JANVIER 2021
NUMÉRO #02 / MENSUEL

la France qui gagne

INSTITUT SAPIENS *POUR QUE L'AVENIR AIT BESOIN DE NOUS*

La cybersécurité : spécificités et forces françaises

Cybersécurité : partager pour ne pas subir

La culture cyber française : un savoir-faire technique, des performances humaines

Intégrer le risque cyber dans les entreprises

l'édito

En septembre dernier, le Belfer Center, centre de réflexion d'Harvard, université américaine de référence, a publié un rapport comparant les différentes capacités en numérique de trente pays. En matière de sécurité du numérique, la France est classée deuxième derrière la Chine. Un résultat qui mérite d'être souligné et qui traduit l'excellence des compétences techniques nationales et la vitalité des entreprises françaises du domaine.

L'apport technologique français à l'origine du numérique est connu. En 1978, la France est également le premier pays à penser la sécurité des données des utilisateurs du numérique en adoptant la loi relative à l'informatique, aux fichiers et aux libertés, modifiée à de nombreuses reprises depuis, et notamment à la suite de l'adoption du texte européen dit RGPD. Ce texte à terme, se révèlera un avantage concurrentiel pour les entreprises européennes. Dix ans après, des règles dédiées à la fraude informatique, loi dite « Godfrain », verront le jour en France. En 2008, la France fait le choix d'une organisation donnant priorité au défensif quand d'autres pays choisissent de miser l'essentiel de leurs efforts sur les capacités offensives. En imaginant une réglementation qui inspirera une directive européenne en 2016 (dite « NIS ») et l'organisation de plusieurs pays, l'ANSSI, acteur étatique central de cette organisation, a su s'appuyer sur un tissu volontaire d'entreprises internationales, de PME et de startups disposé à accroitre les compétences de leurs équipes, à élaborer les référentiels et les méthodes nécessaires. Grâce à ces décisions et ces efforts, nous disposons aujourd'hui d'une offre performante et maîtrisée en matière d'analyse de risques et d'identifications de vulnérabilités, de détection d'attaques informatiques et de remédiation.

À l'initiative du président de la République, le « Campus Cyber », dont l'ouverture est prévue en septembre 2021, favorisera encore plus la coopération opérationnelle et la création de communs entre acteurs publics et acteurs économiques de la cybersécurité. Son élaboration et sa mise en oeuvre en ont été confiées aux entreprises, preuve de la vitalité du partenariat public-privé dans ce secteur clef d'activité.

Forts de ces atouts, et de la poursuite du travail commun dans les orientations choisies il y a dix ans, nous pourrons atteindre en 2025, pour le secteur de la cybersécurité, l'objectif fixé par le gouvernement d'un chiffre d'affaires de 25 Md€, soit 3,5 fois le chiffre de 2019, et de 75 000 emplois, un doublement du nombre actuel. Bien évidemment, ceci sera possible sous réserve que la stratégie sur la cybersécurité annoncée en septembre dans le Plan « France Relance », n'empêche pas le développement international des entreprises françaises par une interprétation inadaptée de la notion de souveraineté numérique.

À travers ses travaux réalisés en collaboration avec les acteurs de la cybersécurité, Syntec Numérique participe au développement de cet écosystème et à la création d'un numérique de confiance. De nombreux de défis sont encore à relever et nous les aborderons avec conviction et détermination !

de Godefroy de Bentzmann

Président de
Syntec Numérique

sommaire

Directeur de publication : Olivier Babeau
Direction artistique : Matthieu Rossat / Crédits photo : Institut Sapiens - cover : Nahel Abdul Hadi

état de l'art

Cybersécurité : État de l'art et enjeux pour les PME et les collectivités territoriales

Jérôme Notin
Directeur Général GIP ACYMA

Impliqué dans la sécurité numérique depuis de nombreuses années, ***Jérôme Notin*** *dispose d'expériences dans la création et la direction d'entreprises. Il a rejoint l'ANSSI en 2016 en qualité de préfigurateur du dispositif et a été nommé en mars 2017 directeur général du GIP ACYMA lors de sa création.*

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

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

Quelles leçons tirer du développement du télétravail pendant la crise sanitaire ?

Le confinement et le passage accéléré au télétravail ont mis au jour une vraie différence entre grands acteurs et acteurs de moindre taille. Les grosses entreprises étaient globalement prêtes à passer au télétravail, ont pu acheter des licences VPN (réseau virtuel privé). Côté public, l'État sait également bien se protéger grâce à l'ANSSI, véritable pépite de l'administration française, reconnue à l'international comme une référence de haut niveau en matière de cybersécurité.

En revanche, les plus petites structures – PME ou collectivités – ont dû trouver des solutions du jour au lendemain pour permettre à leurs collaborateurs de travailler à distance. Elles ont très souvent permis l'utilisation de machines personnelles, dont on sait qu'elles sont beaucoup moins sécurisées que le matériel fourni par les structures professionnelles. De ce fait, beaucoup de structures ont été victimes de rançongiciels puisqu'il suffit aux attaquants de se connecter sur le maillon faible, la machine personnelle, puis à travers le VPN de se connecter au système. Il est ensuite simple de cartographier le réseau, de voler et chiffrer des données et de détruire les sauvegardes existantes, afin de pouvoir réclamer une rançon contre leur restitution.

