçu un diplôme de premier cycle avec une spécialisation en philosophie à l'Université catholique de Toulouse qu'il a ensuite mis à profit pour contribuer à l'étude des questions de bioéthique en génétique et sous la double influence de deux de ses mentors, le docteur Anne Cambon-T homsen, ancien membre du comité national de bioéthique français et le professeur Stephen L. Hauser, membre de la commission présidentielle pour l'étude des questions de bioéthique aux USA. En 2008, il a créé Methodomics, une société française dédiée aux analyses statistiques et au développement d'algorithmes en biologie. Proche du monde entrepreneurial, il accompagne depuis plusieurs entreprises en santé et biotechnologies en leur faisant profiter de son expertise. Depuis 2015, il dirige au sein du Centre de Rechecherche en Immunologie et Transplantation (CRTI) une équipe de recherche INSERM dédiée à la composante génomique de l'autoimmunité et des transplantations où une quinzaine de chercheurs développent des algorithmes d'analyses et d'aide à la décision. Depuis avril 2018, il dirige également un service hospitalier en charge des millions de données générées par le soin au CHU de Nantes, qui en assure l'exploitation dans des conditions de sécurité de transparence et de validité propices à la recherche.

Mathieu MOREUX

Product Marketing Manager Cybersécurité, Microsoft France

Mathieu Moreux est diplômé en Economie-Finance de l'Institut d'Etudes Politiques - Sciences Po Lille et en management international de projets (MIB) de l'Université Paris-Dauphine. Après plusieurs années d'expérience chez des pure-players de la cybersécurité, successivement en tant que Chef de projet Marketing et Stratégie puis Responsable des partenariats technologiques, il est depuis 2018 Product Marketing Manager Cybersécurité chez Microsoft France.

Éric AUGE

Responsable ingénierie système et sécurité, THALES

Expert Sécurité au sein de THALES depuis 2016, Eric AUGE contribue à la qualification/certification des équipements de sécurité. Il suis issu de l'industrie des télécommunications où il a travaillé plus de vingt ans.

Olivier LE TYNEVEZ

Ingénieur commercial cybersécurité, SCHNEIDER ELECTRIC

Olivier Le Tynevez rejoint le groupe Schneider Electric en 1990. Diplômé en Génie Electrique, Il est d'abord automaticien, occupant diverses fonctions dans le développement et les services. En 2010 l'attaque Struxnet prend les industriels de court et ces derniers prennent conscience de la fragilité de leurs installations faces aux cybermenaces. A cette époque Olivier Le Tynevez est directeur de programme pour l'implantation d'un système de contrôle commande d'ampleur majeure. Il participe à la création chez Schneider d'une équipe projet pour sécuriser cette infrastructure associée. L'équipe Network Engineering et Cybersécurité – NEC -- est alors crée. Cette entité a pour vocation la sécurisation de sites industriels. Elle intervient en phase amont (audit, évaluation des risques, définition d'un PSSI industrielle, conception d'architecture), en phase réalisation (déploiement de solutions), en phase exploitation (Maintien en Conditions de Sécurité, veille de vulnérabilités) et propose également des formations. Olivier sera ensuite directeur de projet dans le département Energy Services and Sustainability de Schneider Electric. Il revient dans l'équipe NEC en 2019 pour en soutenir le développement commercial au niveau national.

Stéphane MEYNET

Président-Fondateur, CERTitude NUMERIQUE

Stéphane Meynet, ingénieur de l'École des Mines d'Alès, a démarré sa carrière dans l'industrie de la micro-électronique. Après avoir été en charge pendant 10 ans de systèmes automatisés de contrôle de procédés industriels dans un contexte opérationnel, il a rejoint l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dans un premier temps, il a conduit le projet sécurité des systèmes industriels en traitant les aspects de cybersécurité des infrastructures critiques de la nation. Puis, dans le cadre du déploiement de l'ANSSI au niveau territorial, il a été le délégué à la sécurité numérique pour la région Auvergne-Rhône-Alpes.
Il est aujourd'hui le président de CERTitude NUMERIQUE, entreprise dédiée à la sécurité numérique, et plus particulièrement appliquée aux systèmes industriels, qu'il a fondé en janvier 2018.

Les intervenants

Cédric CARTAU

RSSI, CHU de Nantes

Ingénieur de formation, Cédric CARTAU a exercé dans le privé avant de rentrer au CHU de REIMS en 1999 comme ingénieur spécialiste système et sécurité. Il a ensuite été responsable de département au CHU de RENNES entre 2004 et 2009 avant de rejoindre le CHU de NANTES en tant que Responsable Sécurité des Systèmes d'Information et Correspondant Informatique et Liberté.
Cédric Cartau est chargé de cours à l'Ecole de Hautes Etudes en Santé Publique (EHESP). Il réalise également de façon ponctuelle des audits de systèmes d'information pour le compte d'établissements publics ou privés dans différents secteurs d'activité. Il collabore régulièrement à DSIH Magazine et a publié les ouvrages suivants :

- La sécurité du système d'information des établissements de santé, Presses de l'EHESP, 2012
- Guide pratique du système d'information, Presses de l'EHESP, 2013
- Stratégies du système d'information, vers l'hôpital numérique, Presses de l'EHESP, 2014
- L'informatique d'entreprise au quotidien, Presses de l'EHESP, 2014
- L'informatique de santé, coauteur, Eyrolles, 2015

Auriane LEMESLE

Référente régionale de la Sécurité des SI, GCS e-santé Pays de la Loire

Référente régionale de la Sécurité des SI au GCS e-santé Pays de la Loire depuis 2016, Auriane Lemesle est en charge de l'animation de la sécurité numérique auprès des acteurs de santé ligériens en partenariat avec l'Agence Régionale de Santé. Elle est également Secrétaire Générale de l'APSSIS depuis 2015. Auparavant, elle a construit et animé une démarche d'amélioration de la sécurité des SI pour les établissements membres du GCS TéléSanté Centre durant quatre années. Elle est diplômée de deux Master II « Risques sanitaires dans les structures de soins et industries de produits de santé » et « Management de la SSI de Santé ». Depuis 2014, elle est enseignante pour le DU « Sécurité des SI de Santé » et pour la formation ingénieur en « Gestion des risques des secteurs de santé » à Polytech Angers.

Bruno BENDER

Coordonnateur cybersécurité maritime pour le Comité France maritime Secrétariat général de la mer (SG Mer) - Premier ministre

Bruno BENDER est un spécialiste des technologies de l'informations et de communication.
Sa carrière d'officier de marine et sa position actuelle de consultant l'ont amené à évoluer dans le domaine des systèmes de surveillance et de communication maritimes français, européens et OTAN et d'en appréhender leur protection face à la menace Cyber.
Impliqué dans la gouvernance de systèmes nationaux, européens comme EUROSUR et MARSUR ou multinationaux il dispose d'une expertise dans le domaine de l'interopérabilité, et la cybersécurité des systèmes navals.

