RAPPORT D'ETUDE

« Les formations et les compétences en France sur la cybersécurité »

Mai 2017

Cette étude a été réalisée par le cabinet EY pour le compte de l'OPIIEC.

Préambule

L'étude « Formations et compétences en France sur la cybersécurité » a été réalisée par le cabinet EY pour le compte de l'Observatoire Paritaire de l'Informatique, de l'Ingénierie, des Etudes et du Conseil (OPIIEC).

Elle a été initiée suite à une commande de la Commission Paritaire Nationale de l'Emploi et de la Formation Professionnelle (CPNEFP) de la branche des métiers de l'Ingénierie, du Numérique, des Eudes et du Conseil, et des métiers de l'Evènement, ci-après dénommée la Branche.

Les auteurs remercient les membres du comité de pilotage paritaire de l'OPIIEC, ainsi que les représentants du panel d'entreprises listées en Annexe 1, dont certains ont souhaité rester anonymes, et qui ont accepté de partager leur expérience, leur pratique, leurs préconisations et leur vision sur la cybersécurité. Ces échanges ont été extrêmement précieux pour la préparation de la présente étude.

Table des matières

Contexte et enjeux de l'étude

La Branche est constituée de près de 60 000 entreprises adhérentes, représentant environ 750 000 emplois. Ces entreprises présentent une forte diversité tant en termes de taille (de très grands groupes mais aussi de nombreuses PME, plus de 50 000 entreprises ont moins de 2 emplois) qu'en termes d'activités adressées (secteur de l'énergie, de l'immobilier et de la construction, de la distribution, du commerce en ligne…).

Cette étude a pour objectif d'apporter un éclairage sur le besoin des entreprises de la Branche en termes d'effectifs spécialisés en cybersécurité et d'aiguiller la politique de la formation de la Branche pour construire une offre adaptée. Une approche qualitative et quantitative des métiers de la cybersécurité devra constituer un atout pour la précision et la mise à jour des référentiels existants.

LES 4 SECTEURS COMPOSANT LA BRANCHE

La cybersécurité est une discipline définie par l'Agence Nationale de la Sécurité des Systèmes d'Information comme :

> *État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.*
> *La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.*

En 2014, le premier ministre français déclarait que la cybersécurité « est une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement »[1]. En effet, la cybersécurité présente des enjeux économiques, stratégiques et politiques qui vont donc bien au-delà de la seule sécurité des systèmes d'information. Elle concerne aussi bien l'informatique de gestion, l'informatique industrielle, l'informatique embarquée que les objets connectés. Ainsi, toutes les entreprises, à différents degrés, sont concernées par la sécurité de leur système et pourront faire appels à des fournisseurs de technologies (logiciels, matériels…) et des prestataires de services.

La cybersécurité constitue donc un enjeu majeur pour les entreprises, et notamment pour les entreprises de la Branche. C'est pourquoi cette étude vise à renforcer les formations et les compétences requises en cybersécurité.

[1] Discours de Jean-Marc Ayrault, alors Premier ministre, le 21 février 2014 à l'ANSSI

La cybersécurité est un domaine confronté à des enjeux qu'il convient d'aborder à travers cette étude pour les entreprises de la Branche :

- Enjeux liés à l'évolution des métiers dans le numérique : le besoin en compétences dans le domaine de la cybersécurité est crucial avec le développement du Cloud Computing, Internet des Objets (IoT), Analytics, Big Data, des plateformes multi-canaux ;
- Enjeux liés à la complexité de la cybersécurité avec une multitude de métiers : être en capacité d'identifier les différents métiers en cybersécurité (management, opérationnel et expertise technique) afin de s'adapter aux nouvelles approches de la cybersécurité ;
- Enjeux liés à la valorisation des compétences en cybersécurité : sensibiliser et promouvoir les compétences attendues en cybersécurité afin de disposer d'équipes cybersécurité performantes et d'assurer l'attractivité de la filière ;
- Enjeux liés à la transformation de l'offre formation : être en capacité de proposer des évolutions à l'offre actuelle pour combler la pénurie actuelle de ressources en cybersécurité et accroitre le champ des compétences de la filière cybersécurité ;
- Etablir un plan d'actions pour mieux répondre aux attentes et aux besoins des entreprises en métiers et en compétences cybersécurité.

Dans ce contexte, cette étude vise à identifier les marges de progrès à réaliser pour faire coïncider l'offre de formation française (initiale et continue) et les besoins en recrutement et en compétences (en les chiffrant) des professionnels de la cybersécurité, à court, moyen terme et long terme, afin d'assurer une grande employabilité aux apprenants en France qui se destineraient à ce secteur, ainsi qu'aux professionnels en activité.

Les principaux objectifs de l'étude sont les suivants :

- Faire un état des lieux qualitatif et quantitatif des besoins en recrutement et en compétences dans les entreprises de la Branche, le tout selon les catégories de métiers,
- Effectuer un bilan qualitatif et quantitatif des compétences attendues par les entreprises de la Branche en matière de cybersécurité à court et moyen terme,
- Evaluer l'offre de formation initiale et continue existante en France notamment dans l'enseignement supérieur,
- Mettre en perspective les compétences attendues avec l'offre de formation initiale et continue actuelle et son développement prévisionnel sur 3, 5 et 8 ans,
- Mesurer les impacts sur les emplois existants et les organisations (évolutions législatives et réglementaires : CNIL, ANSSI…)

Cette étude, en cours, est conduite en trois phases :

1. L'analyse des besoins en recrutement et compétences
2. L'état des lieux de l'offre de formation
3. Des préconisations et un plan d'actions

Démarche méthodologique

a. Périmètre de l'étude

Le périmètre de l'étude recouvre l'ensemble des entreprises composant la Branche : les secteurs du numérique, de l'ingénierie, des études et du conseil, et de l'évènement.

Les entreprises de la Branche présentent une variété importante de sensibilité à la cybersécurité, celle-ci pouvant être au cœur de l'offre de services d'une entreprise, ou bien une fonction support plus ou moins intégrée dans la stratégie de l'entreprise. Ces différents degrés d'intervention et de sensibilisation sont inclus dans l'étude.

Par ailleurs, les évolutions des métiers de la cybersécurité et des réglementations sont étudiées et analysées à l'échelle nationale.

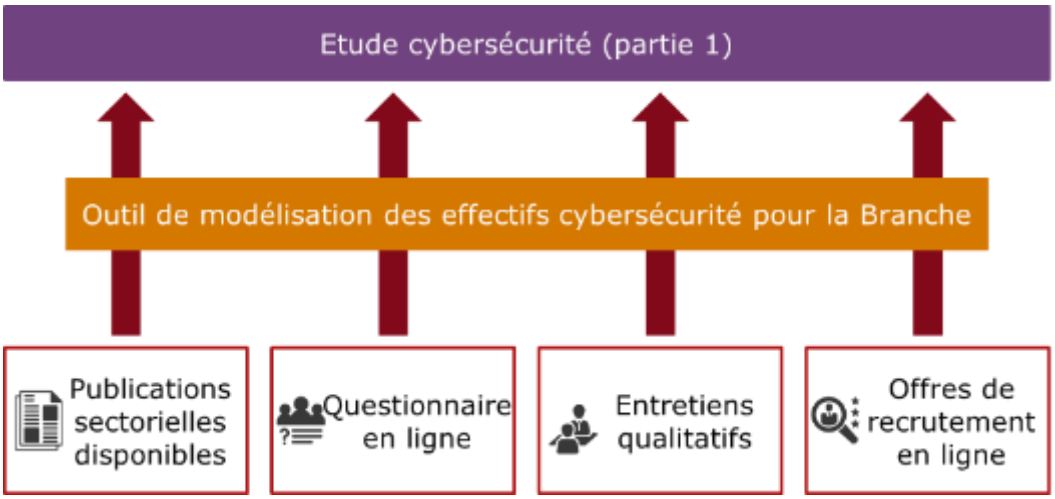
b. Présentation de la méthodologie – Phase 1

Cette phase a pour objectif d'effectuer une analyse des besoins des entreprises en matière de cybersécurité (métiers et compétences) actuels et à venir compte tenu de l'évolution de la cybersécurité, des pratiques de recrutement et de la réglementation.

Afin de répondre aux objectifs de la phase 1 constitutive de cette étude au sein de la Branche, la méthodologie repose sur plusieurs briques d'analyse :

- La revue des publications sectorielles
- L'établissement et l'exploitation d'un questionnaire en ligne auprès d'entreprises de la Branche
- La conduite d'entretiens qualitatifs
- Le relevé des offres d'emplois en cybersécurité

Ces quatre briques ont permis la construction d'un outil de modélisation, à la base de l'exercice de quantification des emplois et des prévisions de recrutement.



SCHEMA RECAPITULATIF DE LA METHODOLOGIE – PHASE 1

❖ *Revue des publications sectorielles*

Une revue de la littérature sur la cybersécurité a été réalisée. Les études sectorielles, textes de réglementation en termes de cybersécurité et publications par les principaux acteurs du secteur ont permis d'alimenter au fur et à mesure le présent rapport.

Cette revue a été conduite sur un périmètre élargi (Branche, France, à l'étranger…), permettant d'apprécier les tendances globales en cybersécurité pour les acteurs économiques français et internationaux.

Une bibliographie est détaillée en Annexe 2.

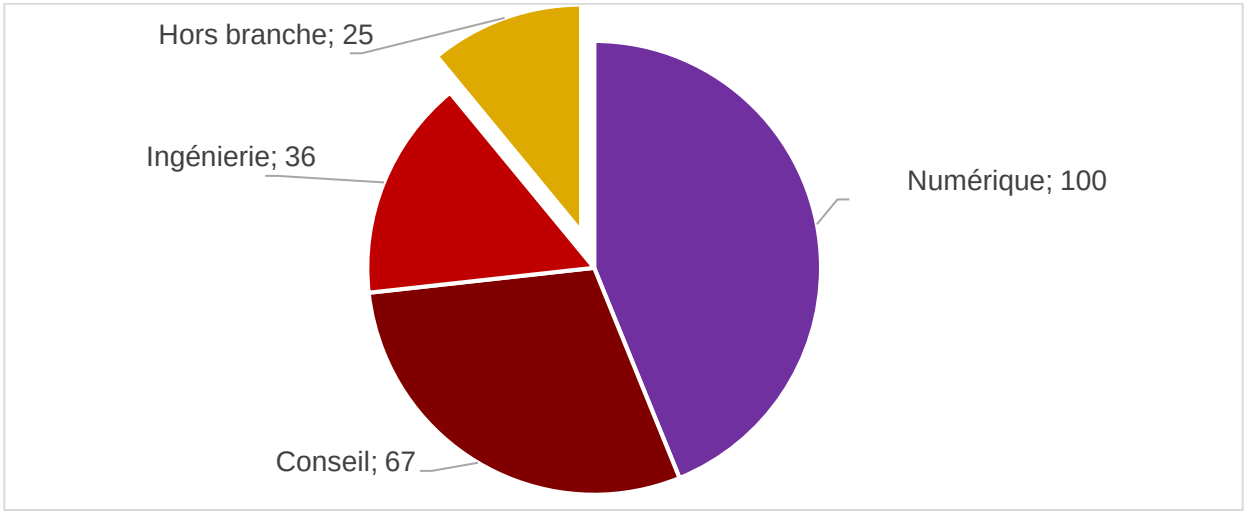
❖ *Questionnaire en ligne*

Sur la base de la méthodologie prévue en amont et validée par le comité de pilotage de l'étude, un questionnaire en ligne a été administré à des entreprises. Plus de 20 000 entreprises de la branche ont été sollicitées : des entreprises « hors branches » ont été intégrées à l'échantillon afin de mettre en perspective les spécificités des besoins et des enjeux des acteurs de la branche.

Ce questionnaire, articulé autour de 23 questions, vise à collecter le point de vue des entreprises sur :

- Leurs effectifs actuels en cybersécurité et les métiers représentés
- L'évolution à venir des effectifs, les recrutements à venir
- Le niveau de sensibilisation de l'entreprise aux problématiques cybersécurité
- Les compétences recherchées en cybersécurité (aujourd'hui et à horizon 5 ans)
- L'offre de formation et son adéquation avec leurs besoins

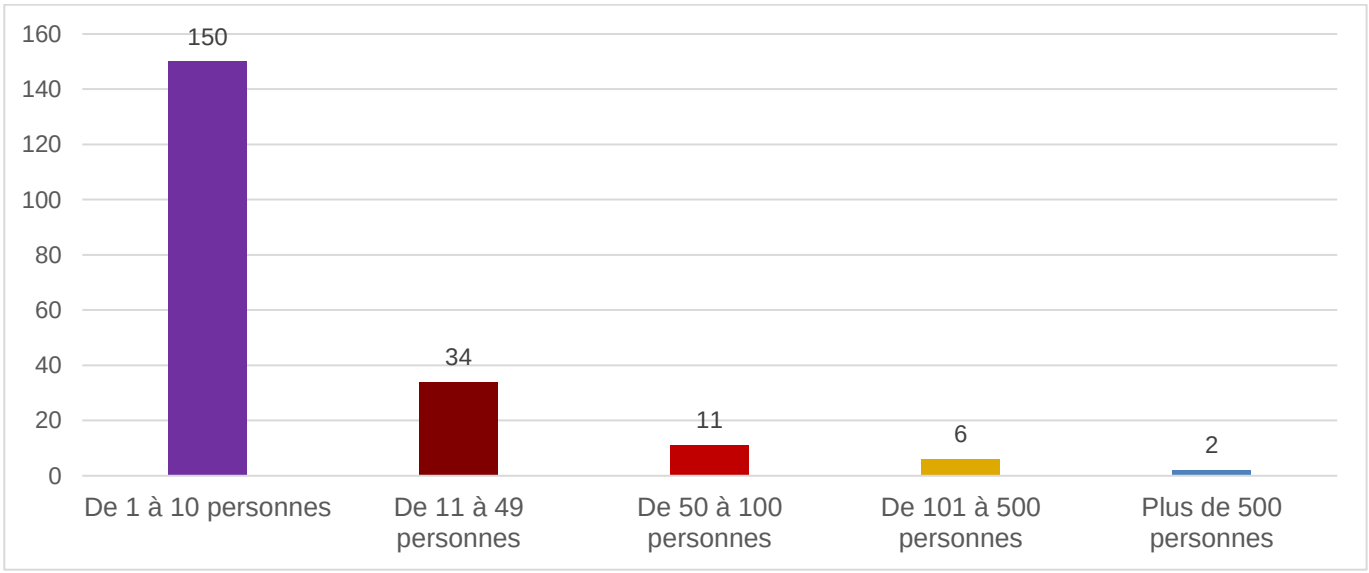
Le questionnaire complet est présenté en Annexe 3 du présent document. Mise en ligne du 12 décembre 2016 au 12 janvier 2017, il a reçu 227 réponses.



TYPOLOGIE DES ENTREPRISES AYANT REPONDU AU QUESTIONNAIRE

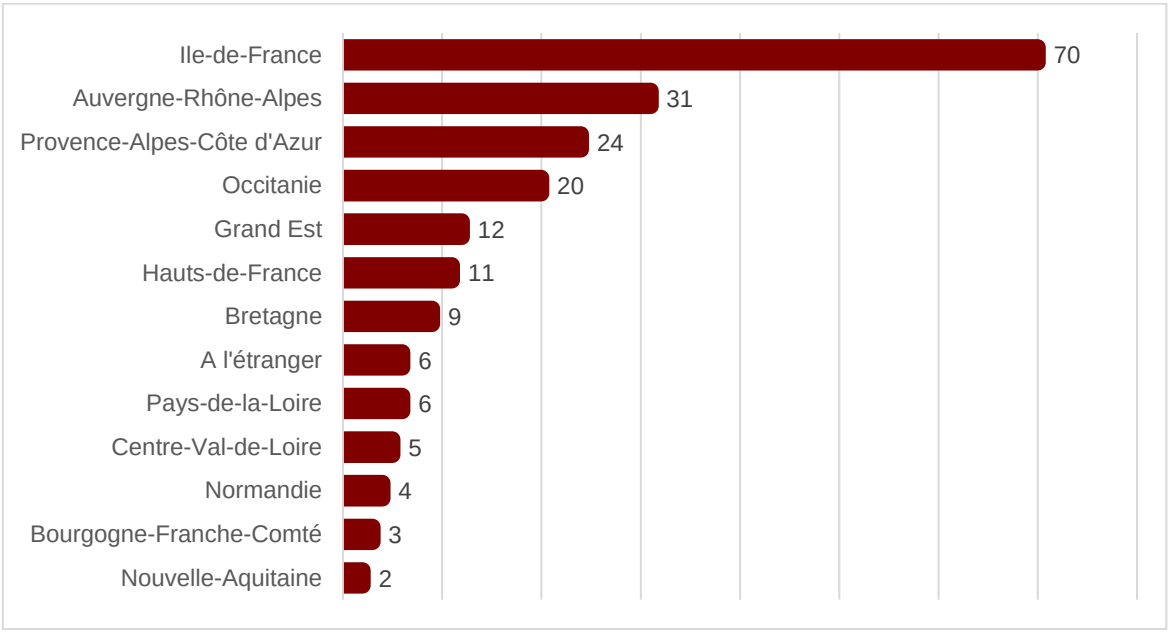
Les entreprises hors branche ayant répondu sont principalement des secteurs suivants : industrie (7) ; banque, finance, assurance (3) ; administration (2) ; Conseil (2) ; Média/presse (2) ; Services aux entreprises (2).