Le problème est encore culturel. On entend peu parler de cas de collectivités ou de PME victimes de cyber-malveillance, en dépit des attaques subies depuis le début de la pandémie. Les médias parlent des grands cas, pas forcément des plus petites structures. Trop de patrons et de responsables pensent encore que ça n'arrive qu'aux autres. D'où la mise en place rapide du télétravail sans prise en compte de la cybersécurité. Désormais, la situation est un peu plus mature, mais nous paierons encore longtemps ce manque de préparation et ce défaut de culture cyber. Les cybercriminels ont encore de beaux jours devant eux.

Où en sont les acteurs français dans le domaine des produits cyber ?

En France, nous avons de très bons ingénieurs ; par contre, les aspects business sont moins développés. Évidemment, il existe d'excellents produits proposés par les grands industriels, comme ceux de la défense à destination des grosses structures privées et publiques. La situation est en revanche toute autre pour les PME et les collectivités. On trouve bien quelques pépites françaises mais, de façon générale, force est de reconnaître un manque d'offre tricolore pour le mass market. Conséquence : les PME ne vont pas acheter français pour leur système de sécurité.

Deux raisons peuvent expliquer cet état de fait insatisfaisant. Le premier point est celui de la confiance. Les grands donneurs d'ordre, comme les entreprises du CAC 40, n'ont pas coutume de faire confiance aux start-ups françaises : on ne reprochera jamais à un responsable sécurité d'acheter américain. Heureusement, cette situation évolue et on observe une plus grande maturité dans l'analyse et la prise de risque potentielle des grands donneurs d'ordre. Le deuxième point est celui des investisseurs. Le stade de l'early stage était compliqué et long, encore récemment, avec des levées faibles, alors que les concurrents américains ou israéliens, n'ont pas la même difficulté. Mais là encore, la situation évolue positivement.

Nous faut-il plus d'Europe en matière de cybersécurité ?

Enfin, si penser la cybersécurité par le prisme national peut avoir du sens dans certains cas liés à la souveraineté, il faut également penser le cyber au niveau européen. Du point de vue business, force est de constater que le marché français est réduit, alors que l'Europe offre un marché de la taille du marché américain. La mise en place d'une obligation légale est également importante. De ce point, la directive NIS (Network and Information Security) de juillet 2016 marque un jalon important, puisqu'elle impose la sécurisation des réseaux. Il y a là un vrai levier de croissance potentielle pour les entreprises européenne et accessoirement françaises.

Sapiens Sapiens

Être humain

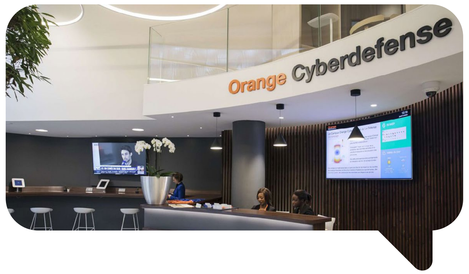
Sapiens Sapiens, c’est chaque mois une conversation en toute liberté avec une personnalité.
Une rencontre entre êtres humains, tout simplement, pour mieux se comprendre et comprendre le monde.

Cliquez ici **pour découvrir *Sapiens Sapiens***

Réalisation : hello@debutdecembre.com

keynote

.01
Cybersécurité : Partager pour ne pas subir



Michel Van Den Berghe et Chief Executive Officer d'Orange Cyberdéfense depuis le 1er juillet 2014. Il a rejoint le groupe en janvier 2014 suite au rachat d'ATHEOS dont il était le Président Fondateur depuis 2002. Il est le fondateur des Rencontres de l'Identité, de l'Audit et du Management de la Sécurité (RIAMS) qui rassemblent depuis 2004 les principaux décideurs publics et privés du marché de la sécurité des systèmes d'information.
Michel est Vice-Président du Pôle d'Excellence Cyber, initié en 2014 par le ministre des Armées (pacte défense cyber) et par le Conseil Régional de Bretagne (pacte d'avenir) avec une portée nationale et un objectif de rayonnement international.
En juillet 2019, Michel Van Den Berghe a été chargé de mission par le Premier ministre français, Édouard Philippe, afin de créer à l'horizon 2021 le premier Campus Cyber en Europe. Réunissant des industriels de la cyber sécurité, des PME-ETI, des start-up, des centres de recherche et de formation ainsi que les principaux services de l'État actif dans le domaine de la sécurité numérique, ce lieu a vocation à doter la France d'une capacité technologique et économique de premier ordre face à la concurrence internationale. Orange Cyberdéfense rassemble l'expertise en cyber sécurité à destination des clients professionnels du Groupe Orange et compte 2200 collaborateurs dans 220 pays.

CAMPUS CYBER

Orange Cyberdefense

Michel Van Den Berghe
Directeur Général chez Orange Cyberdefense

Avec Orange Cyberdefense, la France compte depuis peu une nouvelle licorne, ces entreprises définies par une grosse progression du chiffre d'affaires et une valorisation qui dépasse le milliard de dollars. Notre chiffre d'affaires est en effet passé de 80 millions d'euros en 2014, date du rachat d'Atheos par Orange, à 750 millions six ans plus tard. Quant à notre valorisation, elle avoisine les deux milliards d'euros. 100 % français au départ, Orange Cyberdefense a grandi, notamment avec deux acquisitions importantes en Europe et nous sommes désormais leader européen en matière de cybersécurité.