Lionel GILLES

Consultant en sécurité offensive, SOGETI

Lionel GILLES, consultant en sécurité offensive chez Sogeti avec plus de 19 ans d'expérience dans le domaine de la sécurité a fait des systèmes IoT ainsi que des tests d'intrusion en mode Redteam ses domaines de prédilection et d'expertise. Autodidacte, doté d'un réel esprit d'analyse et critique, c'est sa réelle passion pour l'informatique qui lui a permis une fine compréhension des systèmes embarqués et notamment des couches matérielles et logicielles. Ses premières expérimentations commencèrent à la grande époque de Windows 3.11 ... Il est aujourd'hui plus connu dans le milieu de la sécurité offensive sous l'alias "topotam"

Jean-Marie DUMON

Délégué Défense et Sécurité, GICAN

Double ingénieur de formation (Ecole Navale et ENSTA Paris Tech), officier de marine dès 1984, diplômé de l'Ecole de Guerre et de l'institut des hautes études de la défense nationale, Jean-Marie Dumon a occupé de nombreux postes opérationnels, techniques et managériaux au sein de la marine nationale.
Il a participé aux opérations pendant la guerre Iran-Irak, la guerre du Golfe et le conflit afghan. Il a embarqué sur de nombreux bâtiments de guerre et commandé deux navires scientifiques pour des missions lointaines et des coopérations en matière océanographique sur plusieurs océans.
Il a dirigé des commissions gouvernementales pour des expérimentations de navires, des projets de développement d'activités portuaires civiles et d'enquêtes techniques après des accidents de mer.
Il a été conseillé stratégique de plusieurs hautes autorités du ministère de la défense pour les réformes, l'organisation, les affaires industrielles et l'innovation.
Au grade de capitaine de vaisseau, il a quitté le service de l'Etat pour rejoindre celui des organisations professionnelles. Tout d'abord au MEDEF (mouvement des entreprises de France), comme secrétaire général en charge de la liaison pour les affaires de défense, puis depuis 2018 comme délégué défense et sécurité du syndicat professionnel de l'industrie et des activités navales, le GICAN.

Alain MORAY

Channel Systems Ingineer, FORTINET

A passé 3 ans dans le métier de l'intégration réseau sécurité et téléphonie sur IP. Puis entrée à la CCI Région Île-de-France lors de la fusion de toutes les entités, en tant qu'ingénieur réseau/sécurité/chef de projet lors des déploiements sur la soixantaine de sites gérés par l'équipe. Est devenu adjoint de la responsable SI de la CCI au cours des 5 années passées, a participé à la refonte globale de la sécurité du SI ainsi que tout le réseau Wifi. Fort de cette expérience, a intégré Fortinet en 2018 au sein de l'équipe SE Channel.

RENCONTRES
CYBERSÉCURITÉ
PAYS DE LA LOIRE

NOS PARTENAIRES

CYBERCERCLE FORMATION : UN CADRE DE CONFIANCE POUR FORMER À LA SÉCURITÉ NUMÉRIQUE

Dans le prolongement de l'action qu'il mène depuis 2011 pour rendre plus appréhendables la sécurité numérique, ses enjeux, son cadre institutionnel et réglementaire, et ainsi participer à la diffusion d'**une culture de sécurité numérique**, le CyberCercle a créé des **modules de formation** qui permettent d'approfondir ces champs dans un cadre privilégié.

CyberCercleFormation aborde les sujets de cybersécurité dans toutes leurs dimensions et en particulier **stratégiques, juridiques et réglementaires, de gouvernance et organisationnels.**

CyberCercleFormation s'adresse à trois types de publics :

- les **dirigeants de PME-PMI et les cadres dirigeants non spécialistes de la cybersécurité** – directions générales, directions marketing, digital, conformité, service juridique ou ressources humaines – qui souhaitent mieux maîtriser cette nouvelle dimension indispensable aujourd'hui dans leur champ de compétences ;
- les **RSSI** et **DSI** qui désirent mieux maîtriser les **enjeux juridiques et réglementaires** liés à leurs champ d'action et responsabilités ;
- les **élus et cadres territoriaux** qui sont aujourd'hui confrontés à la transformation numérique des territoires et des usages, et qui doivent mieux appréhender la sécurité numérique pour assurer un développement pérenne de leurs actions, notamment pour garantir **la confiance dans les services numériques qu'ils mettent en œuvre au service des citoyens.**

Les modules de formation ont volontairement des **formats courts**, d'une ou de deux journées, afin d'éviter de peser trop lourdement sur les agendas.

CyberCercleFormation propose quatre modules de formations :

- **La cybersécurité au cœur de la transformation numérique des entreprises** pour les Top managers de PME/ETI, professions libérales et activités de conseil
- **La cybersécurité au cœur de la transformation numérique des collectivités** pour les élus, directions des services généraux, directions métiers
- **La cybersécurité des systèmes industriels** pour les Top managers de PME/ETI, directions générales de service de collectivités, directions métiers, acheteurs et juristes
- **Réglementation, juridique et cybersécurité** pour les risques managers, directions de la conformité, Top managers, directions des services généraux

Les formateurs de CyberCercleFormation sont tous des **professionnels** spécialistes de la cybersécurité et dotés de qualités de pédagogue qui leur permettent de transmettre leurs savoirs de façon efficiente, en adéquation avec leur auditoire. Des **représentants des institutions publiques** viennent apporter un éclairage sur des sujets définis, permettant aux participants un accès à une expertise institutionnelle et un échange personnalisé avec les représentants de l'État en charge de ces questions.

En parallèle des **sessions inter-entreprises** qui seront mises en place à partir de janvier 2019 à Paris et en région, notamment en Auvergne-Rhône-Alpes, le CyberCercle peut **définir et mettre en œuvre des formations et séminaires au sein de votre organisation**, en les adaptant aux besoins et aux profils de vos collaborateurs.

Le Conseil régional des Pays de la Loire

Découvrez comment fonctionne le Conseil régional
et comment la Région intervient dans votre quotidien.

l'esprit grand ouvert

Région
PAYS DE LA LOIRE

Votre Région, mode d'emploi

Coup de projecteur sur le fonctionnement de cette collectivité territoriale, entre gestion quotidienne et projets à long terme.

Comment ça marche ?

Instituée collectivité territoriale en 1982, la Région est l'un des trois niveaux de l'administration locale française, avec la Commune et le Département. Chacune de ces collectivités territoriales dispose de pouvoirs propres et il n'existe aucune hiérarchie entre elles.

