–LA CYBERSÉCURITÉ INDUSTRIELLE–

TENDANCE MÉTIERS DANS L'INDUSTRIE

Les systèmes de production et les solutions de type embarquées sont depuis plusieurs années déjà la cible de cyberattaques. Face à la multiplication de ces menaces, la cybersécurité industrielle est devenue un enjeu crucial pour les entreprises afin de préserver leur image et leur compétitivité. Des opportunités d'emploi cadre existent dans le domaine de la sécurisation informatique appliquée à ces outils industriels que ce soit dans des cabinets d'ingénierie-R&D ou des ESN, avec des compétences attendues en automatisme, ou équipements connectés… En 2017, un peu moins de 200 offres d'emploi ont été publiées sur ce champ, soit une multiplication par 1,6 en un an des besoins en recrutements exprimés.

Avec le concours
du Programme d'Investissements d'Avenir

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

–LES ENJEUX–

La cybersécurité est traditionnellement définie comme l'« état recherché pour un système d'information lui permettant de résister à des évènements venus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises[1] » . Appliquée aux domaines industriels, elle concerne essentiellement les outils de production.

FAIRE FACE À DES ATTAQUES QUI S'INTENSIFIENT

Renault en mai 2017, le géant de l'agroalimentaire Mondelez un mois plus tard... autant de cas de cyberattaques qui ont récemment défrayé la chronique avec, comme impacts, une mise à l'arrêt des unités de production et une lourde perte financière. De telles attaques à destination des industriels se sont multipliées depuis 2010, année au cours de laquelle le virus Stuxtext a contaminé les programmes de contrôle d'un site nucléaire iranien, via l'introduction d'une clé USB. Cet épisode marque un tournant dans l'attitude adoptée par les industriels face aux risques de cyberattaques. Il a élevé leur niveau de sensibilité face aux risques, l'État étant intervenu par ailleurs auprès de certains industriels pour s'enquérir des actions préventives et curatives individuellement mises en place.

Mais cette prise de conscience, même si elle s'accélère, n'est que relative. De nos jours, certains industriels continuent à penser qu'ils ne peuvent pas être victimes d'attaques. Ils jugent leurs outils de production protégés du fait de la sécurisation de leurs systèmes d'information, et considèrent la valeur de leur patrimoine industriel trop faible pour représenter une cible potentielle aux yeux des cyber-attaquants. Et quand bien même ils perçoivent la potentialité d'une menace, ils s'interrogent sur l'impact du processus de sécurisation que ce soit sur leur cadence de production ou en matière de coûts.

Pour certains experts, si la sécurisation des systèmes de production s'impose de manière moins prégnante que la sécurisation des systèmes d'information, c'est peut-être en raison de l'introduction tardive de l'informatique dans la sphère industrielle. Pendant longtemps, celle-ci a reposé sur des systèmes de contrôle-commande (ICS) peu connectés au monde extérieur. De fait, l'enjeu principal des industriels au moment de la conception de ces systèmes était de garantir leur sûreté bien plus que leur sécurité. Mais avec l'introduction de systèmes Ethernet ou de serveurs censés augmenter la performance de ces installations, la question de leur vulnérabilité s'est progressivement imposée, jusqu'à devenir d'autant plus cruciale aujourd'hui que les technologies évoluent[2].

Au-delà même des outils et systèmes de production, les acteurs de l'industrie doivent réfléchir à la sécurisation des produits qu'ils mettent en circulation (systèmes embarqués, objets connectés...). Depuis quelque temps, la presse se fait le relais d'exemples de vulnérabilités si ce n'est de cyberattaques, sur des systèmes de navigation d'avions[3], sur des voitures automatiques[4]...