Une des grandes leçons que je retire de mon expérience à la tête d'Orange Cyberdefense est qu'à expertise égale, les entreprises préfèrent travailler avec un partenaire de nationalité européenne, plutôt que de choisir une grande boîte américaine. La souveraineté numérique européenne, dont on parle temps, commence à exister un petit peu. Les entreprises européennes s'inquiètent de la mainmise exclusive des GAFA. Mais il faut bien insister sur l'expression « à expertise égale » : pour une entreprise française ou européenne, il n'y a pas de raison de favoriser un prestataire cyber sur sa seule nationalité ! Le plus important demeure l'expertise ; la considération de la nationalité vient naturellement ensuite.

Et c'est un point majeur : la France n'a pas à rougir de ses performances en termes d'expertise sur la cybersécurité. Nous nous plaçons en troisième ou quatrième position mondiale, et nous sommes bien identifiés comme un des pays leaders en la matière. Toutefois, trop de nos belles pépites tendent à s'expatrier, parce qu'elles peinaient encore récemment à grandir en Europe.

C'est une des raisons pour lesquelles le Gouvernement a voulu impulser un campus cyber, qui doit devenir une vitrine de notre savoir-faire cyber, un lieu totem. La France se positionne bien en défense, soit. Il s'agit maintenant de permettre à nos start-ups les plus prometteuses de se développer et de s'épanouir sans passer par un exil américain.

Mais les ambitions du campus cyber ne s'arrêtent pas là. Il s'agit plus profondément d'amener tout un écosystème dans un même lieu, en créant une sorte de village d'Astérix. Comme tous les lecteurs de la série le savent, en dépit des désaccords ponctuels, tous les Gaulois sont prêts à se rassembler pour lutter contre l'envahisseur. Et quand les pirates les voient approcher, ils préfèrent encore se saborder. C'est un peu ce que nous visons. Nous voulons rassembler les quatre grandes composantes de la cyber : les industriels, qu'ils soient grands, moyens ou petits ; tout ce qui touche la formation, car on sait le manque chronique de compétences en matière de cybersécurité ; la recherche, qu'il est essentiel de faire cohabiter avec les grands industriels ; et enfin des composantes de l'État comme l'ANSSI, la DGSE ou encore l'Intérieur.

Le défi n'est pas mince, mais la montée en puissance est rapide depuis la lettre de mission que j'ai reçue en 2019. Une SAS vient d'être immatriculée ; nous avons choisi une tour à côté de la défense, où nous disposerons de 25 000 m2. Et nous espérons accueillir plus de 1000 personnes dès septembre 2021. Car notre objectif n'est pas de créer un lieu qui ne vive que lors des visites officielles. Le campus cyber se veut un lieu commun et surtout opérationnel, un lieu où les équipes des entreprises travaillent au quotidien. Toutes les équipes : celles de grandes entreprises comme Atos, Capgemini ou Thalès mais aussi de start-ups, de PME, de l'ANSSI, de certaines écoles.

L'idée phare est de partager pour ne pas subir. Nous sommes face à des gens organisés et créatifs. Il faut donc rassembler les savoir-faire et construire ensemble un écosystème qui monte en expertise. Cette approche est de loin la meilleure pour défendre les intérêts des sociétés françaises. Il n'est pas forcément naturel de mettre en commun un avantage concurrentiel avec ses rivaux. Mais si je peux profiter de l'expertise venue d'une autre entreprise, et lui transmettre la mienne, nous montons ensemble en niveau. La bonne nouvelle, c'est que tout le monde adhère à ce projet d'intelligence collective. Parce que tous les acteurs français savent que pour exister et rivaliser face aux grandes boîtes américaines et chinoises, il faut comprendre la menace, son origine, pourquoi certaines sociétés sont attaquées, etc. Seul le partage peut nous rendre à même de prendre les devants et de contrer les attaques malveillantes, d'où qu'elles viennent.

MVDB

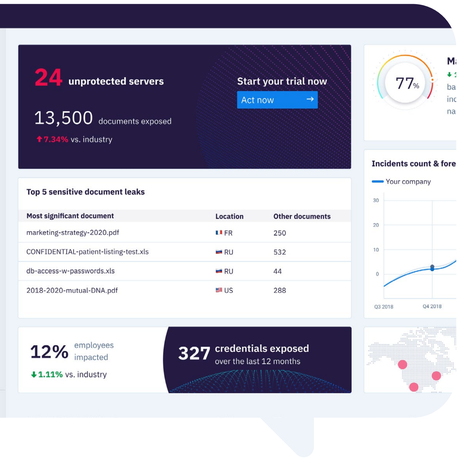
Rapport de Michel Van Den Berghe remis au premier ministre en janvier 2020 : https://www.ssi.gouv.fr/uploads/2019/10/campuscyber-rapport.pdf

Propositions pour 2022

S'attaquer résolument au problème des compétences, en formant davantage aux métiers cyber et en se donnant les moyens de retenir nos talents.