Plus de 200 entreprises de la Branche ont répondu, avec une forte représentation du secteur du numérique et du conseil. Le panel de répondants reflète la répartition sectorielle des entreprises de la Branche. Par ailleurs, 25 entreprises hors branche ont répondu : ces réponses complémentaires ont été prises en compte pour les aspects qualitatifs à titre de points de comparaison, mais sont exclues des analyses quantitatives du rapport.



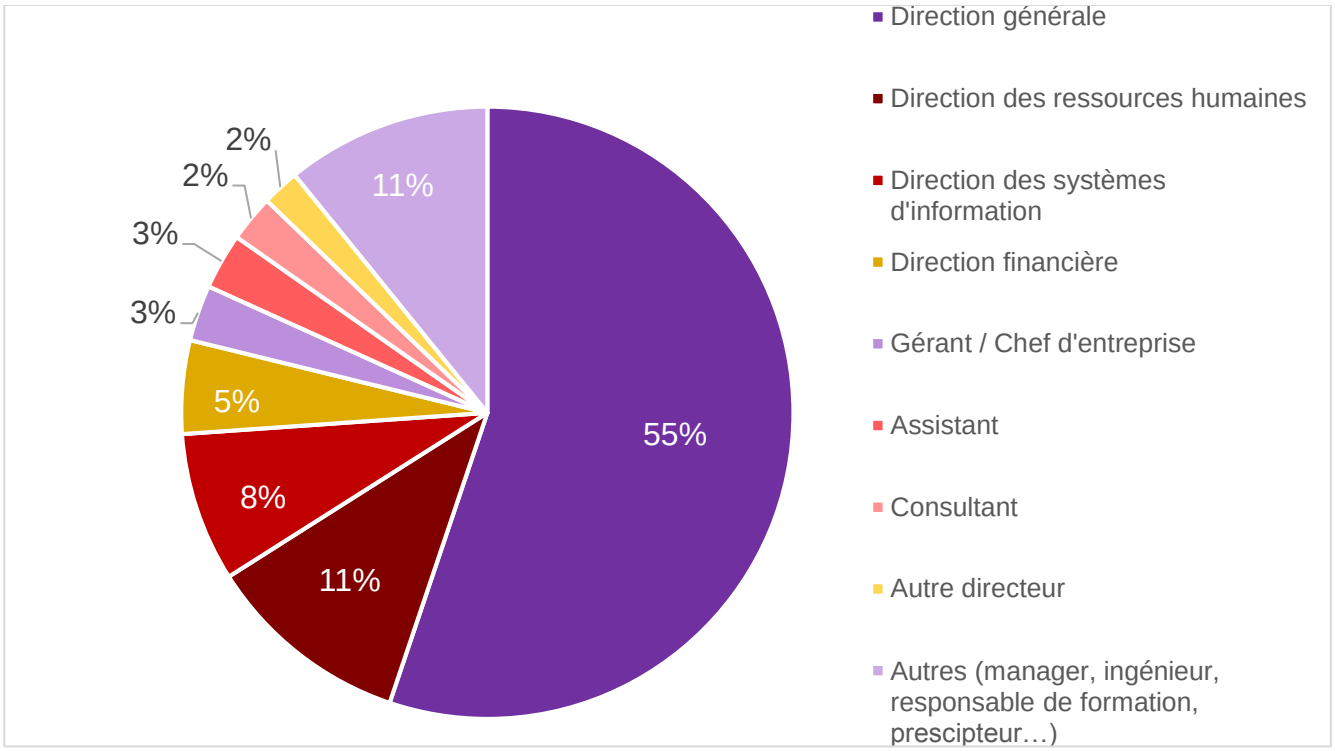
REPARTITION DES ENTREPRISES DE LA BRANCHE AYANT REPONDU EN FONCTION DE LEUR TAILLE

Une très forte majorité des réponses a été faite par des entreprises de la branche de moins de 10 personnes. La prédominance de ces TPE-PME répond à une structure similaire de l'ensemble des entreprises composant la Branche, tous secteurs confondus.



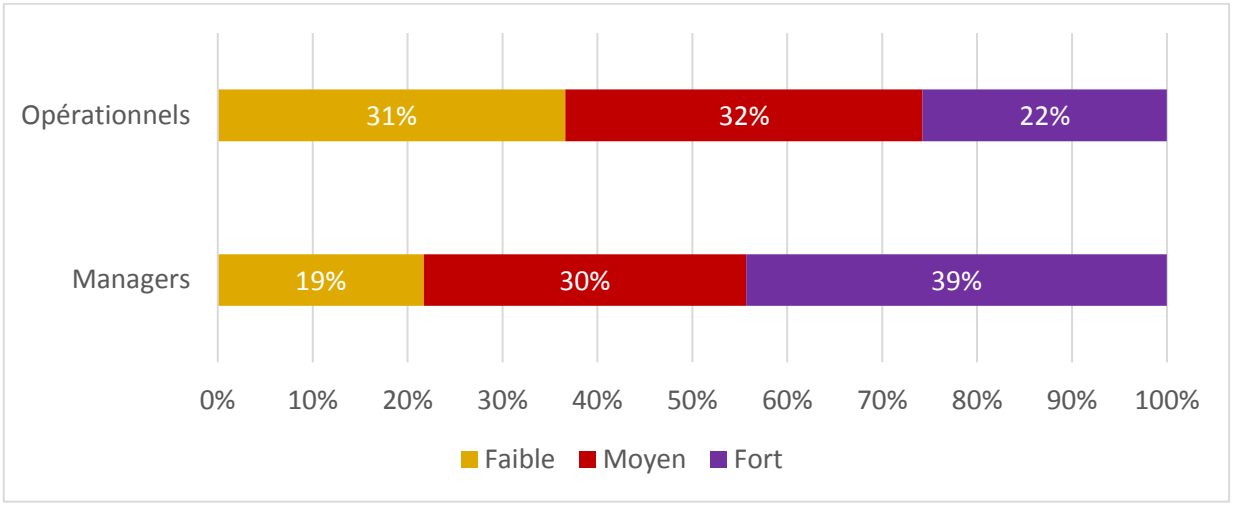
REPARTITION GEOGRAPHIQUE DES EQUIPES CYBERSECURITE

Un grand nombre de réponses provient d'entreprises ayant leur siège et/ou leurs équipes cybersécurité dans la région Ile de France.



FONCTIONS DES REPONDANTS POUR LES ENTREPRISES DE LA BRANCHE

Les répondants sont principalement des cadres dirigeants, voire des professionnels plus directement concernés par la cybersécurité, par exemple avec les directeurs des systèmes d'information.



NIVEAU DE SENSIBILITE DES ENTREPRISES DE LA BRANCHE A LA CYBERSECURITE

Les entreprises se sont exprimées sur leur niveau de sensibilisation à la cybersécurité pour les fonctions opérationnelles et pour les fonctions managériales. Au-delà du fait que les fonctions managériales sont souvent sensibilisés à un niveau plus fort que les opérationnels, on observe des situations très différentes entre des entreprises parfois très peu sensibilisées à tout niveau jusqu'à des degrés de très forte appréhension de cette thématique. Cette approche met en lumière un niveau de maturité très différent d'une entreprise à l'autre.

❖ *Entretiens qualitatifs*

L'approche quantitative menée par l'enquête en ligne a été complétée par la conduite d'entretiens qualitatifs auprès d'entreprises de la Branche. Au total, 17 entretiens individuels et collectifs ont été menés (12 auprès d'entreprises de la Branche, 5 hors Branche).

Les premiers entretiens ont permis de tester et consolider la liste des métiers et des compétences en cybersécurité. Puis, à un stade plus avancé de l'étude, les entretiens ont permis d'affiner les analyses de l'enquête en ligne par une approche qualitative détaillée.

Ci-dessous les principales entreprises rencontrées lors de la phase 1 de cette étude :

Microsoft, IBM, Sogeti, Accenture, Orange Cyberdéfense, Sekoia, Beijaflore, Société Générale, Sanofi, Informatique CDC, etc.

Le panel d'entreprises listées figure en Annexe 1

❖ *Analyse des annonces d'emplois en ligne*

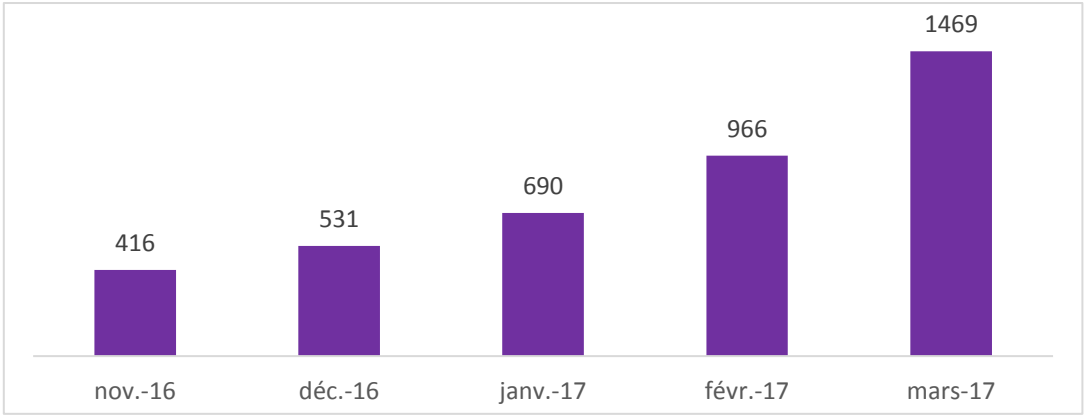
Afin d'alimenter le modèle quantitatif en ce qui concerne l'évolution des besoins, les perspectives de recrutement et la géolocalisation des offres, les offres d'emplois en ligne sur les sites faisant référence dans le domaine de la cybersécurité ont été consultées.

Cette analyse quantitative des annonces a été menée auprès de 5 sites ou cabinet de recrutement, allant des sites généralistes aux sites spécialisés dans la cybersécurité.

Sites de recherche d'emplois en ligne	
Généralistes	spécialisés
LinkedIn, Apec, monster	ADEPTIS, Yes We Hack!

Cette revue n'est pas exhaustive de l'ensemble des offres disponibles en cybersécurité, néanmoins elle se veut illustrative des besoins immédiats des entreprises. La démarche consiste à rechercher les profils les plus demandés sur le marché français, et d'identifier un « top 10 » des profils les plus recherchés. Ces recherches couvrent les annonces d'emplois de type CDD et CDI, en excluant les nombreuses annonces de stages et d'alternances.

Cette revue a été conduite tous les mois pendant la durée de l'étude afin d'apprécier une éventuelle évolution des tendances de recrutement ou une confirmation des besoins ciblés sur une poignée de métiers. A ce titre, ont été recensées plus de 4 000 annonces entre novembre 2016 et mars 2017.



ANALYSE DE PLUS DE 4 000 ANNONCES EN LIGNE D'EMPLOIS EN CYBERSECURITE[2]

[2] Revue EY des sites de recherche d'emplois en ligne : LinkedIn, Apec, Monster, Adeptis, YesWeHack

❖ *Modélisation des effectifs en cybersécurité au sein des entreprises de la Branche*

L'exercice de quantification des effectifs en cybersécurité a été réalisé pour les entreprises de la Branche. Ce travail repose sur la base de données des entreprises appartenant à la Branche (données Fafiec 2016). Les entreprises ne renseignant aucun emploi ont été exclues de la modélisation.

Les entreprises de la branche peuvent être regroupées en quatre catégories, selon leurs activités

- Utilisateur stratégique
- Utilisateur peu sensible
- Prestataire généraliste avec une activité cybersécurité
- Prestataire « pure player » cybersécurité

Chaque entreprise a donc été répartie dans ces catégories en fonction de plusieurs éléments :

- L'activité renseignée via les codes NAF de la Branche[3], permettant une première approche « macro » pour isoler les entreprises « utilisatrices ».
- Les bases de données et l'expertise EY sur l'identification précise notamment des pures players en cybersécurité et des prestataires de services avec une activité en cybersécurité
- Une revue documentaire et la conduite d'entretiens auprès d'entreprises pour qualifier la part des effectifs en cybersécurité ou l'estimer par le chiffre d'affaire réalisé par les pure players.

Un deuxième traitement plus fin a été réalisé, à partir de l'expertise interne EY, des entretiens qualitatifs et d'une revue documentaire afin de contrôler la répartition de chaque entreprise dans la catégorie la plus pertinente.

L'évaluation des effectifs cybersécurité pour chaque catégorie d'entreprise a été estimée à partir :

- Des effectifs et prévisions de recrutement issues de l'enquête en ligne
- De données sur les effectifs en cybersécurité au sein d'un panel d'entreprises (données collectées par EY auprès de son réseau de partenaires et de clients)

Les données sur les effectifs et les recrutements issues des échantillons d'entreprises ont été classées :

- Par catégorie d'entreprise (utilisateur stratégique – entreprise pour laquelle la cybersécurité est stratégique- , utilisateur moins sensible, prestataire généraliste avec activité cyber, pure player cyber)
- Par taille d'entreprise
- Par famille de métiers cybersécurité.

Cette modélisation a permis d'estimer, pour chaque famille, les effectifs dans les entreprises de la branche.

Les prévisions de recrutement à 3 et 5 ans ont été estimées à partir du même modèle en intégrant :

- Les évolutions de croissance économique des entreprises de la branche, et en particulier de la cybersécurité
- Des données issues de l'enquête en ligne sur les projections d'effectifs
- Les entretiens qualitatifs avec des experts et DRH de la filière
- L'analyse des documents de prospective réalisés à l'international sur l'évolution des effectifs dans la cybersécurité.

[3] Liste des codes NAF de référence pour la Branche en Annexe 4

c. Présentation de la méthodologie – Phase 2

La cartographie des formations initiales et continues a été construite selon les étapes suivantes :

- 10 entretiens qualitatifs avec des responsables de formation et des experts du secteur (ANSSI)
- Collecte extensive de données sur les sites des organismes de formations initiales et continues
- Consultation des sites consolidant les offres de formation : Onisep, réseau inter-Carif oref, Commission Nationale de la Certification Professionnelle (CNCP)
- Analyse documentaire des plaquettes de formation des sites de formation continue
- Organisation d'un atelier de travail avec des experts et des professionnels du secteur

Zoom méthodologique sur la cartographie de l'offre de formation « longue »

Une cartographie de l'offre de formation en cybersécurité soulève plusieurs questions :

- Quels sont les niveaux des formations à cartographier ?

Cette réflexion a été abordée notamment avec les établissements de formation lors d'un atelier. Il a été retenu de cartographier les formations de niveau Bac+3 à Bac+5, en raison de leur cohérence avec la réforme LMD Licence-Master-Doctorat et de leur représentation de la majorité des formations dédiées en cybersécurité. Ainsi, ne sont pas cartographiées dans ce présent rapport les formations de niveaux bac+2 ou au-delà de Bac+5. Ces formations correspondront à des cas particuliers : un niveau Bac+2 peut parfois être suffisant pour atteindre des postes d'administrateur sécurité ; certaines personnes pourront poursuivre avec un doctorat (cela ne correspond pas forcément à une formation spécifique mais à une dominante de thèse en lien avec les laboratoires de recherche en cybersécurité).

« Tous les profils sont recherchés, mais ils sont généralement très techniques. Si un bac+3 peut suffire, les entreprises misent principalement sur des jeunes diplômés de niveau bac+5. »[4]

- Quelle est la part des enseignements dédiés à la cybersécurité ? A partir de quand peut-on considérer une formation dans le domaine de la cybersécurité ?

Le label SecNumEdu a apporté une première réponse en demandant un minimum de 70% du volume horaire d'enseignement et travaux pratiques en cybersécurité. Concernant les autres formations identifiées, l'information recueillie repose sur une déclaration des établissements, qui peuvent parfois faire référence à une part moindre des enseignements spécifiquement dédiés à la cybersécurité. Il n'y a pas de seuil clairement défini. En revanche, les formations recensées ont un spectre s'adressant aux métiers et préparant les compétences identifiées en phase 1 de l'étude (paragraphe 2.3. Un socle de compétences partagées).

[4] « La France manque d'experts en sécurité informatique », Techniques de l'ingénieur, janvier 2017

❖ *Cartographie des formations dispensées dans les établissements d'enseignement supérieur*

Cette cartographie s'appuie sur les travaux déjà réalisés par l'ANSSI en matière de référencement des formations initiales et du référencement réalisé par la Commission Nationale de la Certification Professionnelle (CNCP) :

L'initiative CyberEdu, lancée suite à la publication en 2013 du Livre Blanc sur la défense et la sécurité.