L'assemblée régionale, ou Conseil régional, est élue au suffrage universel direct, selon un mode de scrutin proportionnel à deux tours. Depuis 2004, les listes sont régionales et une prime de 25 % des sièges est accordée à celle qui l'emporte.

Le Conseil régional est élu au suffrage universel

CHIFFRES clés

93 conseillers régionaux

1 présidente

15 vice-présidents

3 358 agents régionaux,

dont **2 363** dans les lycées.

1 présidente et 15 vice-présidents

L'autorité exécutive de la Région est le président du Conseil régional

Le président est élu à la majorité absolue des membres du Conseil régional. Il dirige les débats de l'assemblée, prépare les délibérations et engage leur exécution, ordonne les dépenses et prescrit les recettes, gère le patrimoine de la collectivité et dirige les services.

93 conseillers régionaux

Le Conseil régional est l'assemblée délibérative de la Région

Il est composé, en Pays de la Loire, de 93 conseillers régionaux.
En séance plénière, avec l'ensemble de l'assemblée, le Conseil régional vote le budget, règle les affaires de la Région, autorise les emprunts, élabore les actions et projets régionaux, adopte le Contrat de plan Etat-Région...

31 membres

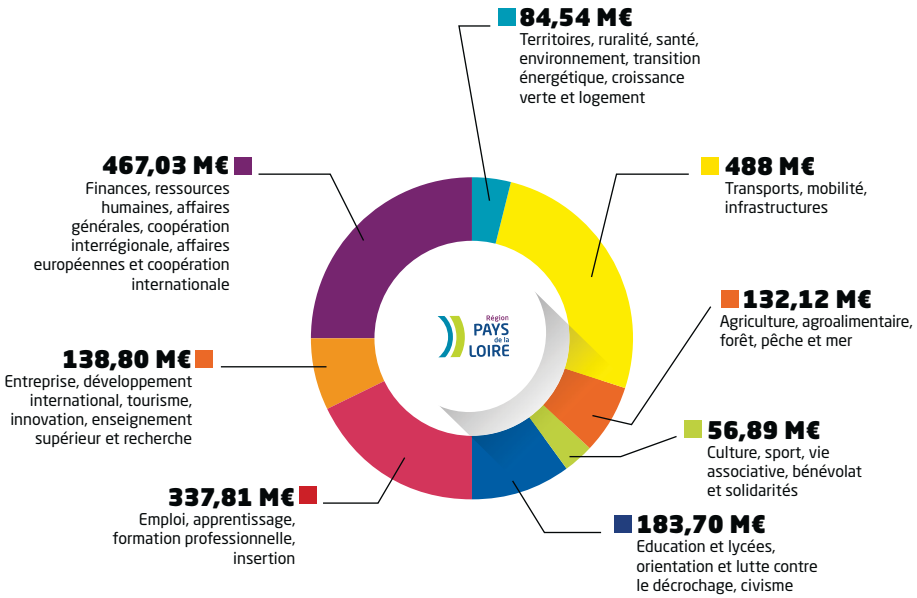
La Commission permanente, «gouvernement» de la Région

Pour gérer le quotidien, le Conseil régional élit parmi ses membres une Commission permanente, composée du président, de 15 vice-présidents et de 15 autres membres représentatifs des tendances politiques.
Cette Commission permanente peut être assimilée au gouvernement de la Région : elle assure la continuité des actions, se réunit chaque mois, en s'aidant des avis des 8 commissions sectorielles (voir ci-contre).

Budget régional 2019

1 888,9 millions d'euros

répartition des dépenses



Le Ceser : un laboratoire d'idées

Le Conseil économique social environnemental régional (Ceser) est une assemblée consultative, composée de 119 membres qui représentent les principales activités économiques et sociales de la région. Il émet des avis, diagnostics et préconisations d'action. Le Ceser est obligatoirement consulté pour certains dossiers (planification stratégique, budget...). Il peut choisir de conduire certaines études, ou être saisi par le président du Conseil régional..

1 directeur général des services

Les services du Conseil régional

La politique définie par l'assemblée régionale est mise en œuvre par l'administration régionale. Les services du Conseil régional sont chargés de préparer les dossiers avant les débats, puis d'appliquer les décisions des élus. En Pays de la Loire, on compte plus de 3 000 agents régionaux, dont la plupart travaillent dans les lycées. Ces agents sont sous la responsabilité d'un directeur général des services.

995 agents au siège et dans les antennes régionales

2 363 agents régionaux des lycées

Des agents sur le territoire

Le siège du Conseil régional est à l'Hôtel de Région de Nantes, où travaillent 861 agents permanents. Les 2 363 agents régionaux des lycées, répartis dans les 109 lycées publics ligériens, sont les plus nombreux des agents régionaux.

Ce que fait la Région des Pays de la Loire

Développement économique

La Région accompagne les entreprises, quelle que soit leur taille (TPE, PME, ETI) et quelle que soit l'étape de leur développement (création, innovation, recherche, export…), avec un outil de financement simplifié : le Contrat de Croissance Entreprise. Elle accompagne les TPE pour le maintien et le développement du commerce et de l'artisanat sur tous les territoires.

Agriculture et agroalimentaire

La Région préserve et appuie le développement des activités et des emplois agricoles, aide les jeunes agriculteurs à s'installer, accompagne une gestion durable du territoire, agit pour la biodiversité et soutient la filière agroalimentaire.

Relations internationales

Outre l'accompagnement des entreprises à l'export, la Région facilite la mise en réseau des acteurs économiques et mobilise les financements européens pour une action plus utile et en proximité sur les territoires.

Emploi et formation

La Région agit aux côtés des demandeurs d'emploi, en finançant les formations professionnelles et des services (mobilité, logement…) au plus près des territoires, et aux côtés des entreprises pour les accompagner dans leurs besoins en recrutement.

Education, jeunesse et orientation

La Région prépare l'avenir et crée les conditions de la réussite de tous les jeunes Ligériens : rénovation et construction durable de nouveaux établissements, actions éducatives au sein des lycées et des CFA, lutte contre le décrochage scolaire, valorisation de l'apprentissage…Tous les parcours de réussite sont mobilisés.

Transports et mobilités

En charge des trains régionaux TER, des cars interrégionaux et, depuis 2017, des cars scolaires, interurbains, du transport à la demande et de la ligne maritime Yeu-Continent, la Région s'est fixé comme objectif d'augmenter l'offre de transport, de renforcer la qualité de service et l'accessibilité des transports régionaux (infrastructures et tarifs).

Territoires et ruralité

La Région apporte des solutions adaptées à tous les territoires, qu'ils soient ruraux, péri-urbains ou urbains. Elle soutient les projets d'aménagement des communes et intercommunalités (services de santé, très haut débit, maintien de commerce) et renforce les réseaux de communication (routes, fer, numérique) pour contribuer à leur attractivité.