Renforcer notre intelligence collective dans un écosystème encore trop éclaté.

keynote



Erwan Keraudy est le CEO de CybelAngel, société qu'il a co-fondée en 2013. Sous son impulsion, CybelAngel est devenu l'un des leaders de la protection contre les risques numériques, permettant aux entreprises à travers le monde de se prémunir contre les menaces cyber tout en préservant leurs actifs stratégiques. Avant de créer CybelAngel, Mr. Keraudy a été l'adjoint au Directeur de l'Investissement chez SBI Funds Management Private Limited, joint-venture entre SBI et AMUNDI. Il a également travaillé en tant que Credit Trader et Portfolio Manager pour la Société Générale Asset Management et en tant qu'analyste financier chez Natixis CIB. Son expérience dans l'univers du trading l'a sensibilisé à la nécessité de protéger l'information confidentielle et aux dommages potentiels causés par la fuite de ces dernières. Erwan Keraudy est diplômé en économie de l'université de Manchester et a obtenu un Master of Science en Finance à l'ESCP Europe à Paris. Il est un alumni de l'Institut des Hautes Etudes de Défense Nationale avec une spécialisation en Affaires Internationales et Intelligence Stratégique. Mr. Keraudy est internationalement reconnu pour son savoir et expertise dans le domaine de la cybersécurité.

.02

Cybersécurité : une course à l'armement sur les logiciels

CybelAngel

Erwan Keraudy

CEO de CybelAngel

Dans le tissu économique de la cybersécurité, il existe deux grandes catégories d'acteurs : les acteurs qui font du service ; les acteurs qui font du software. Le service a une base de clients à laquelle il essaie de fournir un grand nombre de compétences et d'outils ; le software a globalement une compétence ou plusieurs qu'il va essayer de répliquer sur une base plus large à travers la planète. C'est dans cette seconde catégorie que se situe CybelAngel.

Notre particularité est de savoir trouver les fuites de données pour les grands groupes à travers la planète. Nous avons développé une technologie unique qui nous permet de scanner massivement tout ce qui est potentiellement connecté sur la planète – soit 4,3 milliards d'adresses IP. Nous scannons également les forums de hackers, ou encore les requêtes DNS. Grâce à cette énorme collecte d'informations, nous sommes en mesure de posséder une empreinte du réseau mondial en temps réel. Et dans cette immense masse, nous sommes capables de trouver un grand nombre de serveurs qui sont complètement ouverts, alors même qu'ils partagent des données éminemment sensibles pour les entreprises.

Quel type de données ? Le plus simple est encore de donner quelques exemples concrets. Nous avons récemment trouvé, en accès libre, le plan du moteur d'un avion à plusieurs milliards. Il était tout simplement hébergé sur le serveur de la société chargée de fournir des boulons de précision à notre client. Il est normal que ce sous-traitant possède les plans nécessaires à son activité ; mais pas nécessairement qu'il oublie de traiter ces données avec prudence. Pour un des plus gros opérateurs mondiaux de cloud, nous avons trouvé le plan de l'architecture de tout son data center, avec toutes les méthodologies de sécurité. Nous vivons en effet une période de guerre froide, avec une vraie prédation sur les données.

CybelAngel est donc là pour détecter les fuites de données par négligence et les ramener à leur propriétaire, charge ensuite à ce dernier de faire fermer les serveurs incriminés. Cette capacité technologique de repérer les fuites est cruciale, car ces problèmes de données arrivent tous les jours : taper « data breach » dans Google News suffit pour le mesurer. Facebook a récemment perdu les données de 500 millions d'utilisateurs, avec leur numéro de téléphone. Marriott a perdu la base de données de tous leurs clients avec leur numéro de passeport. Dans les deux cas, il s'agissait de serveurs de données hébergées par des prestataires. Pour Marriott, au-delà des dommages en termes d'image, cet incident a représenté 127 millions d'euros en pénalités. CybelAngel avait pourtant vu ces fuites de données des mois avant.

Malgré l'image de complexité qui s'y attache, le hacking est un jeu d'enfants. Au fond, toutes les attaques sont réductibles à trois étapes : la collecte d'informations ; la weaponisation, qui consiste à trouver l'information qui a le plus de valeur et qui est la plus simple à utiliser ; l'exploitation (que l'on décide de détruire, d'espionner ou d'exposer les données recueillies sur la place publique). Il importe peu que l'attaque viennent de hackers malveillants, de journalistes ou des services de surveillance de pays étrangers : la méthode est la même.

CybelAngel a industrialisé la phase de reconnaissance. Notre force est d'avoir créé des algorithmes d'IA qui vont trouver, parmi les milliards de documents quotidiens, les quelques serveurs et documents qui sont extrêmement sensibles. La cybersécurité est une course à l'armement sur les logiciels, et le nôtre permet via le machine learning d'éliminer 99 % du bruit. Nos analystes ou ceux de nos clients peuvent ensuite faire le dernier kilomètre, puis proposer de la valeur en suggérant de fermer tel serveur.