Le label de formation initiale en cybersécurité de l'enseignement supérieur
A l'occasion du Forum International de la Cybersécurité (FIC) du 24 et 25 janvier 2017, ont été dévoilées les 26 premières formations initiales labélisées : des formations universitaires délivrant un grade de Licence ou Master, des formations d'ingénieur dont le diplôme est reconnu par la Commission des Titres d'Ingénieurs (CTI) et des Mastères spécialisés reconnus par la Conférence des Grandes Écoles (CGE).

Le Répertoire Nationale de la Certification Professionnelle (RNCP) et l'inventaire des certifications professionnelles dans le domaine de la sécurité des systèmes d'information (RNCP et Inventaire de la CNCP)

Cette première capitalisation des référentiels existants a permis de construire le socle de la cartographie. Dans un second temps, cette cartographie a été soumise et approfondie via des entretiens avec des responsables de formation en cybersécurité.

Des représentants des structures suivantes ont été interviewés :

- ANSSI
- Centrale Supélec, mastère spécialisé et cycle ingénieur « sécurité informatique »
- ENSIBS, formation ingénieur en cyberdéfense
- ESIEA, mastère spécialisé SIS et parcours ingénieur
- INSA, département STI
- IUT des Pays de l'Adour (Mont de Marsan), licences professionnelles

Le guide d'entretien est en annexe 6.

A noter que les formations ont été recensées à partir des établissements de rattachement. En ce sens, une formation peut être comptabilisée plusieurs fois si elle proposée par plusieurs établissements partenaire. C'est le cas par exemple entre l'Université de Renne 1 et l'IUT de Saint Malo.

❖ *Cartographie des formations continues dispensées par des organismes de formations privés*

La cartographie des formations continues a été réalisée à partir d'une revue extensive des catalogues pédagogiques des principaux organismes de formation continue. Par ailleurs, cette revue a été complétée d'entretiens qualitatifs avec les acteurs suivants :

- HSC by Deloitte
- Fidens
- SANS Institute
- Sekoia

Dans le périmètre retenu des formations continues, ont été écartées les formations dites de sensibilisation à la cybersécurité. Seules les formations spécifiques aux professionnels de la cybersécurité ont été considérées.

❖ *Atelier commun de partage des résultats et de prospective*

EY, avec l'appui de l'ANSSI et de l'OPIIEC, a organisé un atelier de travail le 22 février 2017, réunissant des acteurs des formations initiales et des formations continues. Les objectifs de cet atelier commun étaient de :

- Présenter la cartographie des formations en vue de la tester et la compléter par les professionnels de la formation
- Connaitre la vision globale de ces acteurs sur l'offre de formation en cybersécurité et son évolution
- Aborder les questions d'attractivité des formations, du contenu pédagogique et du niveau des candidats/stagiaires.

Les participants à cet atelier ont représenté les établissements ou organismes suivants :

- L'ANSSI
- Centrale Supélec
- L'ESIEA
- L'EPITA
- Fidens
- Global Knowledge
- L'ISEP
- L'Université de Limoges
- L'Université de Valenciennes
- Telecom Paristech

d. Présentation de la méthodologie – Phase 3

Synthèse problématisée des précédentes étapes, la phase 3 a pour objectif de confronter les deux premiers volets de l'étude en analysant la capacité de l'offre de formation actuelle (initiale et continue) à répondre aux attentes et aux besoins des entreprises en métiers et compétences. Les résultats de cette analyse sont formalisés sous la forme d'enjeux, eux-mêmes déclinés en plan d'actions.

Le plan d'actions a été élaboré en 3 étapes :

- Formalisation de premières propositions à partir des entretiens de la phase 2 et de la phase 3
- Actualisation sur la base d'une analyse documentaire complémentaire
- Mobilisation d'un groupe d'experts en cybersécurité

Focus sur le groupe d'experts en cybersécurité

Un comité d'experts en cybersécurité, rassemblant acteurs de la filière, responsables d'organismes de formation continue et représentants d'établissements de formation initiale, a été mobilisé le 29 mars par EY, avec l'appui de l'ANSSI et de l'OPIIEC.

Les structures suivantes ont été mobilisées lors de cette réunion :

- ANSSI
- ESIEA
- Global Knowledge
- HSC by Deloitte
- Orange Cyberdéfense
- Sekoia
- Sogeti

Le groupe d'experts a permis :

- De partager les principaux constats de l'étude sur l'adéquation entre les besoins en compétences et l'offre de formation identifiée lors des phases précédentes
- D'identifier et de confirmer trois enjeux prioritaires pour la filière cybersécurité en termes de formation et de développement des compétences
- De co-construire un plan d'actions correctrices.

PARTIE 1 : ANALYSE DES BESOINS EN RECRUTEMENTS ET EN COMPETENCES

I. La cybersécurité, une filière en plein développement

1.1 La branche et la cybersécurité : un panel riche d'activités au cœur de la stratégie des entreprises

L'intégration croissante des nouvelles technologies dans les entreprises s'accompagne de nouveaux enjeux tels que la conformité réglementaire, l'évolution des systèmes et des compétences, la sensibilisation à la cybersécurité ainsi que la sécurité et la confidentialité des données traitées, échangées et archivées.

L'émergence accrue de nouvelles menaces liées à la cybercriminalité et leur médiatisation ont induit une prise de conscience générale au niveau de l'entreprise (dirigeants, métiers, comité d'audits, etc.). L'ensemble des entreprises est maintenant exposé à des attaques dont la maturité et la sophistication sont très élevées.

Incontournable et coûteuse, la sécurité a longtemps été considérée comme une « simple » nécessité liée aux risques et aux usages. – Publication Sopra Steria

---

La cybersécurité est devenue un élément stratégique pour l'entreprise. De plus en plus conscientes des enjeux, les entreprises investissent davantage dans la sécurité de leurs systèmes d'information. Plus qu'une simple fonction support, l'intégration de ces problématiques devient un atout différenciant sur le marché, notamment pour les grandes entreprises[5].

Tous les acteurs économiques et les administrations publiques sont aujourd'hui concernés par la cybersécurité. Suivant leur degré d'exposition au risque et à la nécessité de sécurité, les entreprises font le choix d'intégrer et développer en interne une expertise cybersécurité et/ou de recourir à des prestataires ou fournisseurs externes.

« La détention d'informations devient une clé de la réussite et un enjeu majeur en terme concurrentiel, détenir/obtenir des informations sensibles est un avantage. De fait, la protection de ces mêmes données est capital et va devenir encore plus importante dans les années à venir » - dirigeant d'entreprise[6]

Se distinguent ainsi deux types d'acteurs de la cybersécurité pour les entreprises de la Branche :

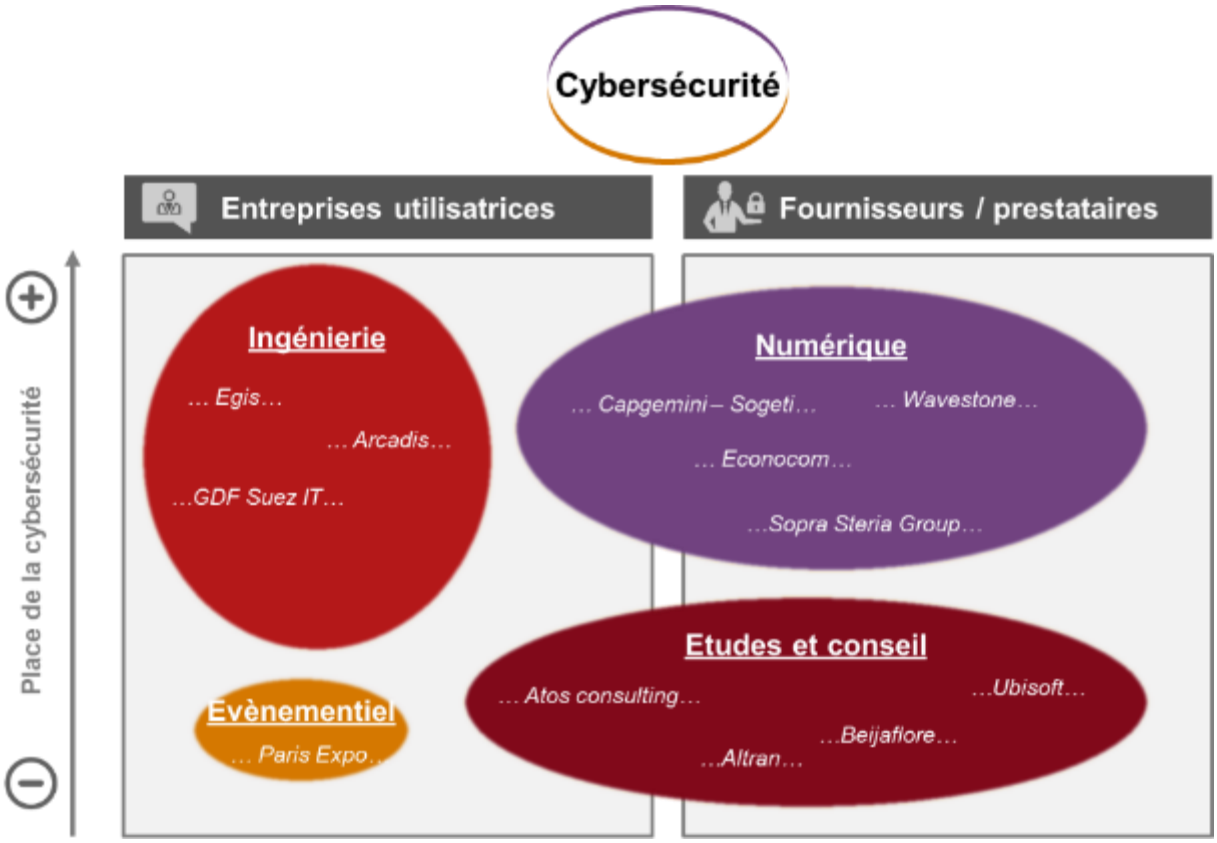
- D'une part les entreprises dites « fournisseurs ou prestataires » de solutions ou de services en cybersécurité : les éditeurs de solutions logicielles de sécurité (pour particuliers et

[5] Sopra Steria, « Quand la sécurité devient un levier compétitif »

[6] Citation d'une entreprise ayant répondu à l'enquête en ligne EY réalisée dans le cadre de cette étude sur les effectifs et les besoins des entreprises en cybersécurité

professionnels) et les prestataires de services cybersécurité acteurs pour le développement de logiciels et la mise en place de protections au sein des entreprises.

- D'autre part, les entreprises dites « utilisatrices » de la cybersécurité, dont le cœur d'activité n'est pas directement lié à la cybersécurité mais qui ont besoin d'assurer un certain niveau de protection des données : données clients, secrets de fabrication, commerce en ligne… Par définition de cette catégorie, ces entreprises ont au moins un professionnel[7] dédié à la cybersécurité parmi leurs employés.



DEUX GRANDS TYPES D'ACTEURS DE LA CYBERSECURITE AU SEIN DE LA BRANCHE

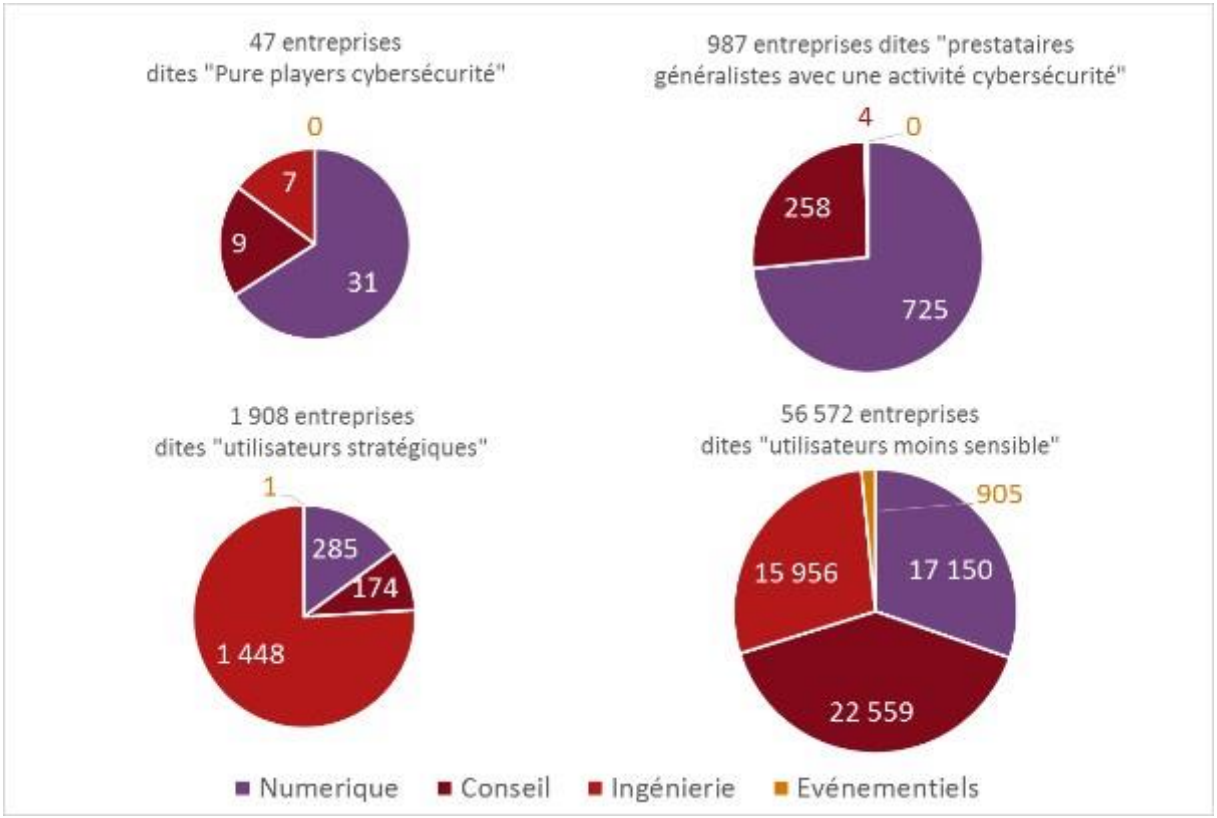
Les entreprises mentionnées sur ce graphique sont indiquées à titre illustratif et non de manière exhaustive.

Les degrés de sensibilités restent très variables d'un secteur d'activité à l'autre. Ainsi, la place de la cybersécurité au sein des entreprises pourra être différente entre :

- Une entreprise utilisatrice avec des activités de type évènementiel ou un Opérateur d'Importance Vitale (OIV)
- Un pure player cybersécurité et une entreprise de conseil généraliste dont une partie des services concerne la cybersécurité.

[7] Au sens d'un équivalent temps plein (ETP) dédié à la cybersécurité

Cette approche des catégories d'acteurs permet de couvrir l'ensemble des entreprises de la Branche, aussi bien les entreprises des secteurs du numérique, des études et conseil, de l'ingénierie ou de l'évènement.



QUELS TYPE D'ACTEURS AU SEIN DES SECTEURS DE LA BRANCHE ?[8]

L'analyse des entreprises de la Branche, par leur activité[9], a permis d'identifier :

- Près de 1000 entreprises dites « fournisseur ou prestataire », réalisant une part ou la totalité de leur activité en cybersécurité[10]
- Plus de 58 000 entreprises de la Branche « utilisatrices » de cybersécurité (stratégique ou moins sensible)[11]

C'est essentiellement dans le secteur du numérique et du conseil où se trouvent les éditeurs de sécurisation des infrastructures informatiques et prestataires de cybersécurité. A l'inverse, les secteurs de l'ingénierie et de l'évènementiel sont composés quasiment exclusivement d'entreprises dites « utilisatrices » de cybersécurité, domaine n'étant pas leur cœur d'activité.

Les principaux emplois en cybersécurité se trouvent ainsi dans les entreprises des secteurs du numérique et du conseil, même si l'ensemble des secteurs reste concerné par les problématiques de cybersécurité.

[8] Modélisation : estimation des effectifs cybersécurité au sein de la Branche, EY 2017

[9] Approche systématique réalisée via les codes NAF des entreprises, puis au cas par cas pour les principaux acteurs reconnus en cybersécurité.

[10] L'hypothèse retenue pour cette catégorie est d'avoir en interne a minima un ETP en cybersécurité.

[11] Suivant la taille de l'entreprise et la sensibilité de cette dernière à la sécurité, il pourra n'y avoir aucun professionnel de cybersécurité dans ces entreprises.