TENIR COMPTE DES RÉGLEMENTATIONS QUI ÉVOLUENT

Les institutions, de leur coté, ont bien compris la nécessité d'inciter les entreprises à mettre en place des politiques et des actions de cybersécurité. Plusieurs directives et réglementations ont été élaborées en ce sens. La Loi de programmation militaire 2014-2019 a

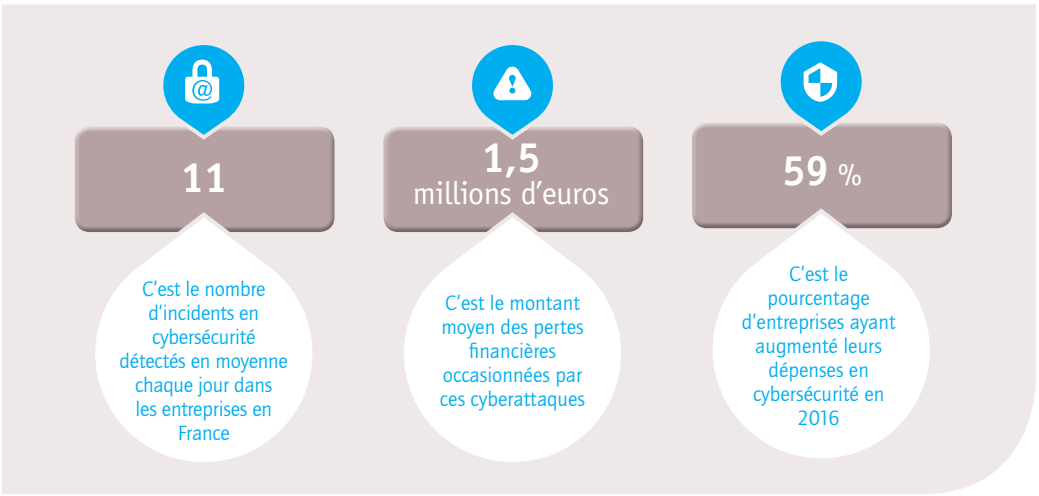
1. Définition de l'Agence nationale de la sécurité des systèmes d'information (l'Anssi) issue du Référentiel technique version 4.1.1 édité par le Pôle d'excellence Cyber.
2. *Cyber protection des systèmes de contrôle-commande industriels : une approche à base de modèles pour détecter et réagir aux cyberattaques.* Franck Sicard, Éric Zamaï et Jean-Marie Flaus, 2018.
3. https://www.riskinsight-wavestone.com/2015/09/cybersecurite-dans-laerien-pirater-un-avion-cest-possible/
4. https://blog.appknox.com/cyber-attacks-in-connected-cars/

permis de dégager un budget important pour recruter des agents au sein de la Direction générale de l'armement, complétant ainsi le plan d'action institutionnel mis en place dès 2009 avec la création de l'Anssi. Elle a aussi fixé des obligations majeures concernant les opérateurs d'importance vitale et les secteurs d'activité dits sensibles (c'est-à-dire des entreprises positionnées sur les champs de l'énergie, des transports, etc.)[5]. À ces réglementations, s'ajoutent celles découlant des mises en conformité exigées dans le cadre du RGPD (Règlement général sur la protection des données). Mais plus qu'une contrainte, la cybersécurité industrielle s'impose de plus en plus aux acteurs de l'économie comme un atout de compétitivité.

« Aujourd'hui, cela est devenu un produit différenciant en termes d'offres. Nos bâtiments sortent avec un label cyber-protégé. » (Recruteur).

C'est d'ailleurs tout l'enjeu de la certification ISO 27000 relative au management de la politique de la sécurité des systèmes d'information que d'accréditer suite à des audits, les produits et solutions délivrées par les industriels.

– Figure 1 –
Les chiffres-clés 2016 de la cybersécurité en France[6]

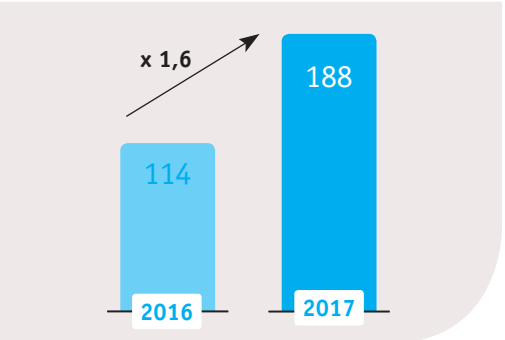


Source : Apec, 2018

– LES OPPORTUNITÉS –

Entre 2016 et 2017, le nombre d'offres d'emploi diffusées par l'Apec dans le champ de la cybersécurité industrielle a été multiplié par 1,6, passant de 114 à 188 **(figure 2)**. Elles ont été publiées par des entreprises recherchant des compétences et/ou proposant des missions en lien avec l'enjeu que représente la sécurisation des outils de production (machines connectées, objets et systèmes embarqués...).