Culture, sport, vie associative et bénévolat

La Région propose, dans tous les territoires, une offre culturelle diversifiée et riche, encourage les coopérations artistiques inédites et innovantes, met en avant les valeurs du sport pour tous en soutenant les pratiques et événements d'envergure. Elle agit également aux côtés des associations et encourage le bénévolat.

Transition écologique

La Région favorise une transition écologique positive, qui conjugue la préservation du cadre de vie, de la biodiversité et du patrimoine naturel avec le développement du territoire et des emplois. Cela passe notamment par le développement de la production d'énergie renouvelable, la mobilité durable et la reconquête de la qualité de l'eau.

Retrouvez en détails l'action de la Région pour votre quotidien sur www.paysdelaloire.fr

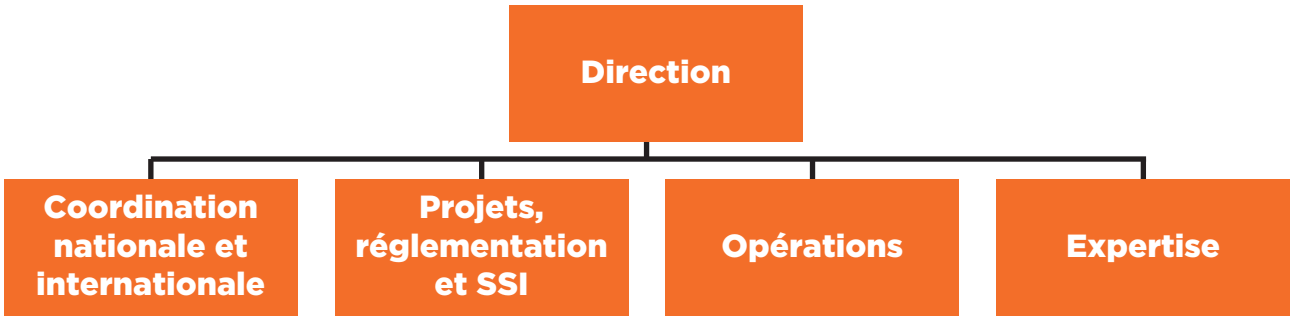
Région PAYS DE LA LOIRE

Région des Pays de la Loire. Mai 2019. Hôtel de la Région, 1 rue de la Loire 44966 Nantes cedex 9 Tél. 02 28 20 50 00 • www.paysdelaloire.fr • Illustrations : RC2C

DIRECTION CYBERSÉCURITÉ GROUPE

LE GROUPE LA POSTE

Organisation de la direction de la cybersécurité du Groupe



La direction de la cybersécurité du Groupe (DCG) a été créée au 1er janvier 2018. Sa création s'inscrivait dans le cadre du projet « Servir le développement » (SLD) qui regroupe les fonctions support du Groupe au Niveau du siège (CORPORATE). Cette structure devait être complètement opérationnelle en septembre 2019 (CA du 7 mars 2018).

La direction de la DCG :

Outre les attributions classiques de direction, elle assure également les missions d'expertise judiciaire au profit du Groupe et de coordination avec les services de sécurité de l'état. Dans l'éventualité de la judiciarisation d'une affaire, elle dirige alors directement les actions des spécialistes du SLCC ou fait appel à des experts indépendants.

Coordination nationale et internationale :

Le coordinateur relations nationales et internationales est en charge du suivi des dossiers impliquant les directions internes chargés de la représentation du Groupe dans les instances internationales (POSTEUROP, Union Postale Universelle, l'Agence Européenne chargée de la sécurité des réseaux et de l'information...) et du suivi des relations avec les instances nationales compétentes en matière de cybersécurité (Ministère de tutelle, l'Agence Nationale de la Sécurité des Systèmes d'Information ...).

Projets, règlementation et sécurité des systèmes d'information (SSI) :

Le pôle est la structure d'intégration et de coordination de la sécurité des systèmes d'information dans les projets du Groupe. Il a pour objet de coordonner les travaux de déclinaison des règlementations de cybersécurité nationales et internationales applicables au Groupe La Poste.

Opérations :

Ce pôle est la structure de management de la composante opérationnelle de la cybersécurité du Groupe La Poste et doit orienter et contrôler l'efficacité des fonctions SOC/CERT opérées par le SLCC et des composantes de cybersécurité opérationnelles des branches et filiales.

Expertise :

Ce pôle est la structure d'expertise technique et organisationnelle, capable d'accompagner les acteurs stratégiques de la transition numérique du Groupe. Il assiste les maîtrises d'ouvrage dans le choix de leurs solutions de sécurité. Il est en charge de la veille technologique et du suivi de l'intégration de la sécurité dans les projets des Systèmes d'Information transverses du Groupe.

La stratégie de Microsoft est d'assurer la sécurité de nos clients pour permettre leur transformation numérique grâce à une plateforme complète, des renseignements uniques sur les menaces et de larges partenariats.

Au-delà d'une protection périmétrique devenue obsolète, il faut présupposer qu'il y aura compromission et être en mesure de détecter les attaques et y remédier avant que celles-ci n'impactent sévèrement vos données et vos systèmes. C'est la raison pour laquelle, l'approche traditionnelle de protection du Système d'Information doit être complétée et s'appuyer, comme nous le préconisons, sur trois piliers : la **Protection**, de tous les points terminaux jusqu'aux centres de données ; la **Détection**, en utilisant des signaux ciblés, l'analyse comportementale et l'apprentissage statistique ; la **Réponse**, pour passer rapidement de la découverte à l'action.

La complexité est l'ennemi absolu de la sécurité : Microsoft intègre nativement dans l'ensemble de ses services des fonctionnalités de sécurité avancées qui protègent de bout en bout les identités, la messagerie, les appareils, les infrastructures et les données, le tout sans compromettre l'expérience utilisateur pour éviter toute stratégie de contournement de vos politiques de sécurité. Ce positionnement unique vous permet de faciliter la gestion, l'administration et la supervision de la sécurité de votre SI tout en renforçant votre posture de sécurité. Ainsi, en février 2019, Microsoft a annoncé le lancement d'Azure Sentinel, une solution de SIEM/SOAR nativement conçue dans et pour le cloud. Cette solution vient compléter les capacités de détection et réponse automatisée de la plateforme de sécurité intégrée de Microsoft.