Un dernier élément : on dit souvent que les métiers cyber sont des métiers masculins. C'est faux. Notre équipe en est une excellente illustration, et il n'y a aucune raison de penser que les femmes n'ont pas leur place dans cette aventure. Je dis souvent que toutes les activités criminelles qui existent dans le monde réel sont aussi en ligne : on n'imagine pas une police fermée aux femmes ; pourquoi penser autrement pour la cybersécurité ? La cyber résout des problèmes majeurs dans le monde et c'est un défi qui peut parler à n'importe quel ingénieur.

EK

Propositions pour 2022

Sensibiliser davantage tous les acteurs de la chaîne (donneurs d'ordre et sous-traitants) au problème des données stratégiques sur serveurs ouverts.

Casser l'image de métiers presque exclusivement masculins attachée au domaine de la cyber.

.03 La culture cyber française : un savoir-faire technique, des performances humaines

Yassir Kazar
CEO & Fondateur de Yogosha

Passionné par la cybersécurité et l'entrepreneriat, Yassir Kazar a monté sa première startup alors qu'il terminait ses études. Par la suite, il fait carrière dans les services informatiques et devient staff manager en Business Intelligence chez CGI tout en enseignant la sécurité à l'université et dans des écoles d'ingénieurs. En 2015, Yassir rencontre Kévin Liagre et fonde Yogosha, une plateforme de cybersécurité qui s'appuie sur une communauté de hackers qui aident les entreprises à détecter et corriger les vulnérabilités de leurs systèmes informatiques et ainsi à sécuriser leurs entreprises – et leur business.
www.yogosha.com

© Yogosha

La cybersécurité française est riche de compétences pointues, mais également d'un socle de valeurs et de notions partagées : l'entraide, la solidarité, la bienveillance, le goût du challenge, la familiarité avec le risque et la notion de vulnérabilité. Deux éléments sont particulièrement forts au cœur du réacteur cyber, l'adaptabilité et la confiance.

L'adaptabilité d'abord car le risque en cybersécurité évolue continuellement. La résolution d'une première faille n'empêche pas l'apparition d'une deuxième. Cette dynamique est due à l'évolution constante des solutions technologiques qui offrent à chaque étape d'amélioration de nouvelles opportunités de détournement de ses usages. Ainsi, une faille détectée au jour 1 n'efface pas la menace, elle nous oblige à être encore plus vigilants face à l'ingéniosité des hackers malveillants Le rôle d'une entreprise cyber comme Yogosha est avant tout d'accompagner ses clients dans la durée et de faire preuve d'agilité pour assurer leur sécurité face à une menace mouvante.

La confiance ensuite car la maîtrise du risque cyber s'inscrit dans une chaîne continue de responsabilités qui sont humaines et partagées. Une confiance qui repose sur un ensemble de compétences au service d'un même objectif : garantir la prospérité et la pérennité d'un État, d'une collectivité, d'une institution ou d'une entreprise. La compétence technique est difficile à trouver dans le secteur de la cyber et c'est la raison pour laquelle Yogosha a choisi de se tourner vers la communauté des hackers dit éthiques.

Au fond, c'est un retour aux sources : historiquement le hacker est né dans les clubs du MIT et avait pour mission de détecter les failles d'un système pour mieux les prévenir. Dans son premier avatar, et avant que ce terme n'en vienne à désigner dans l'imaginaire collectif un pirate informatique malveillant, le hacker possède un rôle positif. Cette approche par le hacker participe à la sécurisation de l'environnement de travail et donc à une meilleure productivité de ses éléments.

Propositions pour 2022

Face à la pénurie de compétences, la communauté des hackers éthiques est une solution pour avoir accès à des solutions rares et indispensables.

Donner toute sa place au domaine de la cyber sécurité dans la réflexion éthique sur la transformation numérique.

Considérer la cyber sécurité comme un angle de lecture indispensable pour mieux appréhender le risque numérique.

Nous avons ainsi créé un marché blanc au sein duquel des hackers sélectionnés travaillent avec les entreprises et où la confiance, l'engagement et l'écoute sont essentiels. Ce sont des valeurs qui innervent tout le secteur de la cyber sécurité, et que l'on retrouve plus largement dans tous les débats actuels sur l'IA et la transformation numérique de nos sociétés. Il est dommage, d'ailleurs, que le projecteur ne soit pas plus braqué sur le secteur de la cybersécurité qui constitue un observatoire inédit des mutations et un laboratoire d'expérimentation unique des usages éthiques des technologies.

YK

.04 Intégrer le risque cyber dans les entreprises.

Directrice de la Practice Cybersécurité, services des infrastructures Cloud de Capgemini, Nolwenn Le Ster préside également le Comité Cybersécurité de Syntec Numérique. Ingénieur de formation, Nolwenn a quinze années d'expérience en management dans le secteur de l'IT. Elle y a occupé différentes fonctions dans le commerce, le bid management, le marketing, le pilotage d'équipes de projet et infogérance, le management de centres de profit et l'innovation sur les thèmes de la cybersécurité, le cloud et le smartdata/IoT.
La cybersécurité est un thème fil rouge de son parcours : elle a construit des offres, mis en place des partenariats, piloté des équipes d'experts, des centres de service et de profit certifié ISO27001 des services cloud.

Nolwenn Le Ster

Directrice de la Practice Cybersécurité, services des infrastructures Cloud de Capgemini.