– Figure 2 –
Nombre d'offres publiées par l'Apec entre 2016 et 2017 en cybersécurité industrielle



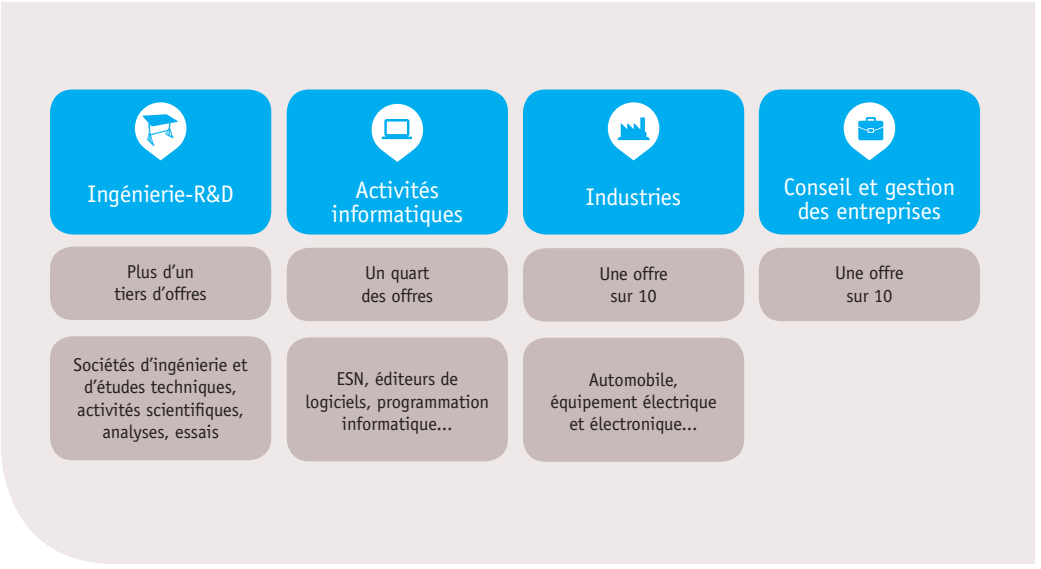
Source : Apec, 2018

5. L'obligation a été étendue, sous l'impulsion de l'Anssi, à l'ensemble des pays européens *via* la Directive NIS de 2016.
6. *The Global State of Information Security® Survey 2017*, PwC.

PLUS D'UN TIERS DES OFFRES CONCERNENT LE SECTEUR DE L'INGÉNIERIE-R&D

Sur l'ensemble des années 2016 et 2017, 36 % des offres d'emploi dans le domaine de la cybersécurité industrielle ont été publiées par des cabinets d'ingénierie-R&D. Avec 26 % des offres publiées sur ce segment, les entreprises du secteur informatique constituent les plus grands pourvoyeurs d'offres, loin devant les entreprises de l'industrie qui, dans leur ensemble, représentent 16 % des recruteurs. Des offres ont également été émises par des sociétés de conseil et gestion des entreprises ainsi que par des cabinets de recrutement pour lesquels le client final est difficilement identifiable. Ceux-ci représentent à eux deux, 20 % des offres diffusées sur la période 2016-2017 (figure 3). Aussi, près de sept candidats sur dix relèvent des métiers de l'ingénierie systèmes, réseaux et données ainsi que des métiers de l'informatique industrielle, de l'ingénierie en informatique électronique ou embarquée.