Ainsi, la protection de nos plateformes prend en compte la **protection et la gestion des identités** avec comme point central le référentiel Azure Active Directory ; la **protection de l'information** qui s'appuie sur Azure Information Protection pour classifier et protéger les données les plus sensibles et assurer le partage sécurisé à l'intérieur et à l'extérieur de l'entreprise ainsi que sur notre solution de CASB Microsoft Cloud App Security pour encadrer le shadow IT ; et enfin la **protection contre les menaces avancées** grâce à la puissance du Cloud et de l'intelligence Artificielle aussi bien sur les environnements collaboratifs Office 365, les appareils et serveurs que les identités. Enfin, nos solutions d'**accès conditionnel** vous assurent une tranquillité d'esprit en bloquant l'accès à l'information confidentielle en dernier ressort, lorsqu'une identité ou un appareil sont compromis.

Nourris par nos 250 services cloud, le **Microsoft Intelligent Security Graph** consolide et analyse des signaux en provenance de plus d'un milliard de systèmes Windows, de 450 milliards d'authentifications mensuelles sur nos services Cloud, aux plus de 18 milliards de page Web qui sont parcourues en permanence par Bing et aux 200 milliards de mails que nous filtrons contre le Spam chaque mois. Cette intelligence est présente dans toutes nos solutions de sécurité grâce à des algorithmes de Machine Learning et d'analyse des anomalies ou des comportements basés sur la puissance du cloud Microsoft et permet d'appliquer des mesures préventives ou des mesures d'atténuation en quasi temps réel pour contrer les cyber menaces.

Tous les services Microsoft sont fondés sur des principes forts en matière de vie privée, de sécurité, de conformité et de transparence. Microsoft est le chef de file de l'industrie en matière de vie privée et de sécurité et c'est à ce titre que nous avons fondé l'**Intelligent Security Association** en 2017 qui réunit les pionniers de l'industrie de la cybersécurité.

Enfin, parce que la sécurité des objets connectés est l'un des grands défis à venir, Microsoft innove avec **Azure Sphere**, une solution 3-en-1 qui sécurise l'IoT du matériel jusqu'au cloud en passant par un système d'exploitation sécurisé dédié.

Retrouvez plus d'informations relatives à la sécurité & à la conformité sur https://aka.ms/MicrosoftSecurity2019

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

NOS CONSEILS POUR VOTRE SÉCURITÉ NUMÉRIQUE

ADOPTER LES BONNES PRATIQUES

LES MOTS DE PASSE

Votre mot de passe doit être différent pour chaque service, suffisamment long et complexe, et impossible à deviner. Ne le communiquez jamais à un tiers. Pour votre messagerie, il doit être particulièrement robuste.

LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

Protégez l'accès à vos comptes, vérifiez vos paramètres de confidentialité et maîtrisez vos publications. Faites attention à qui vous parlez. Vérifiez régulièrement les connexions à votre compte.

LA SÉCURITÉ DES APPAREILS MOBILES

Mettez en place les codes d'accès. Appliquez les mises à jour de sécurité et faites des sauvegardes, évitez les réseaux Wi-Fi publics ou inconnus. Ne laissez pas votre appareil sans surveillance.

LES SAUVEGARDES

Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.

LES MISES À JOUR

Mettez à jour sans tarder l'ensemble de vos appareils et logiciels. Téléchargez les mises à jour uniquement depuis les sites officiels et activez l'option de téléchargement et d'installation automatique des mises à jour.

LES USAGES PRO-PERSO

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez. Ne mélangez pas votre messagerie professionnelle et personnelle et n'utilisez pas de service de stockage en ligne personnel à des fins professionnelles.

RETROUVEZ L'ENSEMBLE DES CONSEILS SUR CES THEMATIQUES DANS NOS FICHES PRATIQUES

COMPRENDRE LES RISQUES ET RÉAGIR

L'HAMEÇONNAGE

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

LES RANÇONGICIELS

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT

Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants

TECHNIQUE

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).

COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

En partenariat avec l'Agence nationale de la sécurité des systèmes d'information

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR :
www.cybermalveillance.gouv.fr

Avec la participation des membres du dispositif :

ISEN
ALL IS DIGITAL!
OUEST

yncréa

ISEN Yncréa Ouest

Devenez ingénieur en 5 ans après le baccalauréat

Vous voulez devenir ingénieur ? Participer aux transformations numériques et à la transition énergétique ? À l'ISEN Yncréa, vous choisissez votre cursus post-bac parmi six cycles thématiques avant de vous orienter au choix vers les 18 domaines professionnels proposés sur les sites de Brest et de Nantes.

L'école est un Établissement d'Enseignement Supérieur Privé d'Intérêt Général labellisé par l'État. Il forme 1000 élèves ingénieurs dans le Grand Ouest.

3 ans pour choisir...

Après une inscription sur ParcourSup.fr et la réussite au Concours Puissance-Alpha.fr, chaque étudiant intègre l'un des 6 cycles post-bac de son choix.

- Généraliste
- Informatique et Réseaux
- Biologie, Sciences et Technologies
- Économie numérique et Technologies
- Environnement, Sciences et Technologies
- Biologie, Agronomie, Sciences et Technologies

... 2 ans pour se spécialiser

À l'issue de ces 3 ans, chaque étudiant a mûri son projet professionnel et peut choisir parmi les 18 domaines professionnels proposés dans le Grand Ouest, voire l'un des 40 domaines professionnels proposés dans les établissements Yncréa.

- Technologies Médicales et de Santé
- Numérique, Environnement et Développement Durable
- Cyber-Sécurité
- Intelligence Artificielle
- Cloud
- Big Data
- Développement Logiciel
- Robotique - Drones
- Robotique - Usine du Futur
- Énergie
- Mobilité électrique
- Systèmes embarqués
- Internet des Objets
- Marine Technologies (cursus international)
- Ingénierie de projets et d'affaires
- Agriculture et Numérique
- Finance
- Double-Diplôme Business School

Schneider Electric

Life Is On Schneider Electric

Conseil, Expertise et Solutions en cybersécurité industrielle

vous aider à optimiser votre rentabilité tout en protégeant vos systèmes des cyber attaques

Data centers

Industrie

Bâtiments

Infrastructures

GICAN

Défendre

- les intérêts de l'industrie maritime française

Promouvoir

- l'expertise technologique et industrielle maritime française

Soutenir

- le développement harmonieux et la compétitivité de la filière

L'industrie Navale

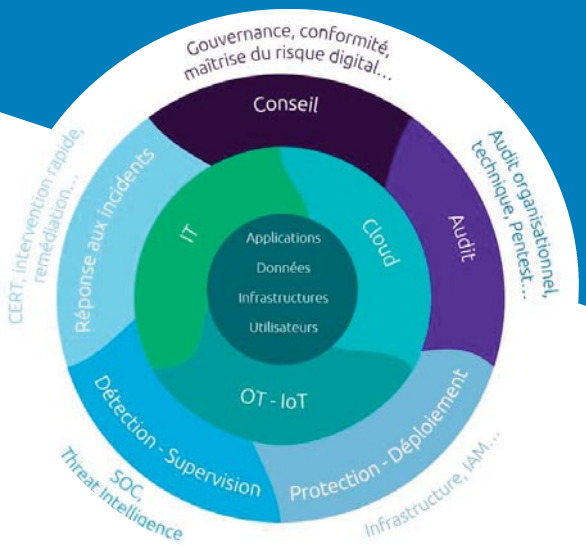
en mouvement !

www.gican.asso.fr

Des services cybersécurité de bout en bout

Protégez tous les aspects critiques de votre identité digitale : utilisateurs, applications, terminaux et infrastructure des cyberattaques et des utilisations internes malveillantes.