En matière de transformation digitale, la crise du COVID a été un formidable accélérateur de tendances. Du jour au lendemain, des milliers d'entreprises ont dû étendre « leurs murs » en passant au télétravail pour continuer leur activité. Néanmoins, cette transformation est allée de pair avec une multiplication et une complexification des attaques cyber, qui impose aujourd'hui d'augmenter la réponse des entreprises en la matière.

La plupart des salariés en télétravail n'utilisant pas les solutions de Cloud, ils ont dû recourir à leur équipement et leur connexion personnels pour travailler. Or ces périphériques sont loin d'avoir les mêmes niveaux de sécurisation que ceux mis à leur disposition sur leur lieu de travail. De même, le fait de travailler chez soi, dans un environnement où l'on se sent en confiance, diminue la vigilance des usagers quant aux différents risques cybers. La crise a ainsi accéléré le diagnostic sur la faiblesse du niveau culturel des actifs en la matière.

Avec de nouveaux usages comme le télétravail, la menace change et la vision des entreprises doit également évoluer. La meilleure stratégie à développer contre le risque cyber est de mettre en place de robustes scénarios de PRA – plan de reprise d'activité – comprenant toutes les réponses à apporter face à une crise ou un évènement exogène perturbant le bon déroulé de l'activité. Ces plans doivent devenir systématiques au sein des entreprises françaises et doivent être réalisés avec le plus grand sérieux pour prévenir toutes les menaces de ce nouveau genre.

L'intégration du risque cyber par les entreprises a déjà bien évolué en 2020. Lors du premier confinement, la plupart des entreprises avaient mis un mois et demi à retrouver un rythme de fonctionnement considéré comme normal. À l'inverse, lors du deuxième confinement, on a pu constater une véritable évolution sur ce sujet : les entreprises se sont clairement adaptées en amont et ont su changer leurs processus pour concilier cybersécurité et continuité de l'activité. La cybersécurité est ainsi en train de devenir un élément important dans la gestion et la stratégie de l'entreprise, et c'est un changement à mettre au crédit du Covid 19.

Un problème demeure néanmoins : si le besoin cyber-sécuritaire est de plus en plus présent chez les entreprises, ces dernières sont confrontées à une pénurie de spécialistes qualifiés. Il est aujourd'hui de plus en plus difficile de trouver les bonnes compétences pour répondre au risque cyber. Cette pénurie de talents ne touche d'ailleurs pas uniquement la France, on estime qu'il y aurait près d'un million et demi d'emplois non-pourvus dans la cybersécurité au niveau mondial. La France peut néanmoins relever ce défi, grâce à sa formation et un écosystème numérique très riche, sur lequel elle peut s'appuyer pour répondre à ces nouveaux besoins. vers une mobilité verte.

NLS

Propositions pour 2022

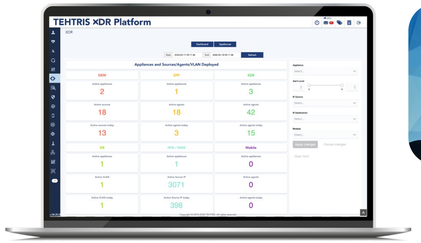
Systématiser les PRA au sein des entreprises pour assurer une continuité de l'activité en toutes circonstances.

Développer les formations initiales et continues préparant aux métiers de la cybersécurité.

Insuffler une véritable culture cyber dans les entreprises en sensibilisant les salariés et les employeurs aux différents risques cyber posés par le télétravail.

guest

Le « made in France » au service de la cyber-paix internationale



Elena Poincet et Laurent Oudot ont fondé Tehtris en 2010. L'entreprise de 70 collaborateurs aujourd'hui s'est construite sur leurs expertises opérationnelle et technologique.

Elena Poincet était pendant plus de 20 ans au Ministère des Armées, experte dans la gestion et la conduite d'équipes spécialisées. Laurent Oudot est un expert international en cybersécurité, dont les compétences furent mises à profit dans des contextes très sensibles comme le Commissariat à l'Energie Atomique, le Ministère de la Défense, l'ONU etc.

TEHTRIS
FACE THE UNPREDICTABLE

Propositions pour 2022

01. Former et informer dès le plus jeune âge pour renforcer la prise de conscience des risques, susciter des vocations et rendre concrets les potentiels et menaces des technologies

02. Continuer à parier sur la recherche appliquée dans le domaine de la cyber

03. Considérer l'angle anti-espionnage pour construire la France cyber

TEHTRIS est un éditeur français de solutions de cybersécurité, cofondé en 2010 par Laurent Oudot et Elena Poincet.

Pendant plus de 15 ans au service de l'État et des missions de paix, Elena Poincet et Laurent Oudot ont acquis une connaissance pointue des méthodes d'attaques des groupes actifs dans l'espionnage et le sabotage. Devant anticiper une menace cyber et savoir réagir à une attaque cyber, ils ont construit une expertise unique, tournée vers la capacité à prévenir, planifier, protéger et se défendre dans l'incertitude du contexte et face à l'imprévisibilité de ces attaquants. Au cœur de cette logique de prévention, trois éléments sont fondamentaux : une technologie robuste, une expertise humaine fiable et des engagements respectés.