– Figure 3 –
Principaux émetteurs d'offres en cybersécurité industrielle publiées par l'Apec sur la période 2016-2017



Source : Apec, 2018

L'ÎLE-DE-FRANCE DRAINE PRÈS DE LA MOITIÉ DES OFFRES D'EMPLOI

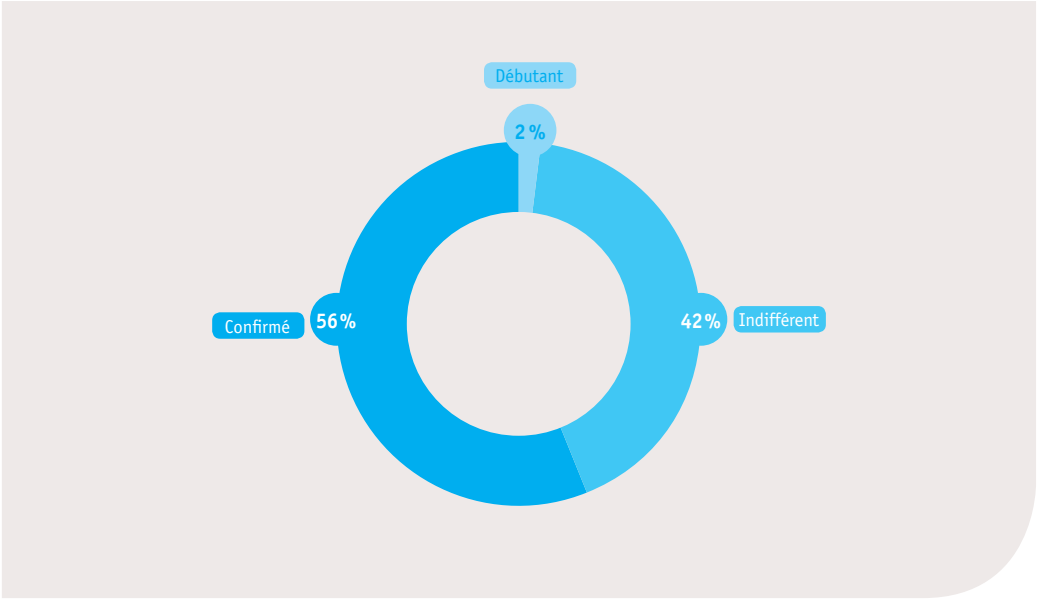
En matière de distribution géographique, les entreprises franciliennes représentent sur les années 2016-2017, 47 % des diffuseurs d'offres. Les structures implantées en Auvergne –Rhône-Alpes et en Provence-Alpes-Côte d'Azur représentent chacune 14 % des pourvoyeurs d'offres, et celles situées en Occitanie, 11 %. Cette distribution est moins le reflet de la place qu'occupe l'industrie au sein des différents territoires, que de la métropolisation de certaines activités de services : cabinets d'ingénierie, entreprises de services du numérique (ESN), sociétés de conseil[7].

PLUS DE LA MOITIÉ DES OFFRES S'ADRESSENT À DES CANDIDATS CONFIRMÉS

En 2016, 56 % des entreprises ayant ouvert des postes dans le champ de la cybersécurité industrielle s'adressent à des candidats confirmés dans le domaine (figure 4). Les ingénieurs et autres candidats de niveau Bac +5 et plus sont également fort prisés des recruteurs. Des acquis dans le champ de l'informatique industrielle peuvent être exigés pour certains postes, ainsi que des certifications dans le domaine de la cybersécurité.

7. *Cartographie et analyse territoriale des offres d'emploi cadre par secteur*, Apec, 2017, n°39.

– Figure 4–
Niveaux d'expérience recherchés par les recruteurs en sur la période 2016-2017



Source : Apec, 2018

–LES COMPÉTENCES RECHERCHÉES–

DES PROFILS MIXTES

En matière de cybersécurité industrielle, plusieurs types de profils peuvent être recherchés par les entreprises : développeurs de logiciels, architectes, consultants… Des profils pour lesquels des compétences en cryptologie et implémentation d'autres mécanismes de sécurité, en diagnostic et analyse de risques sont très souvent requis.
Mais, appliquées aux installations et process industriels, celles-ci ne suffisent pas. Les candidats sont attendus sur leur maîtrise des automates et systèmes de contrôle-commande programmables (Siemens, Schneider, Rockwell, etc.), des solutions embarquées, des objets connectés, des interfaces hommes-machines, etc.