Sogeti vous propose des services de sécurité de bout en bout intégrant conseil, audit, protection/déploiement, surveillance et réponse sur incident pour répondre aux enjeux sécurité de votre entreprise.



Notre engagement Qualité

- **Offre éprouvée** s'appuyant sur le retour d'expérience de nos experts sécurité SOC, MSSP
- **Évaluation** de la qualité de nos prestations
- **150+** consultants multi-certifiés : CISSP, ISO 27001, ISO 27005, CISM, OSCP…
- Formateurs agréé LSTI

PASSI RGS – PASSI LPM

Prestataire de Confiance pour les Audits de Sécurité - depuis 2013 et 2017

SOC PDIS

Prestataire de Détection d'Incidents de Sécurité

PRIS *en cours*

Prestataire de Réponse aux Incidents de Sécurité

Notre engagement Proximité

7 Sites Sogeti ESEC et **500+** consultants et experts ● SOC français 365/7/24 ● 2 SOC mutualisés et SOC sur site client ● CERT français ● Réponse à incident sous 24h en France et 72h à l'international


DevSecOps & Sécurité Applicative


Conformité LPM NIS RGS


Identity & Access Management


Sécurité du Cloud


CERT & réponse aux incidents


SIEM, SOC, Threat intelligence


Gouvernance RGPD / GDPR

POLICE NATIONALE

LE RÉSEAU DES RÉFÉRENTS CYBERMENACES

RCM POLICE NATIONALE DCPJ • RÉFÉRENT CYBER MENACE

Expérimentation depuis mars 2018 au sein des zones Est, Sud-Ouest et Ouest
Généralisation progressive du dispositif à l'ensemble du territoire national

UN CONSTAT

- 80% des entreprises ont constaté au moins une cyberattaque au cours de l'année, en France (Baromètre du CESIN).
- Coût moyen d'une cyberattaque : environ 10 000 € pour les TPE mais dépasse les 100 000 € dans 6% des cas (Rapport Euler Hermès).
- La cybersécurité est aujourd'hui une préoccupation pour 76% des PME (Source : IFOP).
- 71 % des entreprises de 0 à 9 salariés et 85 % des entreprises de 10 à 49 salariés sensibilisent leurs collaborateurs aux risques informatiques, dont 44 % au moins tous les ans (Rapport Francenum / CPME).

4 AXES OPÉRATIONNELS STRATÉGIQUES

AXE 1 Une équipe innovante de référents associant des commissaires de police des DIPJ, des réservistes de la Police nationale issus du secteur privé et des partenaires privés.

AXE 2 Un maillage territorial de la Police nationale permettant la coordination de la lutte contre la cybercriminalité.

AXE 3 Des actions de sensibilisation et de prévention auprès des entreprises pour protéger le tissu économique local.

AXE 4 Une montée en puissance de la collaboration du réseau de la Police nationale et des acteurs du secteur privé, permettant la diffusion de bonnes pratiques, d'alertes préventives, ainsi que la réactivité des services, grâce à une fluidité de la communication fondée sur la confiance.

LA MISE EN ŒUVRE DU RÉSEAU

Par qui ?

Le réseau est constitué :

- Du RÉFÉRENT CYBERMENACES , commissaire de police de la DIPJ/DRPJ.
- D'un réserviste de la Police nationale issu du monde de l'entreprise : chef d'entreprise, cadre salarié, responsable de la sécurité des systèmes d'information.
- Des partenaires privés (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…

Pour qui ?

Le réseau s'adresse principalement :

- à l'ensemble des directions de la Police nationale présentes sur le territoire ;
- aux entreprises qui participent au tissu économique local.

Direction Centrale de la Police Judiciaire
Sous-Direction de la Lutte contre la Cybercriminalité
101, rue des Trois Fontanot - 92000 NANTERRE

THALES

QUI SOMMES-NOUS ?

Ceux qui font avancer le monde s'appuient sur Thales.

Dans un monde en constante mutation, à la fois imprévisible et riche d'opportunités, nous sommes aux côtés de ceux qui ont de grandes ambitions : rendre le monde meilleur et plus sûr.

Riches de la diversité de leurs expertises, de leur talents, de leurs cultures, nos équipes d'architectes conçoivent un éventail unique de solutions technologiques exceptionnelles, qui font de demain la réalité d'aujourd'hui.

Du fond des océans aux profondeurs du cosmos ou du cyberespace, nous aidons nos clients à maitriser des environnements toujours plus complexes pour prendre des décisions rapides, efficaces, à chaque moment décisif.

Nous fournissons des services, des systèmes et des produits pour l'informatique ainsi que des solutions globales faisant face aux ruptures technologiques et aux cyber menaces. Au sein de l'activité Systèmes d'information et de communication sécurisés, nos équipes développent également des produits et solutions de radiocommunications des armées et de communications par satellite.

MESSAGE AUX ETUDIANTS

Avec plus de 80 000 collaborateurs, Thales est un groupe mondial qui opère dans 68 pays. Pour soutenir son développement, Thales compte sur ses nouvelles recrues, jeunes diplômés, personnes plus expérimentées, de tous niveaux et tous horizons, mais mus par les mêmes ambitions : mettre au service de l'entreprise motivation, compétences et dynamisme... Pour 2019, nous prévoyons de recruter 2 500 personnes en France, et chaque année plus de 2000 stagiaires et 1800 alternants en France rejoignent nos équipes ! Alors pourquoi pas vous ?! Rendez-vous vite sur notre stand pour rencontrer nos équipes !