1.2 Les emplois dans la cybersécurité

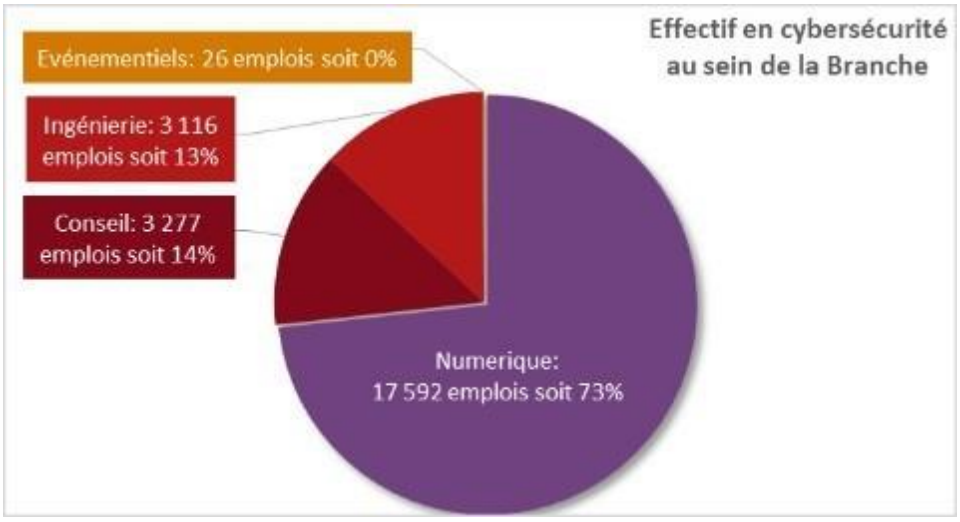
Les professionnels de la cybersécurité pour les entreprises de la Branche, correspondent aux personnes dont le cœur de métier est :

- Le développement de logiciels de sécurité tels que les antivirus, les anti-spams…
- La réalisation de prestations d'audit et de conseil en cybersécurité
- Le développement et l'intégration de solutions de sécurité telles que la gestion des identités et des accès (IAM), la prévention des pertes de donnée (DLP),…
- Les services managés de sécurité tels que le Centre des opérations de sécurité (COS ou SOC)

Tout exercice quantitatif sur les effectifs en cybersécurité se veut délicat et soulève souvent un questionnement des professionnels. Il existe différents rattachements possibles des équipes cybersécurité au sein des entreprises, ce qui ne facilite pas leur identification. Tous les effectifs DSI internes à une entreprise n'ont pas nécessairement une activité majeure en cybersécurité. Les effectifs en cybersécurité ne seront qu'une partie qu'il convient d'estimer. Enfin, les besoins d'une entreprise en cybersécurité ne sont pas nécessairement couverts par les effectifs internes mais également par des prestataires de services aux compétences affirmées.

L'approche quantitative retenue comptabilise non pas les besoins des entreprises mais les effectifs actuels en interne[12], afin de s'affranchir du choix d'internalisation ou d'externalisation partielle des prestations de cybersécurité faites par l'entreprise.

Avec plus de 24 000 emplois[13] en cybersécurité au sein des entreprises de la Branche, les professionnels de la cybersécurité représentent ainsi 3% de l'effectif total des entreprises de la Branche (tous secteurs confondus). 24 000 emplois en cybersécurité au sein de la Branche font de cette dernière un ensemble important d'acteurs de la filière cybersécurité au niveau de la France.



REPARTITION DES EFFECTIFS AU SEIN DE LA BRANCHE SUIVANT LE TYPE D'ACTIVITE EN CYBERSECURITE[14]

[12] Les effectifs correspondant aux prestations de service sont comptabilités pour les entreprises prestataires, de manière à ne pas doubler le décompte.

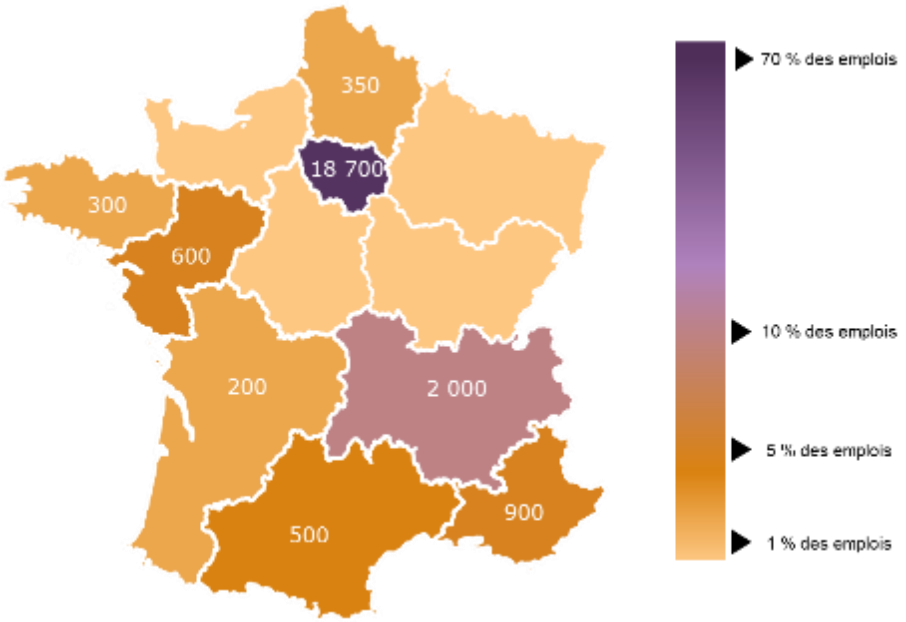
[13] Les emplois en cybersécurité, correspondant à une part des effectifs de la Branche, sont le nombre d'emplois salariés (base ETP).

[14] Modélisation : estimation des effectifs cybersécurité au sein de la Branche, EY 2017

La quantification des emplois en cybersécurité au sein de la Branche a permis de confirmer que la grande majorité des effectifs en cybersécurité de la Branche sont dans des entreprises dites du secteur Numérique (73%).

La grande majorité des emplois en cybersécurité est exercée par des entreprises dites « fournisseurs ou prestataires » en cybersécurité avec 82% des emplois, contre 18% dans les entreprises dites utilisatrices.

La carte de France ci-dessous donne une approche géographique des emplois en cybersécurité pour les entreprises de la Branche :



REPARTITION GEOGRAPHIQUE DES EFFECTIFS CYBERSECURITE AU SEIN DES ENTREPRISES DE LA BRANCHE[15]

Ces emplois sont principalement situés en région Ile-de-France. Ce déséquilibre régional Paris-Province s'explique notamment par :

- Une forte présence des entreprises de la Branche en Ile-de-France (plus de 60% des effectifs)
- Un rattachement fréquent des fonctions en cybersécurité au siège des entreprises, majoritairement implanté en Ile-de-France

[15] Modélisation : estimation des effectifs cybersécurité au sein de la Branche, EY 2017

1.3 Une filière en croissance, et qui recrute !

Qu'entend-on par filière ?

D'après l'INSEE, la filière désigne couramment l'ensemble des activités complémentaires qui concourent, d'amont en aval, à la réalisation d'un produit fini. On parle ainsi de filière électronique (du silicium à l'ordinateur en passant par les composants) ou de filière automobile (de l'acier au véhicule en passant par les équipements). La filière intègre en général plusieurs branches.

Par extension, la cybersécurité se structure en tant que filière, constituée d'un ensemble d'acteurs concourant à assurer la sécurité des systèmes d'information, allant des éditeurs de logiciels aux prestataires de service dans le domaine. La spécialisation des professionnels et la montée en puissance des niveaux de sécurité renforcent cette notion de filière.

La cybersécurité constitue une filière d'avenir. Un million de postes sont à pourvoir à l'échelle mondiale.

Dans le cadre de ce marché qui se structure en France, encouragée par les nouvelles technologies et poussée par la montée en puissance des attaques internet et leur médiatisation, la cybersécurité pourrait, à terme, représenter une vitrine de la compétitivité des entreprises françaises[16].

De plus, les pratiques et la perception des problématiques de cybersécurité évoluent auprès de l'ensemble des entreprises et des administrations. 59% des entreprises françaises ont augmenté leurs dépenses de cybersécurité en 2016[17].

81% des entreprises françaises ont été visées par une cyberattaque en 2015[18]

En France, l'année 2013 a été marquée par les préconisations du Livre blanc sur la défense et la sécurité nationale pour faire face aux menaces cyber puis par la dernière Loi de Programmation Militaire (LPM)[19]. Les pouvoirs publics se saisissent du sujet, notamment via l'ANSSI, en responsabilisant les Organismes d'Importance Vitale (OIV) quant à la sécurisation de leurs systèmes d'information d'importance vitale (SIIV). Deux décrets[20] parus en 2015 viennent confirmer et préciser la mise en œuvre de la LPM.

[16] BPI France, 2016, « La cybersécurité, une filière d'avenir pour l'offre française »
[17] Le Parisien éco, Novembre 2016, « La France booste la cybersécurité »
[18] Microsoft, août 2016, « Cybersécurité : 5 chiffres-clés à connaitre »
[19] Article 22 de la loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013)
[20] Décrets du 27 mars 2015 : Décret n°2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale ; Décret n°2015-350 relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité nationale.

Au niveau de l'Union Européenne, le Règlement Général sur la Protection des Données (RGPD)[21] est un autre aspect réglementaire aux impacts directs pour le domaine de la cybersécurité au sein des entreprises. En renforçant le contrôle de l'utilisation des données personnelles des citoyens européens, le RGPD développe les droits reconnus à la personne au-delà de la loi Informatique et Liberté[22]. Ainsi, d'ici 2018 - date de mise en application du RGPD, les entreprises devront, entre autre, intégrer une approche « privacy by design and by default »[23], une procédure de « Data Breach Notification »[24]. Les prochaines années vont être clés pour les entreprises européennes, pour atteindre et maintenir les différents niveaux exigés par ce règlement.

92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en application du RGPD[25]

Ces marqueurs législatifs agissent comme de véritables déclics et lancent une dynamique française et internationale pour l'ensemble de la filière. Au-delà des OIV, certaines autres grands groupes ont intégré la sécurité dans leur réflexion allant jusqu'à s'aligner sur les dispositifs exigés pour les OIV ou les entreprises collectant les données personnelles de citoyens européens.

Ces mises en conformité et les volontés indépendantes de montée en sécurité de leurs systèmes engendrent pour les entreprises des besoins forts en termes de cybersécurité. La croissance du marché[26] va donc se poursuivre. Cela se traduit par une demande forte, et des attentes croissantes des entreprises en termes de logiciel, matériel et prestations (conseil, formation…). Plus spécifiquement, le marché français des appliances et des logiciels dédiés à différentes problématiques de cybersécurité (gestion de la sécurité, des accès ou des identités…) devrait progresser de 6,5% par an jusqu'en 2020[27]. Une part de cette croissance de marché serait alors portée par la croissance des effectifs dans le secteur.

« Avec les évolutions technologiques (Fintech, Blockchain...),
il est évident que la cybersécurité évolue également.
Par ailleurs, les régulateurs aussi imposent des directives pour des activités plus safe. »
- DRH d'une société de conseil avec une expertise en cybersécurité[28]

Les entreprises de la Branche sont également touchées par ces évolutions réglementaires. Leur besoin en effectif se traduit par une croissance des effectifs à court et moyen terme.

[21] Le Règlement a été adopté le 8 avril 2016 par le Conseil de l'Europe, et le 16 avril par le Parlement Européen. Son application est directe et s'imposera aux Etats Membres à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales.
[22] La loi Informatique et Liberté reconnait 3 droits à la personne (opposition au traitement sous réserve de motif légitime, droit d'accès/communication aux données, droit de rectification/suppression), le RGPD passe à 11 droits (droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit d'opposition…).
[23] Prise en compte du respect de la vie privée dès la conception du traitement – Article 35 du RGPD
[24] Notification des violations de données personnes – Article 33 et 34 du RGPD
[25] Symantec, décembre 2016
[26] +8% de croissance du chiffre d'affaires des spécialistes français de la cybersécurité - Xerfi, juin 2015.
[27] IDC, 2017, « Le marché de la cybersécurité pèsera 1,2 Md€ en France en 2020.
[28] Citation d'une entreprise ayant répondu à l'enquête en ligne EY sur les effectifs et les besoins des entreprises en cybersécurité

A horizon 3 ans, les entreprises de la Branche anticipent une croissance des effectifs en cybersécurité de 6 %, représentant 1 400 créations nettes d'emplois. De même que les emplois actuels sont majoritairement situés en Ile-de-France, les emplois créés seront principalement dans la Région capitale.

A horizon 5 ans, la tendance de croissance (création nette d'emplois) s'est vue confirmée par les entreprises avec une perspective de croissance de 8 %. Cependant, l'estimation des effectifs et même leur localisation deviennent délicates pour cette perspective à moyen terme. La quantification des emplois réalisée repose sur les effectifs en interne et en France des entreprises. Certaines évolutions imprévisibles liées aux choix stratégiques des entreprises seraient susceptibles de faire évoluer ces prévisions (ex : internalisation, externalisation ou délocalisation).

« Nos effectifs suivent les demandes de nos clients, elles vont grandissantes dans ce domaine » - dirigeant d'une entreprise de service[29]

A horizon 8 ans, les entreprises se disent très prudentes sur toute perspective à plus long terme. L'évolution rapide des technologies en cybersécurité, la concurrence internationale et l'impact de nouvelles réglementations sont autant de facteurs d'incertitude quant à des perspectives d'effectifs en France pour les entreprises de la Branche.

Si les grands groupes ont aujourd'hui conscience des risques et intégré les problématiques en cybersécurité à leur stratégie d'entreprise, ce n'est pas encore le cas des TPE-PME. Pour ces dernières, les choses avancent plus lentement[30]. Encore non équipées ou mal protégées, les petites entreprises constitueront vraisemblablement l'un des enjeux fort pour la cybersécurité, et représentent en ce sens un potentiel de croissance important pour la filière.

« Dans notre activité de maintien en conditions opérationnelles des systèmes d'information de nos clients, la cybersécurité doit être maitrisée par tous nos intervenants et sous-traitants » - dirigeant d'une entreprise en Bretagne[31]

Un autre facteur de croissance à plus long terme réside dans la forte expansion des objets connectés, considérés parmi les priorités des entreprises en matière de digital. A l'horizon 2020, le monde sera équipé de quelques 21 milliards d'objets connectés[32]. Leur sécurité va devenir un enjeu pour les années à venir.

[29] Citation d'une entreprise ayant répondu à l'enquête en ligne EY sur les effectifs et les besoins des entreprises en cybersécurité

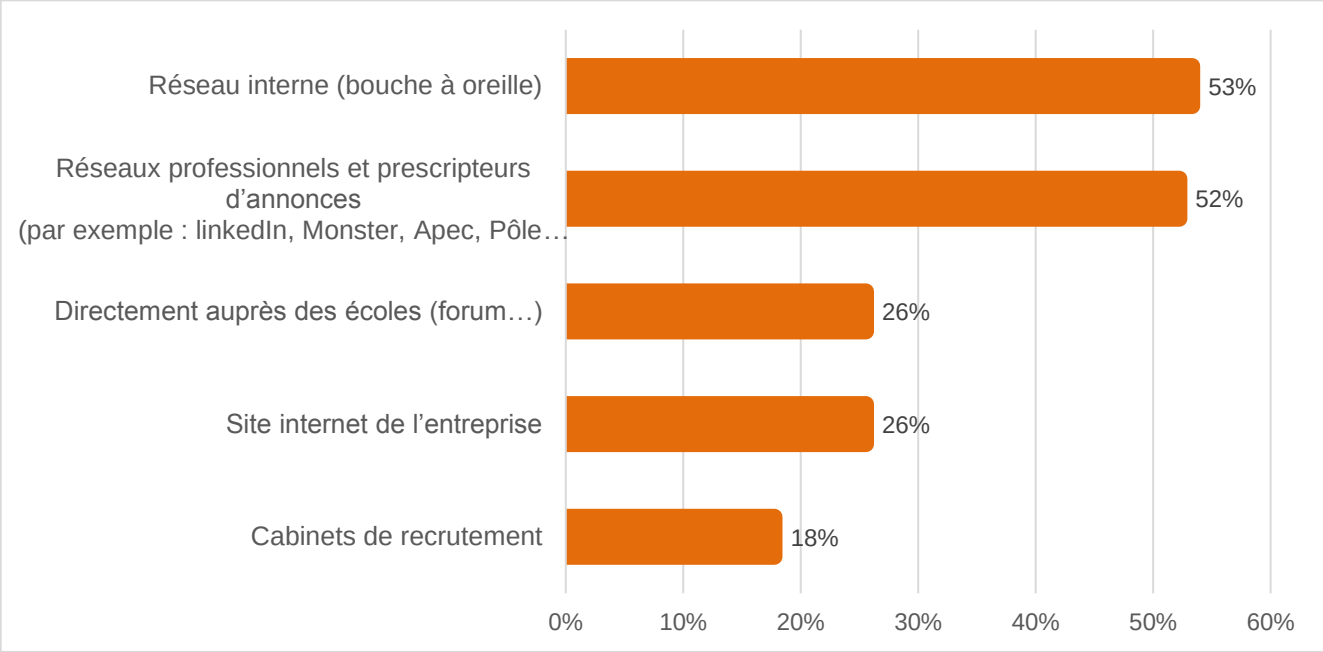
[30] Le Parisien éco, novembre 2016, « La France booste la cybersécurité »

[31] Citation d'une entreprise ayant répondu à l'enquête en ligne EY sur les effectifs et les besoins des entreprises en cybersécurité

[32] Estimation issue du CyberCercle, PwC, 14 décembre 2016

Focus sur les canaux de recrutement en cybersécurité[33]

La croissance des effectifs en cybersécurité dans les entreprises et plus globalement les recrutements dans ce secteur se font de manière diversifiée. Les canaux utilisés par les entreprises sont nombreux et en adéquation avec le caractère numérique et évolutif du secteur.