« Il ne faut pas uniquement des compétences en SI (systèmes d'information), car un ingénieur SI ne connait pas forcément des outils tels que Scada qui permettent de contrôler à distance des installations techniques. » (Expert).

Aussi, les automaticiens qui sont montés en compétences dans le domaine de la cybersécurité représentent des profils intéressants pour les recruteurs car ils possèdent une expertise que d'autres spécialistes de l'informatique ne possèdent pas. Ils ont la maîtrise de la chaîne de production et sont sensibles aux impacts que pourrait entraîner une interruption ou un ralentissement de service suite à une attaque et/ou à une opération de sécurisation.

INGÉNIEUR SÉCURITÉ ET CRYPTOGRAPHIE - INDUSTRIAL IOT H/F

Émetteur de l'offre d'emploi : Activité informatique (Île-de-France).

Missions Rattaché à la Direction Recherche & développement (40 personnes), vous intégrez l'équipe Innovation (10 personnes) et serez impliqué dans des projets de recherche et innovation sur la sécurité de l'IoT. Les systèmes de contrôle industriel ICS/SCADA gèrent les infrastructures critiques de la société, depuis les réseaux électriques au traitement de l'eau, de l'industrie chimique aux transports. Avec la généralisation des interconnexions de réseaux, les télémaintenances et l'utilisation d'Internet, et avec la convergence OT/IT, les risques sont devenus très élevés et les enjeux immenses en termes de cybersécurité. Au sein de ce pôle, vous participerez à nos projets sur la **cybersécurité des systèmes industriels**, en particulier sur les réseaux de distribution électrique. Dans le cadre de ces projets, le client développe une nouvelle offre de service PKI (Public Key Infrastructure) visant à sécuriser les systèmes industriels depuis le réseau intranet de l'entreprise jusqu'au système terrain. Le poste consiste à : spécifier et concevoir les architectures de sécurité ; développer et valider les briques logicielles « sécurité » ; assurer une veille et identifier les technologies émergentes ; contribuer aux instances de normalisation/standardisation ; accompagner les équipes commerciale/marketing pour identifier de nouveaux besoins clients.

Profil Ingénieur(e) généraliste ou docteur en cryptographie/sécurité, vous avez au moins 5 ans d'expérience. Vous avez acquis une expertise en sécurité et cryptographie (protocoles PKI, X.509, RSA, ECDSA, HSM ...), ainsi qu'une bonne connaissance en développement logiciel (Java/JEE, C). La connaissance des systèmes industriels (SCADA, Automates) et/ou embarqués (RTOS) serait un plus, ainsi que la connaissance des vulnérabilités propres à ces systèmes. L'esprit d'initiative, des capacités d'analyse et de rédaction, ainsi qu'une bonne maîtrise de l'anglais sont des éléments indispensables pour ce poste. Des déplacements ponctuels sont à prévoir en fonction des besoins projets ou pour assister à des conférences.

Source : Apec.fr

ARCHITECTE CYBER-SECURITÉ INDUSTRIELLE H/F

Émetteur de l'offre d'emploi : Entreprise de services numériques (Provence-Alpes Côte d'Azur).

Missions Vous intégrez un de nos centres d'expertise sécurité sur l'Ile de France, Grenoble, Lyon, Toulouse ou Aix-Marseille pour y réaliser des missions d'architecte sécurité auprès de nos clients pour concevoir l'architecture de cybersécurité et les mesures de protections de leurs produits et/ou SI industriels.

Profil Conception d'architectures de sécurité et audit d'architecture. Analyse de risque (MEHARI, EBIOS, ...). Normes et standards (ISO27001, ISO27005, RGS, IEC62443, Critères Communs ...). Réseaux: protocoles IP classiques (ex: https, ftps), protocoles IP spécifiques (ex : ModBus over Ethernet) ou protocoles non IP (ex : Bus CAN, protocole RF propriétaire). Sécurité des systèmes et OS (durcissement). SDLC (Secure Development Life Cycle). Maîtrise des techniques de protection (cryptographie, PKI, HSM ...). Une connaissance des systèmes industriels (SCADA, Automates) et/ou embarqués (RTOS) serait appréciée, ainsi que la connaissance des vulnérabilités propres à ces systèmes. Vous avez de l'expérience en cybersécurité dans un ou plusieurs secteurs industriels. Junior, confirmé ou expert, avec une forte appétence pour la cybersécurité des produits ou des SI industriels, rejoignez-nous !