Ces engagements, ce sont ceux que nous avons pris pour notre pays, explique Laurent Oudot. *Nous avons fait le choix du made in France. Tous les produits sont issus de la R&D implantée à Pessac (Gironde). Nous nous sommes également orientés vers de la smart money : des investisseurs capables de nous apporter des fonds mais surtout aussi une expertise. Nous avons donc choisi des acteurs alignés sur nos ambitions, notre croissance à venir, nos défis technologiques. C'est en France que nous les avons trouvés. C'est par exemple le cas d'ACE Management, un fonds sectoriel qui investit depuis quelques années dans la cybersécurité notamment.*

Nous sommes convaincus par le potentiel français et européen : il y a un tissu économique très dense, un grand potentiel d'innovations et des ingénieurs excellents. Il faut transformer la Saison 2, pour ainsi dire, celle qui inclut nos nouveaux participants, investisseurs et nouveaux collaborateurs. Nos valeurs sont vécues, pas écrites. C'est pourquoi nous allons adopter un mode de fonctionnement proche du compagnonnage et de l'artisanat. En cuisine, on apprend les bons gestes auprès des plus anciens. Nous procèderons de la même manière : les nouveaux arrivants apprendront les bons gestes, ceux de Tehtris, au contact de nos collaborateurs actuels.

Il faut dès à présent accélérer la formation de nos jeunes au code, aux enjeux du numérique, mettre en perspective la technologie et les potentiels sur la vie de chacun : à la fois pour rendre plus concret le monde de l'entreprise et pour faciliter les recrutements d'ingénieurs.

Il faut également que la France puisse être motrice dans la construction d'une Europe de la Cyber en considérant deux dimensions qu'elle sous-estime encore aujourd'hui, l'intelligence économique et l'anti-espionnage. Il est essentiel d'anticiper pour ne pas subir : la vélocité et la technicité des attaques sont très puissantes et alimentées par de l'intelligence artificielle. La France et l'Europe doivent se placer à la pointe de la recherche appliquée dans le domaine.

guest

Valoriser les réussites françaises c'est créer des champions sur le marché mondial

Jacques de La Rivière est Président, Co-fondateur de Gatewatcher. Après des études d'ingénieur à l'ESIEA, il débute sa carrière chez Mahindra Satyam en Inde en tant que chef de projet offshore. Il poursuit ensuite en tant qu'Ingénieur d'Affaires chez ADNEOM et BK Consulting sur des projets de commercialisation de plateformes de trading haute fréquence. En 2015, il créé Gatewatcher, solution de détection de menaces avancées en temps réel. Gatewatcher s'adresse à toutes les organisations qui souhaitent sécuriser leur système d'information face à la menace cyber dont les Opérateurs d'Importance Vitale, identifiés par la LPM 2014-2019. Les produits Gatewatcher sont certifiés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Présentation de la technologie :
Gatewatcher est le premier éditeur de logiciels de sécurité spécialisés dans la détection des intrusions avancées basé sur l'intelligence artificielle, développés en France et qualifiés par l'ANSSI pour l'application de la Loi de Programmation Militaire.
GATEWATCHER édite entre autre le système de détection Trackwatch®. Basé sur une technologie nouvelle génération, il protège efficacement les organisations contre les intrusions et le piratage.
Fondé en 2015 par Jacques de La Rivière, son Président, ingénieur ESIEA, Gatewatcher a été propulsé par l'accélérateur Le Village by CA entre 2015 et 2017.

Propositions pour 2022

01. Renforcer l'accès au marché local pour les entreprises cyber

02. Bâtir un marché européen de la cybersécurité

03. Orienter la décision publique vers des solutions industrielles déjà en œuvre

GATEWATCHER

La France dispose d'une culture forte en ingénierie et en sécurité mais elle reste un petit marché pour le secteur de la cybersécurité, qui est principalement trusté par les acteurs anglo-saxons.

Il faut surtout distinguer les activités de services de la création de produits dans le domaine de la cybersécurité. Si les entreprises françaises excellent dans le service en cyber, la réalité n'est pas la même pour les produits. Ce contraste s'explique simplement : le secteur des services est beaucoup plus dynamique grâce, entre autres, à une demande locale renforcée par les contraintes du droit du travail. Cette spécificité française dynamise le marché du service et permet aux offreurs français de s'exporter facilement à l'international. L'objectif dans les années à venir est de créer les mêmes leviers pour les produits cyber.

Pour faire émerger des champions cyber en France, on ne le redira jamais assez, la commande publique est essentielle. C'est une première étape cruciale pour solidifier la confiance en nos produits à l'international. Sans leader local et sans valorisation des réussites françaises, il sera plus difficile pour la France de créer des champions sur le marché mondial. De premières évolutions réglementaires tendent en ce sens, l'objectif pour les années à venir est de les rendre encore plus performantes afin de créer un socle solide pour nos entreprises.

Par ailleurs, l'administration a encore trop tendance à se positionner comme un industriel du numérique. Elle développe ses propres solutions, qui viennent concurrencer les industriels. C'est une difficulté supplémentaire pour les entreprises qui veulent effectivement percer sur le marché français.