CANAUX DE RECRUTEMENT UTILISES PAR LES ENTREPRISES DE LA BRANCHE POUR LA CYBERSECURITE

Le bouche à oreille et les réseaux professionnels (annonces en ligne) restent utilisés par la majorité des entreprises pour le recrutement d'effectifs en cybersécurité. Viennent ensuite les recrutements directement auprès des écoles (via les forums, ou l'alternance par exemple) et les annonces directement sur le site des entreprises (26%). Enfin, moins courant, le recours à des cabinets de recrutement est pratiqué par 18% des entreprises.

Le recrutement direct auprès des écoles est pratiqué par plus d'un quart des entreprises, ce fort taux laisse présager :

- une certaine tension sur des profils avec une nécessité de recruter plus de jeunes candidats dès l'obtention de leur diplôme
- une proximité peut être plus forte que d'autres filières entre les écoles et les entreprises de la filière.

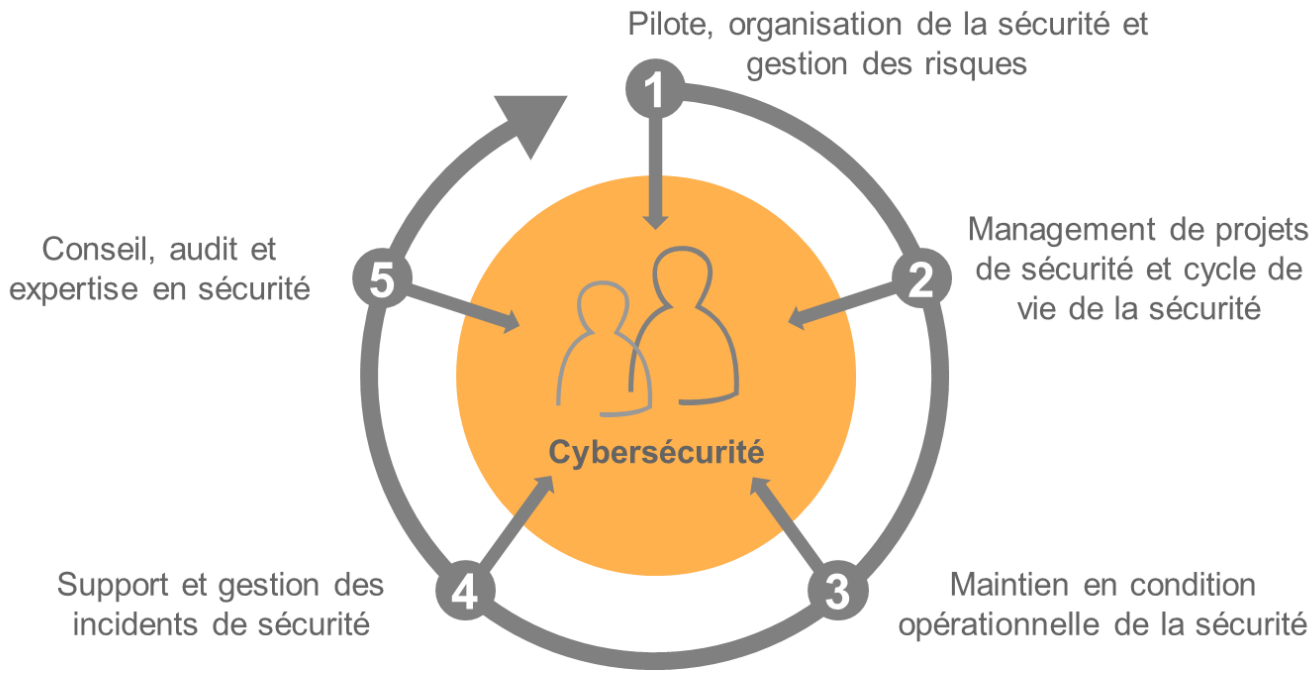
[33] Les données chiffrées sont issues du questionnaire en ligne mené par EY auprès des entreprises de la Branche.

II. Un écosystème de métiers

2.1 Les 5 familles de métiers de la cybersécurité

La filière de la cybersécurité repose sur un capital humain d'une grande variété. Cette diversité lui permet de couvrir un large champ de métiers et d'activités.

Ces métiers se structurent autour de cinq grandes familles correspondant à un bloc d'activités partagées. Ces familles de métiers répondent à l'ensemble des besoins actuels des entreprises, sans pour autant organiser ces métiers autour de produits cybersécurité (logiciels, équipements, prestations de service…) mais bien autour d'activités et compétences communes.



5 FAMILLES DE METIERS EN CYBERSECURITE

La 1ère famille « pilotage, organisation de la sécurité et gestion des risques » regroupe l'ensemble des métiers à fortes responsabilités en termes de management de la sécurité du système d'information de l'entreprise en lien avec la gestion des risques. Ces métiers jouent un rôle direct dans la définition de la stratégie de sécurité de l'entreprise et sont responsables de l'évolution du corpus documentaire de la sécurité et notamment des politiques de sécurité.

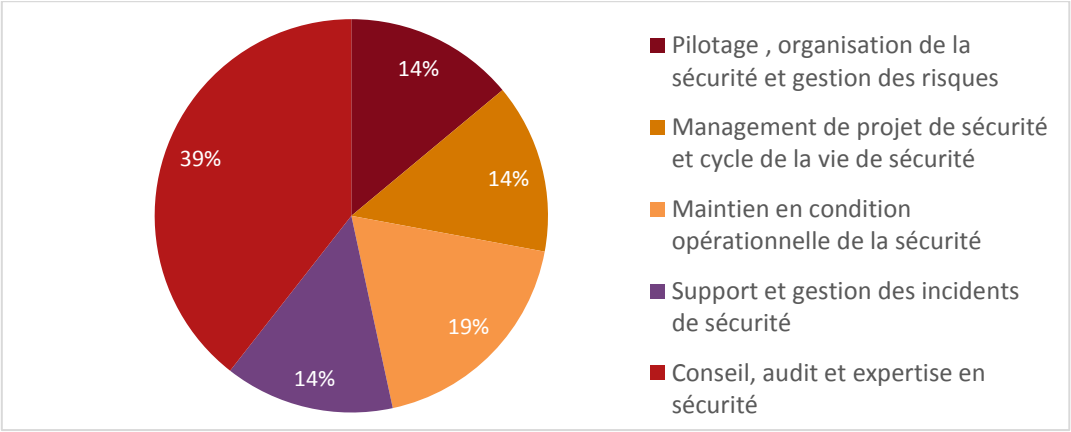
La 2ème famille « Management de projets de sécurité et cycle de vie de la sécurité » regroupe l'ensemble des métiers jouant un rôle important dans l'ensemble des projets d'évolution de la sécurité du système d'information. Ils sont soit superviseurs de ces projets soit des acteurs majeurs de ces projets.

La 3ème famille dite de « maintien en condition opérationnelle de la sécurité » couvre l'ensemble des métiers opérationnels ayant en charge la configuration et le déploiement de correctifs de sécurité et l'application de mesures de sécurité sur l'infrastructure technique (réseau, système et sécurité) de l'entreprise.

La 4ème famille « Support et gestion des incidents de sécurité » est constituée de l'ensemble des métiers intervenant directement sur les incidents de cybersécurité (infection virale, ransomware ou rançongiciel, fuite d'information…). Ils participent à l'amélioration continue des méthodes de détection et de prévention (veille sécurité, contrôles de sécurité…) des incidents de sécurité dont ils assurent également le traitement.

Enfin, la 5ème famille « Conseil, audit et expertise en sécurité » rassemble les métiers de la cybersécurité réalisant des missions d'expertise en cybersécurité. Ils sont généralement missionnés par les entreprises pour répondre à un besoin ponctuel ou parce qu'ils disposent de compétences non disponibles au sein de l'entreprise mais les entreprises peuvent également faire appel à eux dans le but d'obtenir un avis indépendant.

Les 24 000 emplois estimés aujourd'hui en cybersécurité pour la Branche se décomposent suivant ces familles de métiers :



REPARTITION DES EFFECTIFS EN CYBERSECURITE PAR FAMILLE DE METIERS

Cette répartition des effectifs suivant la famille de métier est spécifique à la Branche. Cette répartition ne peut être extrapolée à l'ensemble de la filière cybersécurité en France. En effet, la Branche est constituée de nombreuses entreprises du numérique plus concernées par la cybersécurité mais également d'entreprises aux activités diverses. Ces dernières non spécialisées en cybersécurité (dites entreprises utilisatrices) ont des effectifs internes en cybersécurité souvent limités et concentrés sur une famille de métiers : les fonctions dites de pilotage, d'organisation de la sécurité et gestion des risques. Elles sont amenées cependant à faire appel à des prestations externes diverses : audit, conseil, expertise…

La cybersécurité en France (ainsi qu'au niveau européen et mondial) est un marché complexe, novateur, sans cesse en mouvement et contraint par le manque de compétences. Ceci explique le taux important de sous-traitance par rapport à d'autres marchés : en France, 69% des entreprises déclarent être accompagnées par des prestataires privés et 17% par des institutions gouvernementales pour la définition et la mise en œuvre de leur stratégie de sécurité[34].

« Etant seule dans l'entreprise, j'externalise les missions de prestations informatiques générales, dont la protection cybersécurité auprès d'un prestataire extérieur. » - gérante d'une petite entreprise d'ingénierie[35]

---

[34] PAC, Juin 2015 « Cybersécurité : Investissements, opportunités et challenges pour les entreprises françaises »

[35] Citation d'une entreprise ayant répondu à l'enquête en ligne EY sur les effectifs et les besoins des entreprises en cybersécurité

2.2 Cartographie des métiers

Cette cartographie des métiers se veut représentative mais surtout explicite et pratique d'usage pour tous les professionnels, quel que soit leur degré d'appétence à la cybersécurité.

Plus qu'un simple référencement des métiers, la liste présentée ci-dessous donne également les différentes appellations utilisées en France pour un même métier ainsi qu'une définition succincte de son rôle / de ses activités, et le profil type en termes de formation[36].

1. Pilote, organisation de la sécurité et gestion des risques

Métier	Autre appellation	Définition	Profil[37]
Responsable de la Sécurité des Systèmes d'Information (RSSI)	Directrice/eur de la sécurité de l'information CISO (Chief Information Security Officer) CSO (Chief Security Officer) Responsable sécurité informatique Responsable de la protection des informations OSSI (Officier de la sécurité des systèmes d'information) ISSM (Information Systems Security Manager)	Définit la politique de sécurité du SI et de l'information et veille à son application. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers ou de la direction générale. Il préconise, ou valide toute intervention en cas d'incidents de sécurité.	Bac +5 5 à 10 ans d'expérience
Correspondant(e) Sécurité	Correspondant(e) Sécurité du Système d'Information (CSSI) Gestionnaire de Risques cyber Correspondant(e) risques opérationnels (CRO) Assistant RSSI	Assure un rôle d'intermédiaire entre le RSSI et les lignes métiers. Sa forte proximité avec le métier lui permet d'intervenir sur des thématiques de gestion des risques, de gouvernance et de sensibilisation auprès des utilisateurs. Il définit et remonte les tableaux de bord (KRI / KPI) au RSSI.	Bac +4/5 5 ans d'expérience
Responsable du Plan de Continuité d'Activité (RPCA)	Responsable PCA et risques opérationnels, expert en gestion de crise	Elabore et met en œuvre dans son entreprise un Plan de Continuité d'Activité (PCA) et un dispositif de Gestion de Crise (GdC).	Bac +4/5 3 ans d'expérience

[36] Définition basée sur une revue documentaire, notamment les fiches métiers référencée par le ministère http://www.metiers.internet.gouv.fr/mot_cle/securite , par des entretiens complémentaires et par l'expertise EY.

[37] La notion de profil renvoie au niveau de formation et nombre d'années d'expérience « usuel » pour le métier. Il n'exclue pas des candidats plus « atypique », tenant plus spécifiquement des qualités personnelles ou expériences professionnelles. Ce profil plus « standard » repose sur l'analyse des offres d'emplois en ligne (pré requis et formation) et la conduite d'entretiens auprès de professionnels en cybersécurité. Lorsqu'il n'est pas précisé un nombre d'années d'expérience minimale, il s'agit d'un métier qui est ouvert la plupart du temps aux jeunes diplômés.

2. Management de projets de sécurité et cycle de vie de la sécurité

Métier	Autre appellation	Définition	Profil
Directrice / directeur de programme sécurité	Responsable projet	Assure le pilotage d'un ou plusieurs projets sécurité de l'entreprise (coût, délai, qualité et risques)	Bac +5 5 à 10 ans d'expérience
Chef de projet sécurité	PMO Sécurité Chef de projet sécurité informatique Chef de projet sécurité des systèmes d'information	Assure la réalisation d'un projet sécurité depuis l'analyse des besoins jusqu'aux tests, la mise en route et la formation des utilisateurs	Bac +5 3 à 5 ans d'expérience
Développeuse / développeur sécurité	Développeur en sécurité informatique Source code auditor Security software developer Auditeur sécurité de code source Information Systems Security Developer	Assure le sous-ensemble des activités d'ingénierie nécessaires au développement de logiciels (design, interfaces, spécifications, conception, codage, production de binaire, assemblage, tests, préparation à l'intégration de niveau solution, gestion des sources, gestion de configuration, gestion des faits techniques, archivage, documentation) répondant à des exigences de sécurité. Développe de façon méthodique, en appliquant des règles de conception / codage / tests et s'assure que les composants qu'il produit sont testables en termes de conformité fonctionnelle, de robustesse, de sécurité (résistance aux attaques identifiées en entrée de la conception), et de performances.	Bac +2/3 et plus
Architecte sécurité	Architecte Sécurité Informatique Architecte Réseaux et Télécom	Conçoit l'architecture et l'implémentation afin d'adopter les solutions qui disposent du niveau de Sécurité adapté aux contextes du projet et de la future application (technologiques, techniques, usages, criticité Business…)	Bac +3 à Bac +5 5 à 10 ans d'expérience

3. Maintien en condition opérationnelle de la sécurité

Métier	Autre appellation	Définition	Profil
Administratrice / administrateur sécurité	Administratrice/eur Sécurité Informatique Opératrice/eur en sécurité des systèmes d'information Ingénieur(e) sécurité infrastructure support specialist	Met en œuvre de la politique de sécurité de l'entreprise et administre des solutions de sécurité de type antivirus, antispam, IPS, la gestion des habilitations (départ, arrivée, mobilité) et les dérogations	Bac +2/3
Technicien(ne) sécurité	Technicien(ne) support SSI Télé-assistant	Installe et la mise en œuvre et à l'exploitation des solutions de sécurité	Bac +2/3

4. Support et gestion des incidents de sécurité

Métier	Autre appellation	Définition	Profil
Analyste SOC (Security Operations Center)	Analyste Cyber SOC Veilleur-Analyste	Paramètre les systèmes de supervision de la sécurité (SIEM, sondes, honeypots, équipements filtrants). Catégorise, analyse et traite les alertes de sécurité de façon régulière pour en améliorer l'efficacité. Assure la détection, l'investigation et la réponse aux incidents de sécurité.	Bac +2/3
Chargé(e) de la réponse aux incidents	Expert(e) réponse à Incidents CERT Spécialiste en investigation numérique	Analyse et traite les incidents de sécurité au sein d'une structure ou d'une équipe de réponse à incident (CERT, CSIRT, etc.). Communique et fournit des recommandations de sécurité aux services clients de la cellule de réponse à incident ou à d'autres CERT (ou CSIRT).	Bac +3 à Bac+5

5. Conseil, audit et expertise en sécurité

Métier	Autre appellation	Définition	Profil
Consultant(e) et auditrice/auditeur gouvernance, risques et conformité	Consultant(e) en sécurité des systèmes d'information (SSI) Auditrice/eur sécurité organisationnelle Auditrice/eur conformité Evaluatrice/eur sécurité Consultant(e) en sécurité organisationnelle	Fournit des conseils fonctionnels, méthodologiques et techniques pour des clients afin de pouvoir proposer des solutions améliorant leur sécurité. Réalise des missions d'audits du volet organisationnel (contrôle de conformité, analyse de documents et de procédures, entretiens, vérification des preuves fournies, audit de sécurité physique, etc.)	Bac +4/5
Consultant(e) et auditrice/auditeur sécurité technique	Spécialiste cybersécurité/Expert produit/technologie (IAM, MDM, IDS, IPS, etc.) Pen testeur Expert(e) audit sécurité et intrusion Ethical Hacker	Apporte une expertise produit/technologie sur la sécurité des informations depuis la conception, l'élaboration jusqu'à la mise en œuvre des solutions de sécurité. Réalise des missions d'audits du volet techniques (code, configuration, composants, tests d'intrusions, etc)	Bac +4/5
Evaluatrice/évaluateur sécurité des systèmes et des produits	System testing and evaluation specialist	Vérifie la conformité d'un produit, voire, d'un système, par rapport à un référentiel (normatif ou spécifique) selon des critères et en mettant en œuvre une méthode	Bac +4/5
Cryptologue	Expert(e) en cryptographie	Peut être amené à concevoir des algorithmes de chiffrement visant à sécuriser l'information Apporte son expertise dans tout ou partie des domaines suivants (selon l'organisation à laquelle il appartient) : utilisation d'algorithmes / protocoles cryptographiques, gestion des clés, implémentation sécurisée et évaluation d'algorithmes cryptographiques, analyse cryptographique...	Bac +5 à Doctorat
Expert(e) juridique en cybersécurité	Magistrature, Conseil juridique, Investigatrice/eur de droit privé, avocat(e), juriste cyberdéfense, consultant(e) juridique en cyberdéfense, juriste spécialisé en cyberdéfense	Réalise des missions de recherche des informations sur tout support numérique afin de produire des rapports pour la Justice ou les entreprises	Bac +5 3 à 5 ans d'expérience

Métier	Autre appellation	Définition	Profil
Délégué(e) à la Protection des Données (DPD)	Correspondant informatique et libertés (CIL) Data protection officer (DPO) Privacy officer Privacy compliance Manager	Garantie la protection des données personnelles traitées par l'entreprise	Bac +5 10 ans d'expérience
Formatrice / formateur en sécurité	Instructrice/instructeur SSI Professeur(e) enseignement secondaire	Conçoit, développe et réalise des outils de formation et d'entraînement pour les domaines du service : réseaux, système d'information et cybersécurité.	Bac +5 3 à 5 ans d'expérience

D'autres métiers non sélectionnés dans le référencement ci-avant, peuvent également être considérés comme des métiers de la cybersécurité (métiers en devenir, peu présents actuellement) ou moins au cœur de la cybersécurité : le responsable d'intelligence économique, le responsable sûreté-sécurité, le référent sécurité projet, l'analyste cybersécurité, le cyber data scientist, le responsable CERT, l'analyste/actuaire cyber assurance…

Les entreprises de la Branche se sont exprimées[38] sur les métiers les plus représentés au sein de leurs effectifs :

A noter que les appellations peuvent être nombreuses pour un même métier, suivant les entreprises (leur taille, le caractère français ou international de leur activité…). Il convient de rappeler également que ces métiers répondent aux besoins très variés des entreprises en cybersécurité suivant leur secteur d'activité ou leur taille.