Source : Apec.fr

GOÛT POUR L'INNOVATION ET DISCRÉTION SONT REQUISES DANS CES MÉTIERS

Au-delà des compétences techniques requises, les recruteurs ont des exigences en matière de savoir-être. Leurs recherches ciblent des profils à l'écoute des nouvelles technologies qui se déploient dans la sphère industrielle (solutions numériques, objets connectés...). Dans certaines entreprises positionnées sur des secteurs dits vitaux (énergie, défense, télécommunications...), des attendus forts sont exprimés en matière de confidentialité et certains établissements exigent des habilitations défense ou diligentent des enquêtes administratives avant recrutement.

Ces process peuvent ou non être spécifiées dans le contenu des offres publiées.

« Poste basé sur un établissement soumis à une enquête administrative. »

En complément, la rigueur et de fortes capacités analytiques sont également posées comme des aptitudes essentielles pour être recruté dans ce domaine.

–PRINCIPAUX DÉFIS RH–

Sur le segment de la cybersécurité industrielle, le marché de l'emploi est souvent décrit comme tendu et pénurique. L'accroissement des besoins en recrutement n'est pas le seul facteur explicatif de cette tension. Deux autres éléments rentrent en jeu.

Le premier est lié à la nécessité, de trouver des profils habilités « Confidentiel Défense » ou « Secret Défense ». L'habilitation délivrée par le ministère de la Défense, est un processus long et que les entreprises estiment méconnu des jeunes diplômés. De sorte qu'à la sortie d'une école d'ingénieurs, tous ne sont pas dans une situation favorable pour accéder à des postes en cybersécurité, surtout s'ils n'ont pas la nationalité française et qu'ils ne peuvent donc prétendre à l'habilitation[8]. Quant aux experts en cybersécurité qui possèdent ces habilitations, ils ne peuvent pas en faire mention hors entretien d'embauche. D'où la difficulté pour les recruteurs de les identifier comme des candidats potentiels, à moins de passer par leur réseau de connaissances ou la cooptation.

Ce sont là d'ailleurs des modes de *sourcing* très souvent utilisés dans le champ de la cybersécurité, au même titre que la chasse de profils déjà en poste. Cependant, pour les petites structures, il peut s'agir d'une démarche trop coûteuse pour être engagée.

Le manque de candidatures répondant aux besoins réels des entreprise et le peu de formation en cybsersécurité industrielle, sont également mis en avant pour expliquer le côté pénurique du marché. Cette pénurie est telle qu'elle pousse les entreprises à renoncer à recruter en externe et à préférer le développement de solutions en interne. C'est typiquement le cas pour les métiers de développeurs pour lesquels les recrutements sont déjà difficiles hors champ de la cybersécurité.

« Même nos clients abandonnent parfois sur ce type de profil. Pourtant s'il y avait 100 % de profils disponibles sur le marché, je pourrais les recruter, j'aurais des projets pour eux. » (Recruteur).

La montée en compétences de salariés est alors souvent priorisée et portée vers les automaticiens qui possèdent l'avantage de bien connaître le monde de l'industrie.

« Quelqu'un qui a une expérience dans la sécurisation des systèmes d'information dans le milieu bancaire par exemple ne sera pas forcément un bon candidat pour nous. » (Recruteur).

Face à la multiplication des menaces, il y a tout à la fois un impératif et une urgence pour les entreprises de développer des solutions en ce sens.

« Cinq ans d'expérience sont nécessaires pour avoir des profils d'experts dans ce domaine. Mais cinq ans, c'est trop tard par rapport aux besoins et aux enjeux. Du coup, on fait de la montée en compétences de développeurs en informatique industrielle. » (Expert).