Thales recrute 70% d'ingénieurs et cadres, principalement dans 4 familles professionnelles :

- R&D dans les métiers de l'ingénierie logiciel, matériel et systèmes : postes de développeur IHM, développeur web, hacker éthiques, architecte systèmes...
- Industrie : ingénieur hyperfréquences, ingénieur en électronique, opérateur en électronique, supply chain
- Service client pour maintenir les systèmes et plateformes livrés ainsi que la documentation correspondante : technicien réparation, soutien logistique intégré
- Management d'offres et de projets : responsable d'offre, responsable d'appel d'offre

CONTACT

Adresse postale :
Thales SA – Tour Carpe Diem – 31, place des Corolles CS 2001, 92098 Paris La Défense Cedex
Mail : forum.opportunites@thalesgroup.com
Site carrières : www.thalesgroup.com/

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention du risque numérique

VICTIME D'ACTES MALVEILLANTS SUR INTERNET ?

PIRATAGE

ARNAQUE

VIRUS

1

ASSISTANCE AUX VICTIMES
D'ACTES DE CYBERMALVEILLANCE

2

INFORMATION ET SENSIBILISATION
SUR LA SÉCURITÉ NUMÉRIQUE

3

OBSERVATION ET ANTICIPATION
DU RISQUE NUMÉRIQUE

RENDEZ-VOUS SUR
WWW.CYBERMALVEILLANCE.GOUV.FR

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

avec

MINISTÈRE DE LA JUSTICE
MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES
MINISTÈRE DE L'INTÉRIEUR
SECRÉTARIAT D'ÉTAT CHARGÉ DU NUMÉRIQUE

DIGITEMIS
CYBERSECURITY & PRIVACY

CYBERSÉCURITÉ

- État des lieux, tests d'intrusion
- Audits : architecture, configuration, code, …
- Conformité ISO 27001, RGS, LPM…
- Analyse des risques et politique de sécurité
- Plan de continuité (PCA/PRA)
- Externalisation fonction RSSI
- Externalisation RSSI

PROTECTION DES DONNÉES PERSONNELLES

- Audit de conformité CNIL
- Mise en conformité avec le RGPD
- PIA (Analyse d'Impact sur la Vie Privée)
- Externalisation du DPO (Délégué à la Protection des Données)
- Audit de conformité des sites web
- Cartographie des traitements

FORMATIONS ET SENSIBILISATION

- Tests de malveillance : Phishing, intrusions, fraude…
- Sensibilisation des utilisateurs et des dirigeants
- Coaching et formation de RSSI et de DPD
- Formations labellisées CNIL

PILOTAGE DES FOURNISSEURS

DIGITEMIS s'est spécialisée dans l'évaluation et le pilotage de la Cybersécurité des fournisseurs. Nous proposons des solutions adaptées à toutes les organisations, désireuses de piloter de manière simple, rapide et complète la performance de leurs fournisseurs.

NOS LOGICIELS INNOVANTS

PERIDIAG

- Solution d'évaluation et de pilotage de la Cybersécurité des fournisseurs et filiales.

BOOKMYDATA

- Solution de gestion de conformité pour la gestion des données personnelles.

LABEL CNIL GOUVERNANCE RGPD — GOUVERNANCE N°2018-242 EXPIRE : 24/05/2021

PASS FRENCH TECH — Accompagner l'hyper-croissance

UGAP

Contact : Sophie Quinchard
communication
squinchard@esaip.org
06 16 71 31 64

L'esaip, école d'ingénieurs à Angers et Aix-en-Provence

L'**e**saip, Grande École d'ingénieurs reconnue par la Commission des Titres d'Ingénieur (CTI) et membre de la CGE (Conférence des Grandes Écoles) est labelisée EESPIG (Établissement d'Enseignement Supérieur Privé d'Intérêt Général).
L'**e**saip propose un parcours de formation en 5 ans sur 2 spécialités :

- Numérique
- Sécurité, Environnement et Prévention des risques

La volonté de l'esaip est de former des hommes et des femmes responsables, engagés, tous différents, agiles dans un contexte global et multiculturel grâce à de fortes capacités d'adaptation et grâce à des compétences opérationnelles.

L'esaip, école historique de la cybersécurité et du hacking éthique

L'**e**saip, propose une majeure cybersécurité dans sa spécialité numérique. Les élèves sont formés à la prévention, aux tests d'intrusions, aux protocoles de défense et aux attaques éthiques afin de contrer les hackers.

L'esaip est labelisée SecNumEdu, Label délivré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), mettant en avant l'expertise et l'implication de l'école en matière de cybersécurité.

L'esaip organise chaque année 2 évènements dédiés à la cybersécurité :

CTF ESAIP HACK CHALLENGE

Le CTF ESAIP HACK CHALLENGE est un hackathon relatif au monde de la sécurité informatique.
Il s'agit pour les challengers de résoudre des épreuves contenant des failles volontaires et de retrouver des informations/données, appelées «flags», qui sont placées sur les serveurs de manière chiffrée, cachées ou à des endroits difficiles d'accès.
Il est ouvert à tous et rassemble des équipes d'étudiants de différentes écoles et des professionnels.

L'édition 2020 se déroulera en Mars, à Angers.

INTERNATIONAL SYMPOSIUM CYBERSECURITY & IOT

Le rendez-vous Cybersécurité & IoT, avec des experts nationaux et internationaux, à ne pas manquer !
L'édition 2020 se déroulera en Mai, à Angers.
Objectifs :

- Réunir des experts internationaux dans le domaine de la cybersécurité et de l'internet des objets et présenter les enjeux aux entreprises, étudiants et au grand public
- Approfondir la recherche et mettre en avant le « Ethical Hacking »
- Guider les entreprises dans les domaines de la cybersécurité et de l'IoT
- Partager les bonnes pratiques

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

UNE GRANDE ÉCOLE D'INGÉNIEURS GÉNÉRALISTES RECONNUE INTERNATIONALEMENT

UNE RECHERCHE D'EXCELLENCE POUR LA SÉCURITÉ DES SYSTÈMES COMPLEXES, DE L'INDUSTRIE DU FUTUR ET DES INFRASTRUCTURES CRITIQUES

IMT Atlantique est une grande école d'ingénieurs généralistes (parmi les 400 premières universités du monde du THE World University Ranking 2020 - 59e université mondiale de moins de 50 ans -, reconnue internationalement pour sa recherche (présente dans 4 disciplines des classements de Shanghaï, de QS et de THE). Elle est membre de l'Institut Mines-Télécom et dépend du ministère en charge de l'industrie et du numérique.

Forte de ses 3 campus (Brest, Nantes, Rennes) d'un incubateur présent sur les 3 campus, et d'un site à Toulouse, IMT Atlantique a pour ambition de conjuguer le numérique, l'énergie et l'environnement pour transformer la société et l'industrie par la formation, la recherche et l'innovation et d'être, à l'international, l'établissement d'enseignement supérieur et de recherche français de référence dans ce domaine.

L'Ecole propose une formation d'ingénieurs généralistes (recrutement sur le concours Mines-Ponts) et délivre 2 diplômes d'ingénieur par la voie de l'apprentissage (un 3ème parcours ouvrira à la rentrée 2020), des diplômes de masters, mastères spécialisés et doctorats.