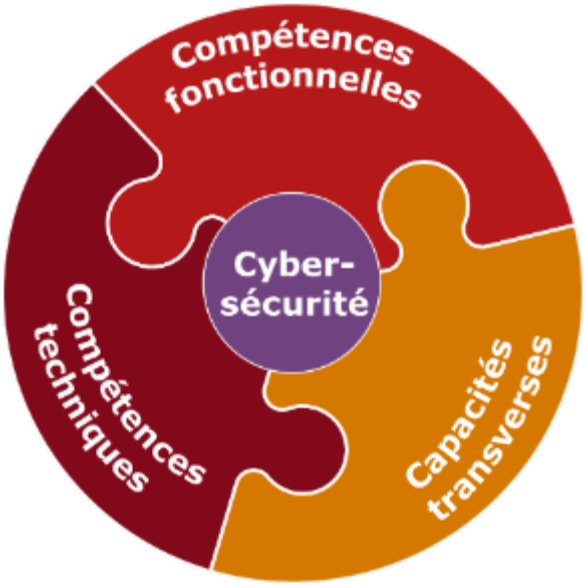
[38] Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité

2.3 Un socle de compétences partagées

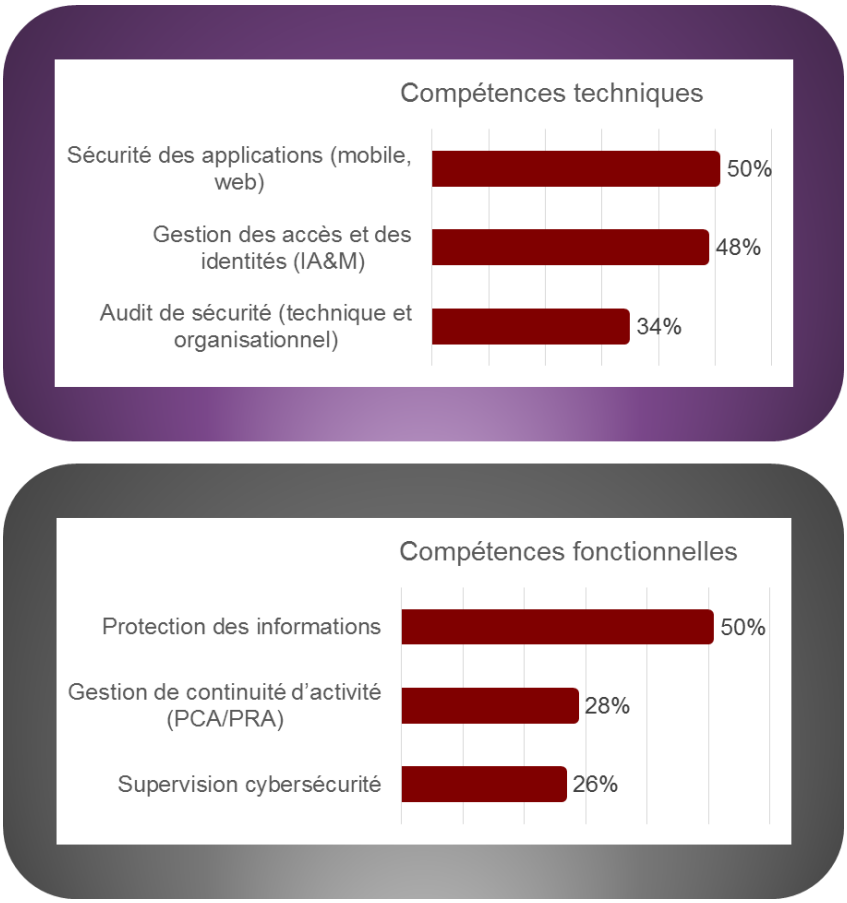
Les métiers de cybersécurité font appels à des connaissances et niveaux de compétences très variées. Dans la plupart des cas, la triple **compétence fonctionnelle, technique et transverse** permet d'établir le socle de compétences partagé pour la filière cybersécurité.

Ces compétences ont été classées en 3 grandes catégories :

- Les compétences fonctionnelles, telles que l'analyse et la cartographie des risques, les normes de sécurité, la protection de la vie privée…
- Les compétences techniques, telles que l'architecture de sécurité, la sécurité des applications, la gestion des accès et des identités…
- Les capacités transversales, représentant plus largement des aptitudes non spécifiques au secteur de la cybersécurité.



Une première approche globale des principales compétences en cybersécurité a été menée. Les entreprises, afin de répondre à l'ensemble de leur problématique et besoins dans le domaine, se sont exprimées sur les principales compétences techniques et fonctionnelles qu'elles recherchent aujourd'hui. Cela pourrait se traduire par un « profil type » du professionnel, s'adressant aux attentes actuelles des entreprises, comprenant à la fois des compétences fonctionnelles et techniques.



PROFIL TYPE AUX PRINCIPALES COMPETENCES TECHNIQUES ET FONCTIONNELLES ATTENDUES[39]

Ce profilage type reste évidemment un exercice limité par son caractère théorique. Les attentes nombreuses des entreprises sont couvertes par des professionnels aux expériences, compétences et spécificités différentes. Cependant, il permet de mettre en avant les principales compétences attendues des entreprises.

« D'ici 2018, 34% des dépenses en sécurité pourraient être consacrées à la protection des données personnelles, de la vie privée, ainsi qu'à la mise en conformité avec les règlementations européennes. »[40] *La maitrise des compétences comme la gestion des accès et identités, ou la protection des informations est alors essentielle aujourd'hui mais aussi à l'avenir.*

Au total, 19 compétences fonctionnelles et techniques composent les savoir-faire « cœur de métier » de la filière cybersécurité.

[39] % correspondant aux entreprises ayant répondu au et qui ont choisi ces compétences cybersécurité. Source : enquête en ligne EY menée auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité

[40] IDC, 2017, « Le marché de la cybersécurité pèsera 1,2 Md€ en France en 2020 »

Compétences fonctionnelles	Définition	Exemples de métiers associés
Analyse et cartographie des risques (EBIOS, MEHARI, ISO 27005, etc)	• Connaître et savoir mettre en pratique une ou plusieurs méthodologies d'analyse de risques. • Animer des ateliers de travails et réaliser les questionnaires de ces ateliers. • Restituer les risques au responsable métier	• RSSI • Consultant(e) et auditrice/auditeur gouvernance, risques et conformité • Correspondant(e) Sécurité • Chef de projet sécurité
Normes de sécurité (ISO 2700x)	• Connaître les différentes normes de sécurité existantes couvrant son périmètre de fonction. NB :Certaines certifications relatives à ces normes sont souvent demandées par les entreprises.	• RSSI • Directrice / directeur de programme sécurité • Consultant(e) et auditrice/auditeur gouvernance, risques et conformité • Architecte sécurité • Administratrice / administrateur et technicien(ne) sécurité • Expert(e) judiciaire en informatique
Elaboration des politiques et des procédures de sécurité	• Connaître l'articulation des différents référentiels de sécurité • Connaître les référentiels/normes relatifs au système de management de la SSI • Savoir exploiter une analyse de risques • Savoir rédiger l'ensemble des documents du référentiel (politiques, procédures, normes…)	• RSSI • Consultant(e) et auditrice/auditeur gouvernance, risques et conformité • Architecte sécurité • Administratrice / administrateur et technicien(ne) sécurité
Gestion des incidents de sécurité (cyber crise)	• - Détecter des incidents de sécurité • Qualifier des incidents de sécurité • Gérer le traitement des incidents de sécurité (pilotage des équipes) • Rédiger un post-mortem	• Responsable Security Operations Center • Chargé(e) de la réponse aux incidents • RSSI • Chef de projet sécurité
Gestion du plan de continuité et de reprise d'activité	• - Rédiger un PCA/PRA • Rédiger un plan de test • Piloter des tests de PCA/PRA • Identifier les évolutions à apporter au PCA/PRA	• Responsable du Plan de Continuité d'Activité • Responsable Security Operations Center • Administratrice / administrateur et technicien(ne) sécurité • Développeuse et développeur sécurité

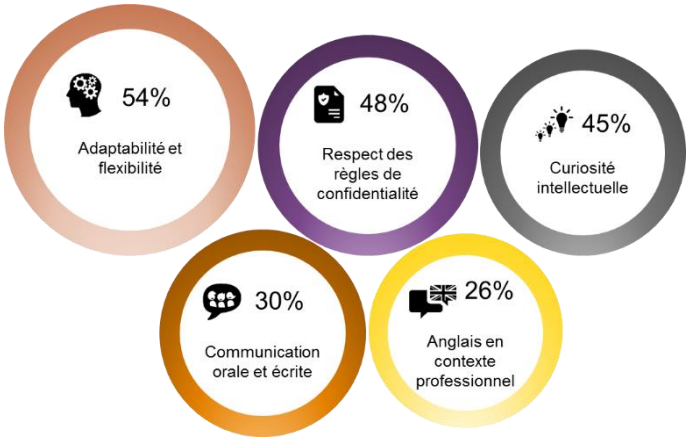
Compétences fonctionnelles	Définition	Exemples de métiers associés
Sensibilisation et formation aux enjeux de la sécurité	• Identification et création des scenarios de sensibilisation en tenant compte du contexte utilisateur (métier) • Animation des ateliers de formation et de sensibilisation • Réalisation des campagnes de sensibilisation et de formations	• RSSI • Chef de projet sécurité • Administratrice / administrateur sécurité • Consultant(e) et auditrice/auditeur gouvernance, risques et conformité • Cryptologue • Responsable du Plan de Continuité d'Activité
Veille sur les évolutions règlementaires (LPM, NIS, RGS…)	• Connaître les nouvelles règlementations • Identifier leurs impacts technologiques et organisationnels ; • Proposer des mesures de mise en conformité du SI	• Expert(e) judiciaire en informatique • Délégué(e) à la Protection des Données • Responsable du Plan de Continuité d'Activité • Administratrice / administrateur sécurité
Protection de la vie privée (data privacy)	• Identifier des données à caractère personnel • Connaître les contraintes imposées par les règlementations locales	• Délégué(e) à la Protection des Données • Architecte sécurité • Cryptologue • Responsable du Plan de Continuité d'Activité
Classification et protection des informations	• Définir une politique de classification des données • Définir les mesures de protection à mettre en œuvre selon ces classifications.	• Architecte sécurité • Chef de projet sécurité • Administratrice / administrateur et technicien(ne) sécurité • Responsable Security Operations Center

Compétences techniques	Définition	Exemples de métiers associés
Architecture de Sécurité (sondes, IDS, IPS…)	• Savoir construire une architecture technique sécurisée • Connaitre les différents équipements de sécurité existants • Connaitre leur périmètre d'actions • Savoir les configurer et les manager	• Architecte Sécurité • Chef de projet sécurité • Responsable Security Operations Center • Consultant(e) et auditrice/auditeur sécurité technique • Consultant(e) et auditrice/auditeur gouvernance, risques et conformité
Sécurité des réseaux et des télécommunications	• Comprendre le fonctionnement des réseaux informatiques • Savoir configurer des réseaux informatiques • Savoir sécuriser des communications	• Architecte sécurité • Administratrice/administrateur et technicien(ne) sécurité • Analyste cybersécurité • Consultant(e) et auditrice/auditeur sécurité technique • RSSI • Chargé(e) de la réponse aux incidents
Sécurité des systèmes d'exploitation	• Connaître les différents systèmes d'exploitation • Savoir configurer et administrer ces systèmes • Connaître les fonctionnalités étendues de ces systèmes et les paramétrer • Choisir le système répondant le mieux aux besoins	• Architecte sécurité • Administratrice/administrateur et technicien(ne) sécurité • Consultant(e) et auditrice/auditeur sécurité technique • Directrice / directeur de programme sécurité • Responsable du Plan de Continuité d'Activité • RSSI • Correspondant(e) sécurité
Sécurité des applications	• Connaître les principales vulnérabilités applicatives (Top 10 OWASP par exemple) • Comprendre la source de ces vulnérabilités • Savoir trouver ces vulnérabilités • Connaître les solutions de corrections et savoir les mettre en œuvre	• Consultant(e) et auditrice/auditeur sécurité technique • Responsable Security Operations Center • Administratrice / administrateur et technicien(ne) sécurité • Développeuse / développeur sécurité
Cryptographie	• Connaître et comprendre les différentes solutions de chiffrement (Symétriques, asymétriques…) • Connaître les principales méthodes de chiffrement (RSA, MD5…) • Connaître les méthodes de chiffrements robustes existants • Savoir choisir une méthode de chiffrement selon le besoin	• Cryptologue • Directrice / directeur de programme sécurité • Analyste cybersécurité • Consultant(e) et auditrice/auditeur gouvernance, risques et conformité • Expert(e) judiciaire en informatique

Compétences techniques	Définition	Exemples de métiers associés
	• Apporter son expertise dans la structuration de projets impliquant des techniques de chiffrement	
Détection, réponse à incident de sécurité	• Connaître les mécanismes de détection et de protection contre les menaces • Savoir analyser des menaces (malwares, vulnérabilités…) • Comprendre les nouvelles menaces et connaître les méthodes de traitement associées • Etre capable d'aider une entreprise à répondre à une attaque à grande échelle	• Responsable Security Operations Center • Analyste cybersécurté • Architecte sécurité • RSSI • Correspondant(e) sécurité
Gestion des accès et des identités	• Connaître les solutions de gestion des accès et des identités • Savoir déployer et manager ces solutions • Savoir choisir les solutions adaptées au contexte et au(x) besoin(s)	• Chef de projet sécurité • Administratrice/administrateur ou technicien(ne) sécurité • RSSI
Audit de sécurité (technique et organisationnel)	• Identifier les vecteurs de risques liés aux infrastructures et systèmes du SI • Identifier et présenter les vulnérabilités d'une organisation, d'un SI ou d'une infrastructure • Identifier les défauts de configuration • Identifier des risques au sein des procédures, processus et organisations • Analyser les solutions techniques	• Consultant(e) et auditrice/auditeur gouvernance, risques et conformité • Consultant(e) et auditrice/auditeur sécurité technique • Chef de projet sécurité
Tests d'intrusion	• Connaître les vulnérabilités les plus répandues • Connaître les méthodologies de tests d'intrusion • Savoir analyser son périmètre d'intervention (cartographie) et y rechercher des vulnérabilités • Savoir utiliser les outils essentiels à la réalisation de tests d'intrusion	• Consultant(e) et auditrice/auditeur sécurité technique • Responsable Security Operations Center • Correspondant sécurité • Architecte sécurité
Sécurité liée aux nouveaux usages	• Connaître les nouveaux usages • Etre en mesure d'analyser les impacts en termes de sécurité de l'information • Identifier des solutions en cas d'impacts négatif sur le niveau de sécurité du SI	• Architecte sécurité • Développeuse / développeur sécurité

Si la matrice des compétences techniques et fonctionnelles par métiers est indispensable (en Annexe 5), une approche des appétences ou capacités transverses est également importante afin de bien comprendre les profils recherchés aujourd'hui, mais également les ambitions à venir.