À noter que la montée en compétences des collaborateurs n'est pas le seul défi RH qui attend les industriels à la recherche de profils en cybersécurité. Des actions de sensibilisation des collaborateurs aux bonnes pratiques d'hygiène d'informatique industrielles sont aussi impératives à mener, étant entendu que dans de nombreux cas, ce sont les salariés eux-mêmes qui rendent leurs systèmes d'information et de contrôle perméables aux cyberattaques. D'où aussi des besoins de profils permettant de vulgariser et de systématiser ces messages.
De fait, une augmentation du nombre d'offres d'emploi en cybersécurité industrielle pourrait être attendue dans les années à venir.

8. L'Anssi stipule que « en application de l'article 5 du décret n°2014-364 du 21 mars 2014 modifiant le décret n°86-83 du 17 janvier 1986 relatif aux dispositions générales applicables aux agents non titulaires de l'État pris pour l'application de l'article 7 de la loi n°84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'État, les agents contractuels de nationalité étrangère ou apatrides ne peuvent être recrutés pour pourvoir des emplois dont les attributions soit ne sont pas séparables de l'exercice de la souveraineté, soit comportent une participation directe ou indirecte à l'exercice de prérogatives de puissance publique ».

MÉTHODOLOGIE

Cette note prend appui sur l'exploitation quantitative des offres publiées en 2016 et 2017 sur Apec.fr dans le champ de la cybersécurité industrielle. Une sélection exhaustive a été lancée à partir des champs de requête suivants : 1/mots-clés : « cybersécurité », « cyberattaques. » - 2/secteur d'activité émetteur : entreprises relevant du domaine de l'industrie, des services de l'ingénierie-R&D et de l'informatique. Toutes les offres d'emploi citées ici à titre illustratif sont extraites de ce cahier d'offres. En complément de cette analyse, des entreprises ayant publié des offres en 2017 ainsi que des experts du domaine ont été interrogés. Ces entretiens, associés à une recherche documentaire, ont permis d'apporter un éclairage contextuel sur cette technologie, et d'en analyser les grandes tendances en termes de marché.

LE PROJET DÉFI&CO

Le projet DEFI&Co *(développer l'expertise future pour l'industrie et la construction)**, piloté par CESI et soutenu par le programme Investissements d'Avenir, vise à construire des contenus de formation adaptés aux transformations en cours dans l'industrie et la construction. Dans le cadre de ce projet et sur une durée de cinq ans (2017-2021), l'Apec va réaliser chaque année une revue des tendances liées à l'usine du futur et au bâtiment du futur ayant un impact potentiel fort en matière d'évolution des compétences et des métiers pour les cadres. Ce document consacré à la **cybersécurité industrielle** s'inscrit dans la revue des tendances 2018. D'autres documents sont disponibles sur les thèmes de l'**intelligence artificielle**, de la **cobotique**, de la **simulation numérique**, de la r**éalité virtuelle/réalité augmentée**, du **bâtiment intelligent**. Un dernier document est consacré à l'opinion des cadres de l'industrie et du bâtiment concernant l'impact des nouvelles technologies sur leur métier.

*Le projet DEFI&Co a été retenu dans le cadre de l'appel à projets « Partenariats pour la formation professionnelle et l'emploi » du programme Investissements d'Avenir. Le projet regroupe 34 partenaires dont on peut retrouver la liste à cette adresse : https://recherche.cesi.fr/projets/defico/

Toutes les études de l'Apec sont disponibles gratuitement sur le site **www.cadres.apec.fr > rubrique *Observatoire de l'emploi***

www.apec.fr

ISSN 2557-6283
SEPTEMBRE 2018

Cette étude a été réalisée par la Direction Données, Études et Analyses (DDEA) de l'Apec.
Analyse et rédaction : Caroline Legrand.
Direction de l'étude : Gaël Bouron.
Direction de la DDEA : Pierre Lamblin.

Maquette : Ludovic Bouliol.

ASSOCIATION POUR L'EMPLOI DES CADRES
51 BOULEVARD BRUNE – 75689 PARIS CEDEX 14

CENTRE DE RELATIONS CLIENTS
0 809 361 212 Service gratuit + prix appel
DU LUNDI AU VENDREDI DE 9H À 19H
*prix d'un appel local

EDOBSA0257-I/CYB-09.18