Naturellement, toute stratégie nationale doit s'inscrire dans une stratégie européenne forte puisque le code des marchés publics français dépend du code des marchés publics de l'Union Européenne. Le Small Business Act est une demande récurrente chez les acteurs économiques français. À raison, puisque c'est un instrument qui permettrait d'orienter les achats vers des produits français, ou du moins européens. Alors que le concept de souveraineté numérique innerve tous les discours politiques, c'est le moment ou jamais de mettre en œuvre cette volonté et ces ambitions par des moyens qui ont prouvé leur efficacité, notamment aux États-Unis.

Il faut toutefois prendre conscience que le chemin de la souveraineté numérique sera long, surtout dans le secteur de la cyber. Créer les conditions d'une autonomie stratégique européenne alors que l'Allemagne a déjà une culture d'achat local forte dans ce secteur sera difficile mais pas irréalisable si la France soutient dans un premier temps le dynamisme et le savoir-faire de ses acteurs. La création du Campus Cyber est une initiative majeure qui va renforcer l'attrait de la filière cyber française.

La France a de sérieux atouts pour renforcer sa place dans le domaine de la cybersécurité. Misons ainsi sur notre écosystème entrepreneurial dynamique et combattant et profitons d'un contexte propice à l'expression d'un besoin cyber, pour mettre en œuvre les ambitions d'une souveraineté technologique que nos politiques appellent de leurs vœux.

agenda
de l'Institut Sapiens

Mardi 22 décembre

Sortie de Sapiens Sapiens #2

L'économie de marché a-t-elle encore un avenir ?

Courant janvier

Publication de notre étude

La jeunesse face au défi climatique

Courant janvier

Podcast

L'écologie à tout prix ?

Mardi 12 janvier

Visio café #11

Les biais algorithmiques: un faux problème ?

agenda
de l'Institut Sapiens

Mercredi 20 janvier

Les Rencontres de la France qui gagne #3

Santé & innovation

Vendredi 22 janvier

Sortie de Sapiens Sapiens #3

La démocratie : un système obsolète ?
avec Pierre-Henri Tavoillot

Courant février

Visio café #12

Santé : luttons contre la douleur chronique

Courant février

Les Rencontres de la France qui gagne #4

L'industrie 4.0

Syntec Numérique est l'organisation professionnelle des entreprises de services du numérique (ESN), des éditeurs de logiciels et des sociétés de conseil en technologies. Il regroupe plus de 2 000 entreprises adhérentes qui réalisent 80% du chiffre d'affaires total du secteur (plus de 57 Md€ de chiffre d'affaires, 530 000 employés dans le secteur). Présidé par Godefroy de Bentzmann depuis juin 2016, Syntec Numérique contribue à la croissance du secteur et à la transformation numérique de notre pays à travers la promotion des nouveaux usages du numérique, le soutien à l'emploi et à la formation, l'accompagnement de ses adhérents dans leur développement et la défense des intérêts de la profession.

Contacts média

Caroline Fouquet – 06 99 85 48 24
cfouquet@syntec-numerique.fr

Amélie Rochette – 01 41 34 20 27
arochette@hopscotch.f

syntec numérique

INSTITUT
POUR QUE L'AVENIR AIT BESOIN DE NOUS
SAPIENS

Qui sommes-nous ?

L'Institut Sapiens est un organisme à but non lucratif dont l'objectif est de peser sur le débat économique et social.
Il se veut le premier représentant d'une think tech modernisant radicalement l'approche des think tanks traditionnels. Il souhaite innover par ses méthodes, son ancrage territorial et la diversité des intervenants qu'il mobilise, afin de mieux penser les enjeux vertigineux du siècle.

Sa vocation est triple :
Décrypter — l'Association aide à la prise de recul face à l'actualité afin d'être capable d'en comprendre les grandes questions. L'Institut Sapiens sera un centre de réflexion de pointe sur les grands enjeux économiques contemporains.

Décloisonner et faire dialoguer — l'Association veut mettre en relation des mondes professionnels trop souvent séparés : Universitaires, membres de la sphère publique, praticiens de l'entreprise ou simples citoyens, ils doivent pouvoir se rencontrer pour réfléchir et dialoguer. Afin d'être réellement représentatifs de toutes les compétences et expériences, les groupes de travail associent systématiquement des personnes d'horizons professionnels divers (de l'ouvrier au dirigeant de société cotée) et peu important leur lieu de vie (Métropole, DOM-COM).

Former — Le XXIe siècle est le siècle de l'information ; il doit devenir pour l'individu celui du savoir. Comprendre le monde implique une capacité à faire un retour sur notre histoire, à connaître le mouvement millénaire des idées, à posséder ces Humanités dont l'importance est plus grande que jamais. Parce qu'il veut faire accéder à une compréhension du monde, l'Institut Sapiens se fixe aussi pour objectif de promouvoir cette culture générale sans laquelle demain plus personne ne pourra comprendre son environnement.

Adhérez !

Indépendant et non partisan,
l'Institut Sapiens vit grâce à votre soutien.
Cliquez ici pour adhérer.

Nous acceptons aussi les mécénats,
pour cela il vous suffit de nous contacter
à contact@institutsapiens.fr

INSTITUT
POUR QUE L'AVENIR AIT BESOIN DE NOUS
SAPIENS

Début Décembre
Design / hello@debutdecembre.com

Suivez-nous sur les réseaux sociaux :