Les entreprises de la Branche ont sélectionné les principales capacités transversales sur lesquelles portent leurs attentes. Ci-dessous un « top 5 » des capacités que les professionnels en cybersécurité devront développer lors de leurs formations et expériences professionnelles :



LE « TOP 5 » DES CAPACITES TRANSVERSALES RECHERCHEES PAR LES ENTREPRISES DE LA BRANCHE POUR LES PROFESSIONNELS DE CYBERSECURITE[41]

A ces cinq principales capacités transversales, s'ajoutent également des attentes en termes de :

Ces capacités transversales, attendues pour les professionnels de cybersécurité, ne sont pas spécifiques à la filière. Quand le respect des règles de confidentialité est un point d'attention particulièrement important pour un acteur de la cybersécurité, le travail en équipe est la première compétence transverse attendue pour l'ensemble des filières[42] mais concentrant peu d'attentes en cybersécurité. Pourtant, la capacité à travailler en équipe reste d'autant plus critique dans une période où les frontières de l'entreprise s'étendent et où l'on constate de plus en plus de cas d'entreprises « étendues » : écosystème avec des sous-traitants, des partenaires, des fournisseurs au sein d'une filière ou d'un territoire par exemple.

[41] Source : enquête en ligne EY menée auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité (périmètre : Branche)

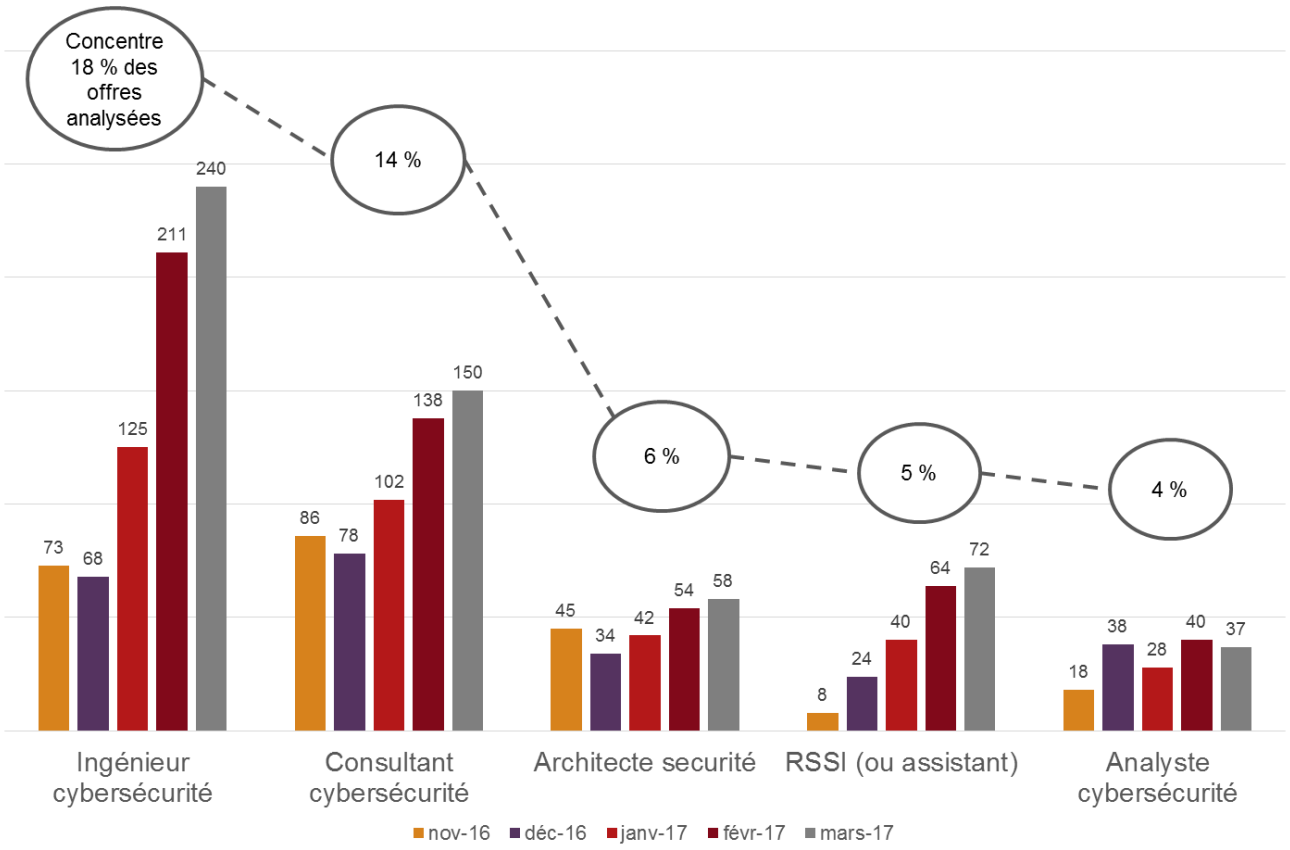
[42] Sondage CSA, sur les compétences comportementales importantes dans les 5 années à venir, La Révolution des Métiers, EY-LinkedIn, 2014

2.4 Des métiers très recherchés !

La plupart des entreprises met en exergue le manque de ressources et compétences dans le domaine de la cybersécurité. Au niveau mondial, plus d'un million de postes sont non pourvus en cybersécurité[43]. En France également, les profils spécialisés en cybersécurité sont très convoités par les entreprises : seulement 25% des besoins en recrutement dans le secteur sont couvert en 2015[44]

Les entreprises françaises investissent de plus en plus dans la sécurité de leurs réseaux. Les bons profils professionnels, encore trop rares, sont recherchés.[45]

Les métiers de la cybersécurité sont nombreux et répondent à des besoins de compétences diverses. Cependant, les offres d'emplois actuelles[46] se concentrent sur un nombre plus restreint de métiers : près de la moitié des offres d'emplois se concentrent sur 5 métiers en cybersécurité. L'analyse de plus de 4000 annonces en ligne a permis d'illustrer cette dynamique :



PRES DE LA MOITIE DES OFFRES D'EMPLOI ANALYSEES EN CYBERSECURITE EST CONCENTREE SUR 5 METIERS[47]

[43] CyberCercle, PwC, 14 décembre 2016
[44] Estimation ANSSI, Les Echos.fr, janvier 2016 « Cybersécurité : recherche candidats désespérément »
[45] Le Parisien Eco, Novembre 2016, « La France booste la cybersécurité »
[46] Périmètre de la filière cybersécurité en France
[47] Analyse EY des offres d'emplois pour la filière cybersécurité entre novembre 2016 et mars 2017

Il convient de noter que cette analyse des annonces en ligne ne vise pas une représentativité des recrutements :

- premièrement parce que ces annonces ne sont qu'un échantillon de toutes les offres en ligne, dont la représentativité n'est pas démontrée ;
- deuxièmement parce que seulement une part des recrutements font l'objet d'une annonce en ligne (2ème canal de recrutement utilisé par les entreprises de la Branche après le bouche à oreille)
- troisièmement parce qu'une annonce n'est pas forcément synonyme d'une offre d'emploi (une annonce vise à identifier un profil pour un ou plusieurs postes disponibles, et peut être renouvelée sur plusieurs mois)

Plus précisément, les entreprises de la Branche ont exprimé leur volonté actuelle de recruter des professionnels en cybersécurité :

« TOP 5 » DES METIERS QUE LES ENTREPRISES DE LA BRANCHE RECRUTENT ACTUELLEMENT[48]

D'un point de vue quantitatif, les besoins des entreprises de la Branche sur la création nette de postes à horizon 3 ans peuvent s'exprimer sur ces 5 métiers[49] :

- 200 postes créés en consultants en cybersécurité,
- 100 postes d'analyste SOC (Security Operations Center),
- 100 nouveaux chefs de projet en sécurité (à l'interface entre compétences techniques et management de projet),
- 80 architectes sécurité,
- 80 administrateurs sécurité.

Ces cinq métiers concentrent ainsi 40% des créations nettes estimées de postes pour le périmètre Branche à horizon 3 ans. Ces métiers répondraient ainsi aux attentes prioritaires et immédiates des entreprises en termes

[48] Source : enquête en ligne EY menée auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité (périmètre : Branche)

[49] Modélisation : estimation des effectifs au sein de la Branche, EY 2017. Enquête en ligne et analyse des offres d'emplois en ligne, 2016

de cybersécurité. Plus largement, ces métiers sont également vecteurs des compétences associées à rechercher demain pour la filière. Ils s'adressent aux deux principales problématiques et facteurs de croissance de la filière[50] :

- D'une part, la gestion de la sécurité et des vulnérabilités qui vont se complexifier notamment avec les évolutions réglementaires (GDPR…)
- D'autre part, la gestion des identités et des accès, pressentie comme le second grand chantier qui animera la filière à l'horizon 2020, avec notamment le développement des objets connectés donc les habilitations d'accès doivent être gérées.

[50] IDC, 2017, « Le marché de la cybersécurité pèsera 1,2 Md€ en France à horizon 2020.

III. La cybersécurité de demain[51]

3.1 Un enjeu de « massification » de la filière

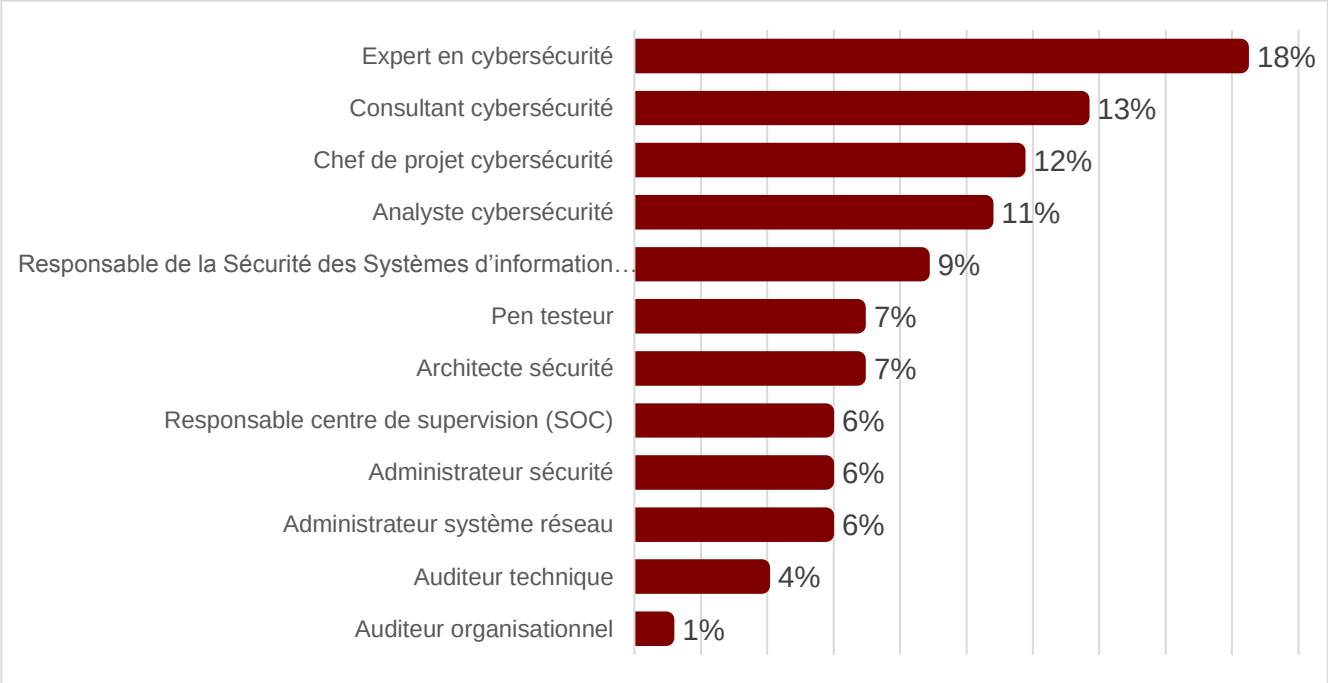
Les besoins des entreprises sont immédiats mais vont également s'accroitre dans le temps en raison de l'émergence des nouvelles technologies et du renforcement des réglementations.

Les entreprises ont exprimé leur volonté de recruter un certain nombre de métiers en cybersécurité, à la fois pour répondre au renouvellement et au renforcement de leurs équipes. Cependant, les attaques se multiplient et sont de plus en plus complexes ce qui nécessite d'avoir des profils qualifiés avec une forte expertise sur le sujet.

Les entreprises rencontrent des difficultés de recrutement aujourd'hui, qui les placent parfois en difficulté par manque de ressources.

Seulement 1 entreprise sur 3 ne rencontre pas de difficultés de recrutement[52]

Ci-dessous, les principaux métiers en cybersécurité dits « en tension » pour les entreprises :



PRINCIPAUX METIERS OU LES ENTREPRISES RENCONTRENT DES DIFFICULTES DE RECRUTEMENT

[51] Cette partie relève de tendances prospectives pour l'ensemble de la filière cybersécurité – tendances qui s'appliquent également aux entreprises de la Branche

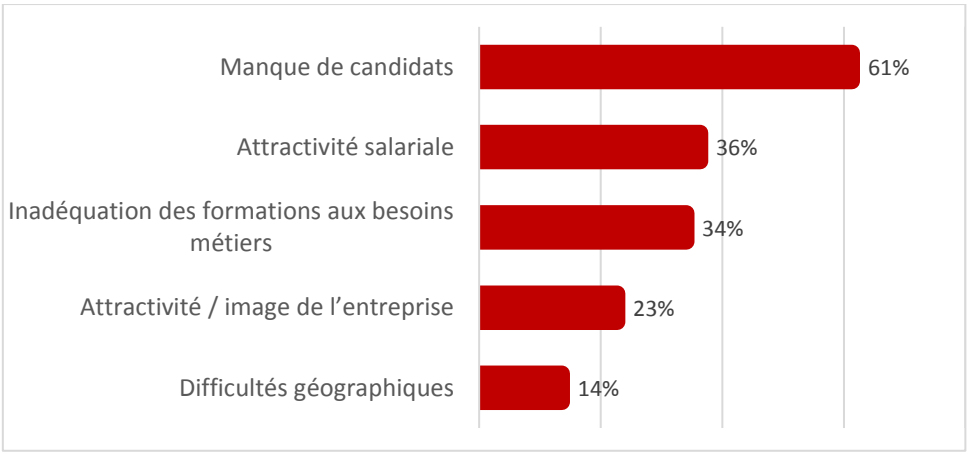
[52] Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité (périmètre : entreprises de la Branche et hors Branche)

La première raison invoquée par les entreprises concernant ces difficultés de recrutement est le manque de candidat (61%[53]). Ce point met l'accent sur la pénurie de talents en cybersécurité à laquelle les entreprises sont confrontées. La filière cybersécurité est ainsi face à un enjeu de massification. Les professionnels formés ne sont pas assez nombreux pour répondre aux demandes des entreprises.

Ce manque de candidat soulève une série d'interrogations : Quelle est l'attractivité de la filière ? Les attentes des acteurs sont-elles bien formulées / relayées auprès des candidats ? L'offre de formation et de certification est-elle suffisamment lisible ? Quels sont les parcours professionnels possibles en cybersécurité ?

> *« Nous avons une nécessité de faire évoluer nos solutions logicielles au regard des thématiques sécurités, afin de garantir auprès de nos clients des solutions fiables en termes sécuritaires, cela implique des recrutements mais aussi des compétences plus pointues »*[54]

Le manque de candidats est la principale raison des difficultés de recrutement rencontrées par les entreprises, mais n'est pas la seule. L'attractivité salariale et l'inadéquation des formations aux besoins métiers sont aussi des éléments explicatifs cités par les entreprises. Les niveaux d'exigence et de compétence des candidats ne semblent pas toujours correspondre aux attentes des entreprises. Enfin, des entreprises expliquent aussi leurs difficultés de recrutement par une attractivité relative de l'entreprise et des difficultés liées à la l'implantation géographique de l'entreprise[55].



PRINCIPALES RAISONS DES DIFFICULTES DE RECRUTEMENT RENCONTREES PAR LES ENTREPRISES

[53] Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité (périmètre : entreprises de la Branche et hors Branche)

[54] Citation d'une entreprise ayant répondu à l'enquête en ligne EY sur les effectifs et les besoins des entreprises en cybersécurité

[55] Il s'agit aussi bien d'entreprises implantées en Ile-de-France, qu'en Auvergne-Rhône-Alpes, en Provence-Alpes-Côte d'Azur et en Occitanie. Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité

3.2 Une transformation des compétences et des métiers clés à accompagner

Un métier est amené à évoluer, intégrant à la fois les changements globaux auxquels sont confrontés les entreprises et le renouvellement / le développement de compétences. 90% des décisionnaires anticipent des évolutions, voire même des changements de métiers dans les années à venir au sein de leurs entreprises[56]. Le domaine principal de changement pour ces métiers est justement celui de l'informatique et du digital, devant la logistique, la finance et le marketing[57].