Les formations d'IMT Atlantique s'appuient sur une recherche de pointe, au sein de 6 unités mixtes de recherche (avec le CNRS, l'INRIA, l'INSERM, des universités ou écoles d'ingénieur), dont elle est tutelle : GEPEA, IRISA, LATIM, LABSTICC, LS2N et SUBATECH. L'école s'appuie sur son excellence en recherche dans ses domaines phares (énergie et numérique, cybersécurité, environnement et numérique, industrie du futur, nucléaire, santé et numérique, risques et interactions) et en couplant les domaines scientifiques pour répondre aux défis de demain : transition numérique, transition environnementale, transition industrielle, transition énergétique, santé du futur et recherche fondamentale.

L'expertise Cyber D'IMT ATLANTIQUE

Thématiques de recherche

Protection, défense et résilience des systèmes complexes organisées autour de 4 challenges scientifiques :

> Analyse : techniques d'analyse avancées pour la détection d'intrusion (détection du jour zéro)
> Métrique : métriques de sécurité pour l'analyse des risques de sécurité
> Atténuation : réponse aux attaques multiples et coordonnées
> Gestion des données : traçabilité et anonymisation des données pour la cybersécurité

Deux chaires industrielles de recherche et d'enseignement

> **Cybersécurité des infrastructures critiques**
> **Cyberdéfense des systèmes navals**

La dualité civile et militaire de ces 2 chaires permet aussi de travailler étroitement avec les agences gouvernementales. Ces chaires contribuent au rayonnement du Pôle d'excellence Cyber, signé entre l'Etat, la région Bretagne et différents acteurs de la recherche publique en cyber sécurité, dont IMT Atlantique.

De jeunes entreprises en cybersécurité dans l'incubateur d'IMT Atlantique

De jeunes entreprises en cybersécurité sont hébergées dans l'incubateur d'IMT Atlantique, parmi lesquelles Yagann (Analyse de vulnérabilité de code source), AnozWay (Intelligence Artificielle en cybersécurité) ou encore tout récemment Acert.io (Monitoring et analyse des risques sur les devices en entreprise) et Obviews (Plateforme d'analyse des risques numériques via un RSSI virtuel).

Deux mastères spécialisés (labellisés SecNumEdu par l'ANSSI)

> **Mastère spécialisé Cybersécurité**
> **Mastère spécialisé Sécurité des systèmes maritimes et portuaires**

Une thématique d'approfondissement en formation initiale

Accessible en 2ème ou 3ème année de la formation d'ingénieur généraliste d'IMT Atlantique, la thématique d'approfondissement « Cybersécurité » forme des ingénieurs en sécurité des réseaux et des systèmes industriels. Elle intègre des enseignements spécialisés en architecture des systèmes, cybersécurité du web et des bases de données, cybersécurité des objets connectés, et protection des données.

Conception et réalisation : Direction de la communication IMT Atlantique - Décembre 2019

Un ancrage territorial commun

- **Un enracinement au cœur des territoires :** comme une réponse aux attentes de la population exprimées à l'occasion du Grand Débat, spécialement l'accessibilité du service public, la gendarmerie partage avec les élus locaux, au premier rang les maires, une présence dans tous les territoires.
- **Un maillage** permettant à la gendarmerie de décliner pleinement ses 4 fonctions socles :
  - **le contact** avec la population et les élus,
  - **la prévention** par des actions directes ou en lien avec les partenaires,
  - **l'intervention** d'initiative ou à la demande des usagers,
  - **l'investigation**, quand la prévention n'a pu éviter le crime ou le délit.
- **Une offre territoriale de sécurité adaptée** et favorisant le dialogue avec toutes les populations, l'intervention en tout point du territoire dans des délais contraints, la compréhension des tissus économiques et sociaux.

La gendarmerie au contact

- Une **sécurité du quotidien** adaptée aux spécificités de chaque territoire dans une démarche partenariale avec les élus, et notamment les maires qui sont en charge d'assurer le bon ordre, la sûreté, la sécurité et la salubrité publiques dans leurs communes.
- Du **sur-mesure territorial** laissant la place aux initiatives et à de nombreuses expérimentations (groupes de contact, brigade de gestion des événements, extension du dispositif de participation citoyenne aux commerçants...).
- La priorité à la **proximité** : présence visible des gendarmes sur le terrain pour resserrer les liens entre la gendarmerie, la population et les élus. La gendarmerie assure la sécurité de vos administrés mais elle garantit également votre propre intégrité physique, votre qualité d'élu supposant une attention particulière.

Des initiatives et des actions communes

- Des contacts réguliers gendarmerie – élus permettent de créer des **relations de confiance** et favorisent l'**échange réciproque d'informations** :
  - de la gendarmerie vers les maires, ceux-ci devant être tenus informés des événements causant des troubles à l'ordre public sur le territoire de leurs communes,
  - des maires vers la gendarmerie, les élus étant des capteurs locaux privilégiés à l'écoute des attentes de la population.
- Des dispositifs de **participation citoyenne**, placés sous l'égide des maires et encadrés par la signature d'un protocole, visant à sensibiliser les référents citoyens aux postures de vigilance, aux gestes de prévention, aux réflexes à développer pour relayer le renseignement.
- Des **intervenants sociaux de la gendarmerie** (ISG) qui appuient l'action de la gendarmerie en prenant en compte le volet social des sollicitations et dans lequel les élus jouent un rôle essentiel en les employant.





- **3073 brigades** en métropole et outre-mer
- Une intervention toutes les **15 secondes**
- **33 800 communes** en zone de gendarmerie
- **354 contrats opérationnels** de protection adaptés et déclinés pour chaque territoire
- Des outils numériques s'adaptant aux nouveaux usages : la **brigade numérique** (offre de service **24/24 en ligne**)
- **46 brigades territoriales de contact et 250 groupes de contact** pour capter les « signaux faibles »
- **+ de 32 millions de français protégés et rassurés** par les gendarmes
- **+ de 5000 protocoles de participation citoyenne** signés en zone gendarmerie
- **+ de 150 intervenants sociaux de la gendarmerie** qui assurent des fonctions d'écoute, de médiation, d'information, d'appui dans l'accompagnement social


TROUVEZ LE JOB
QUI VOUS CORRESPOND
DANS LA CYBERSÉCURITÉ
cyberjobs.fr
#jobboard
#média
CYBERJOBS

MERCI À
LA RÉGION DES PAYS DE LA LOIRE
ET À NOS PARTENAIRES

Région
PAYS DE LA LOIRE

CYBER CERCLE

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

Réalisation : S.I.M. Publicité : 01 40 92 05 55