> *Demain, sous un intitulé de fonction inchangé depuis des années, la réalité vécue par un professionnel aura radicalement changé, notamment sous la pression de la technologie et de la globalisation. – La Révolution des Métiers, EY-LinkedIn*

Une tendance à la spécialisation

La cybersécurité se constitue en tant que filière au sens d'un ensemble d'activités complémentaires exercées par ces professionnels. Une des caractéristiques de cette filière est son degré d'expertise, important et en croissance. Face aux enjeux stratégiques auxquels elles doivent faire face, les entreprises recrutent avant tout des profils spécialisés[58]. La complexification de la gestion de la sécurité, des vulnérabilités, des accès ou encore des identités sont autant d'éléments nécessitant des professionnels de la cybersécurité aux compétences techniques et fonctionnelles avérées. La montée en expertise du professionnel est une attente forte du marché français : à la fois pour un plus grand nombre d'experts, mais aussi avec des compétences techniques plus maitrisées et à développer.

> *« Dans le cadre d'un marché qui se structure en France, encouragée par les nouvelles technologies et poussée par la montée en puissance des attaques internet et leur médiatisation, la cybersécurité pourrait, à terme, représenter une vitrine de la compétitivité française. »*[59]

[56] La Révolution des Métiers « Nouveaux métiers, nouvelles compétences : quels enjeux pour l'entreprises ? », EY & LinkedIn, 2014

[57] Sondage CSA sur les domaines des métiers qui vont évoluer le plus fortement dans les 5 ans à venir, La Révolution des Métiers, EY-LinkedIn, 2014

[58] L'étudiant, 2015, « Cybersécurité : passez à l'attaque du secteur, cela recrute ! »

[59] BPI France, juillet 2016 « La cybersécurité, une filière d'avenir pour l'offre française »

Des profils transversaux

Une tendance à la spécialisation des métiers est dès aujourd'hui observable et s'accompagne d'un mouvement parallèle de recherche de profils transversaux capables de « parler toutes les langues » de la cybersécurité. C'est-à-dire à une connaissance et compréhension globale des différentes techniques et outils en cybersécurité (sans atteindre une maitrise sur l'ensemble) et une capacité à faire le lien entre les différents professionnels de cybersécurité mais aussi avec les dirigeants d'entreprises sur les aspects stratégiques des problématiques de cybersécurité.

LA RECRUE IDEALE ? UN CAMELEON[60]

« Les professionnels de cybersécurité, peut être dû à leur formation, manquent d'une approche transversale des problématiques : les 360 ° »[61]

Une montée des volets stratégiques

De fonctions dites « support » il y a plusieurs années, la cybersécurité est aujourd'hui devenue jusqu'à un levier de compétitivité pour les entreprises[62]. La cybersécurité devient progressivement un avantage compétitif pour l'entreprise. Au cœur des produits et processus internes, ce sujet atteint les volets stratégiques pour les entreprises. Véritable enjeu pour les directions, il convient alors de sensibiliser voire former les professionnels non spécialisés en cybersécurité. Les comités exécutifs (COMEX) de grandes entreprises se saisissent du sujet, faisant alors appel à une diversification des compétences tant pour les professionnels de cybersécurité plus seulement attendus sur leur maitrise des compétences techniques et fonctionnelles mais aussi sur leur esprit de synthèse, et leur capacité de management.

Le monde de la sécurité reste encore trop technique donc incompréhensible par les directions générales. Il faut absolument que les directions Sécurité abordent le problème par les risques et non par la technique.[63]

[60] La Révolution des Métiers « Nouveaux métiers, nouvelles compétences : quels enjeux pour l'entreprises ? », EY & LinkedIn, 2014

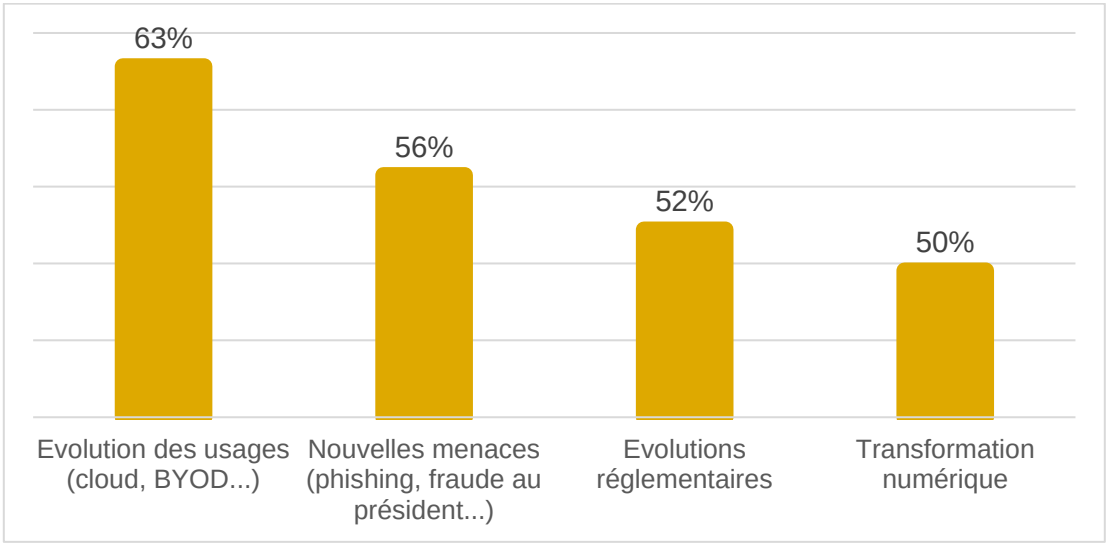
[61] Citation d'une entreprise ayant répondu à l'enquête en ligne EY sur les effectifs et les besoins des entreprises en cybersécurité

[62] Sopra Steria, 2016, « Quand la sécurité devient un avis levier compétitif »

[63] CyberCercle, PwC, 14 décembre 2016

3.3 Identifier et faire émerger les métiers de la cybersécurité de demain

Une autre caractéristique de cette filière réside dans son caractère dynamique : les technologies évoluent très vite, et les besoins des entreprises se développent aussi rapidement. Les métiers existants évoluent, avec des attentes : pour de nouvelles compétences, mais aussi pour un plus fort niveau de maitrise de certaines compétences existantes. Les entreprises de la Branche ont identifié quatre grands facteurs d'évolution de ces métiers :



PART DES ENTREPRISES AYANT CHOISI CES ELEMENTS COMME PRINCIPAUX FACTEURS D'EVOLUTION DES METIERS[64]

QUELLES COMPETENCES RECHERCHEES A HORIZON 5 ANS ?[65]

Le professionnel de demain devra développer ses compétences sur la protection des informations, la sécurité des applications et l'audit de sécurité.

Le degré de maitrise pourra varier d'un métier à l'autre au vu de la diversité des principaux métiers identifiés, mais donne cependant une tendance générale pour la filière.

Les entreprises se sont aussi exprimées de manière moins prononcée sur des attentes pour les compétences suivantes : le traitement des vulnérabilités, la supervision des projets, la gestion et l'analyse des risques, la conformité, la détection/réaction aux incidents…

[64] Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité (périmètre : entreprises de la Branche et hors Branche)

[65] Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité (périmètre : entreprises de la Branche et hors Branche)

L'évolution des compétences et des métiers en cybersécurité nécessitent une adaptation des cursus de formation pour les actuels et futurs professionnels. Filière particulièrement dynamique, la formation se doit d'être à la pointe des technologies voire moteur de ces transformations par des programmes performants à la fois sur la formation initiale et continue.

Digital Risk Manager-Officer

Security & Privacy (or Digital Security) Compliance Manager

Analyste big data

Pilotages de prestations extérieures en cybersécurité

Juriste cybersécurité

Responsable Sécurité des Systèmes Industriels

Responsable de la sécurité des objets connectés (IOT)

Expertise sécurité pour PME et TPE

Consultants cybersécurité systèmes spécifiques (industrie, énergie, transport…)

Cloud Manager

Risk cybersécurité manager

Sécurisation des applications mobiles et objets connectés

EVOLUTIONS DES METIERS ET COMPETENCES EXISTANTES, ET L'EMERGENCE DE NOUVEAUX METIERS ?[66]

[66] Source : entretiens menés et enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité (périmètre : entreprises de la Branche et hors Branche)

PARTIE 2 : ETAT DES LIEUX DE L'OFFRE DE FORMATION

I. Principaux résultats

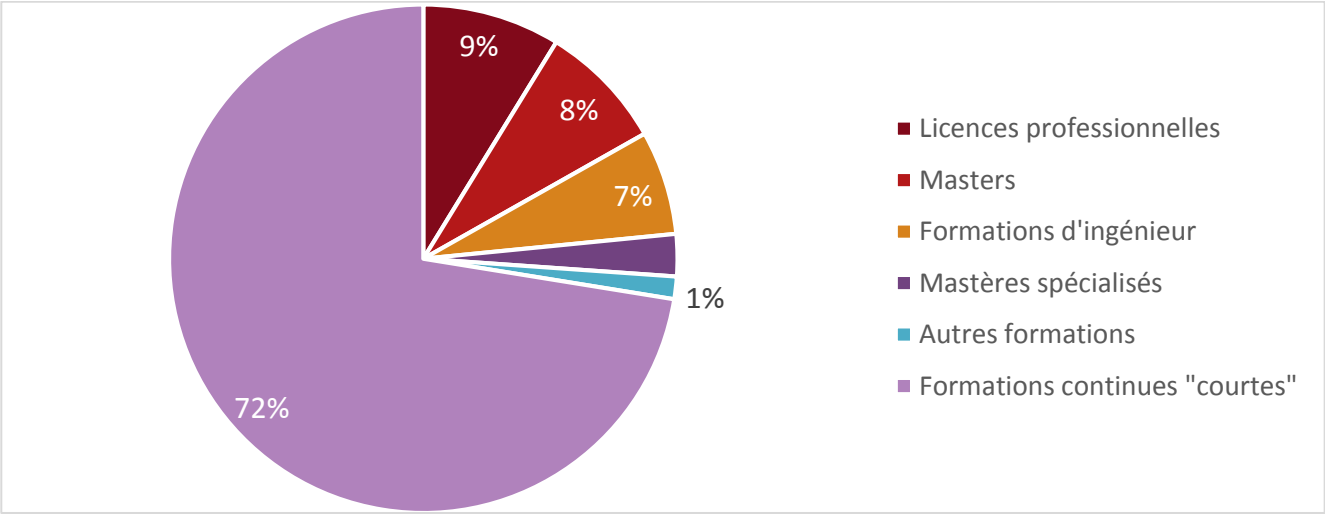
Au total, plus de 550 formations ont été identifiées, avec une forte diversité en termes de durée (formations courtes et formations longues) et en termes de structures formatrices, allant des établissements d'enseignement supérieur aux organismes de formation privés. Nous avons recensé la plupart des formations en cybersécurité en France, que nous avons classifiées en 8 catégories :

Près de 150 formations dispensées par des établissements d'enseignement supérieur :

- 48 licences professionnelles
- 45 masters
- 37 formations d'ingénieur
- 15 mastères spécialisés
- 8 autres formations (type BADGE[67], bachelor…)

Plus de 400 formations dispensées par des organismes privés :

- 242 formations techniques
- 102 formations en management de la sécurité
- 46 formations d'audit
- 15 formations en sécurité juridique



REPARTITION DES FORMATIONS EN CYBERSECURITE PAR TYPE DE FORMATION

Cette cartographie n'a pas vocation à être exhaustive de l'ensemble des formations françaises en cybersécurité, et n'inclut pas les formations dites de « sensibilisation » à la cybersécurité. Le focus est fait ici sur les formations professionnalisantes, proposant des cursus de qualité reconnus par les professionnels et les experts du secteur. Cet état des lieux a été réalisé de janvier à février 2017.

[67] Bilans d'Aptitudes Délivrés par les Grandes Ecoles

II. Formations dispensées par les établissements d'enseignement supérieur

1.1. Un point de départ : les labélisations des formations menées par l'ANSSI

L'ANSSI a réalisé un premier référencement (non exhaustif) des formations délivrant un titre reconnu par l'Etat de niveau équivalent à Bac+3 jusqu'à Bac+5, faisant état de 69 formations initiales : 24 licences professionnelles et 45 formations de niveau Bac+5.[68]

« On ne peut pas comparer une licence professionnelle avec le diplôme d'une école d'ingénieur, chaque formation a sa place et ses spécificités », Pascal Chour pour Mag-Securs, 2017

En 2016, l'ANSSI a souhaité améliorer le référencement des formations en sécurité du numérique par la mise en place d'un processus de labélisation[69] qui éprouve et garantit la pertinence de la formation par rapport à ses objectifs. Un programme de labélisation des formations a été lancé, dévoilant au FIC en janvier 2017 vingt-six formations. D'autres dossiers sont en cours d'instruction : des labélisations supplémentaires sont à prévoir.

SecNumedu
ANSSI

« [Ce label a] pour but de rendre plus visibles et plus lisibles pour les intéressés les formations de cette spécialité », Guillaume Poupard en page Tribune, 2017

La labélisation des formations certifie la conformité d'une formation vis-à-vis du cahier des charges demandé dans le dossier de certification et la charte d'engagement de l'établissement. Parmi les critères quantitatifs, par exemple, le volume de cours et de travaux pratiques dédiés à la sécurité doit être supérieur à 70%[70]. Construite sur une base déclarative, cette labélisation ne préjuge en rien néanmoins de l'évaluation de la qualité des enseignements proposés.

26 formations ont été labélisées SecNumEdu:

- 8 licences professionnelles
- 7 masters
- 6 formations d'ingénieur
- 5 mastères spécialisés

10 formations labélisées intègrent des certifications dans leurs cursus : "Stormshield" (Airbus DS Cybersecurity), CISCO, CCNA, ISO 27001 Lead Implementer et Lead auditor.

[68] La liste de formations référencées par l'ANSSI est disponible à l'adresse suivante : https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/
[69] Le référentiel de labélisation est disponible à l'adresse suivante : https://www.ssi.gouv.fr/entreprise/formations/secnumedu/
[70] Interview pour : « Le challenge de la formation aux compétences SSI »Mag Sécurs, 2017

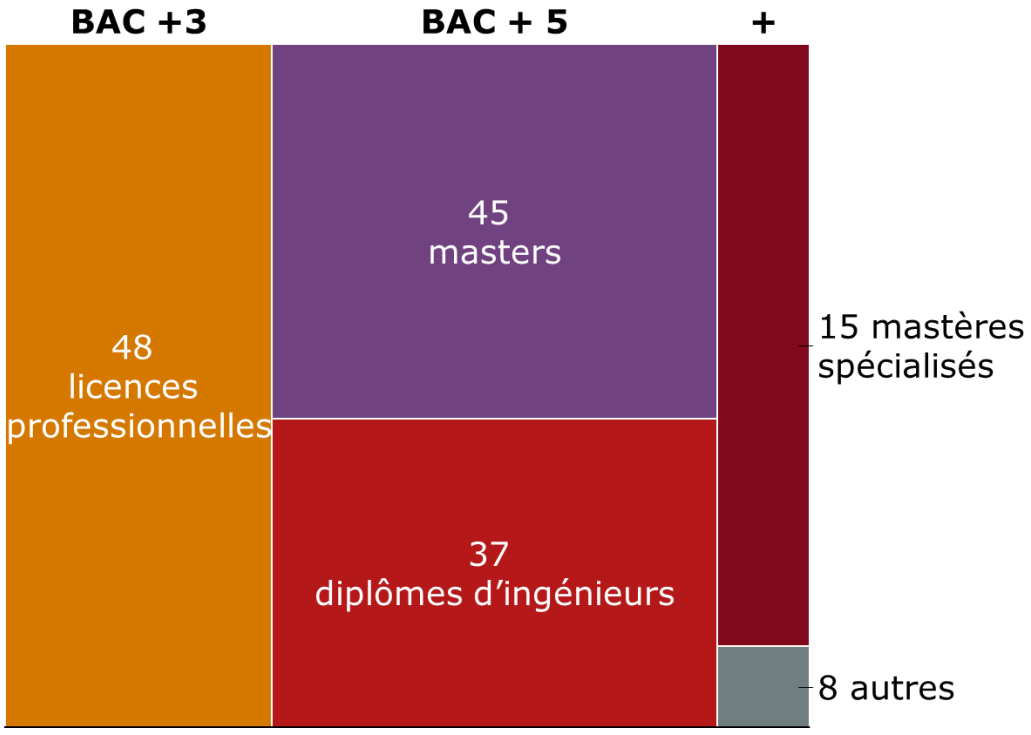
1.2. Etat des lieux des formations longues

❖ *Nombre*

Nous estimons qu'une formation est considérée comme longue à partir du moment où le nombre de jours de formation est supérieur à 1 mois.

Cette liste fait état de près de 150 formations initiales aboutissant à des diplômes délivrés au niveau Bac+3 et Bac+5. La liste des formations est placée en annexe du document, avec les informations suivantes :

- Nom de l'organisme
- Intitulé de la formation
- Type de formation (master, licence professionnel…)
- Localisation
- Formation initiale/formation continue/VAE
- Formation enregistrée au CNCP (répertoire ou inventaire)
- Labélisation SecNumEdu.



REPARTITION DES FORMATIONS LONGUES EN CYBERSECURITE

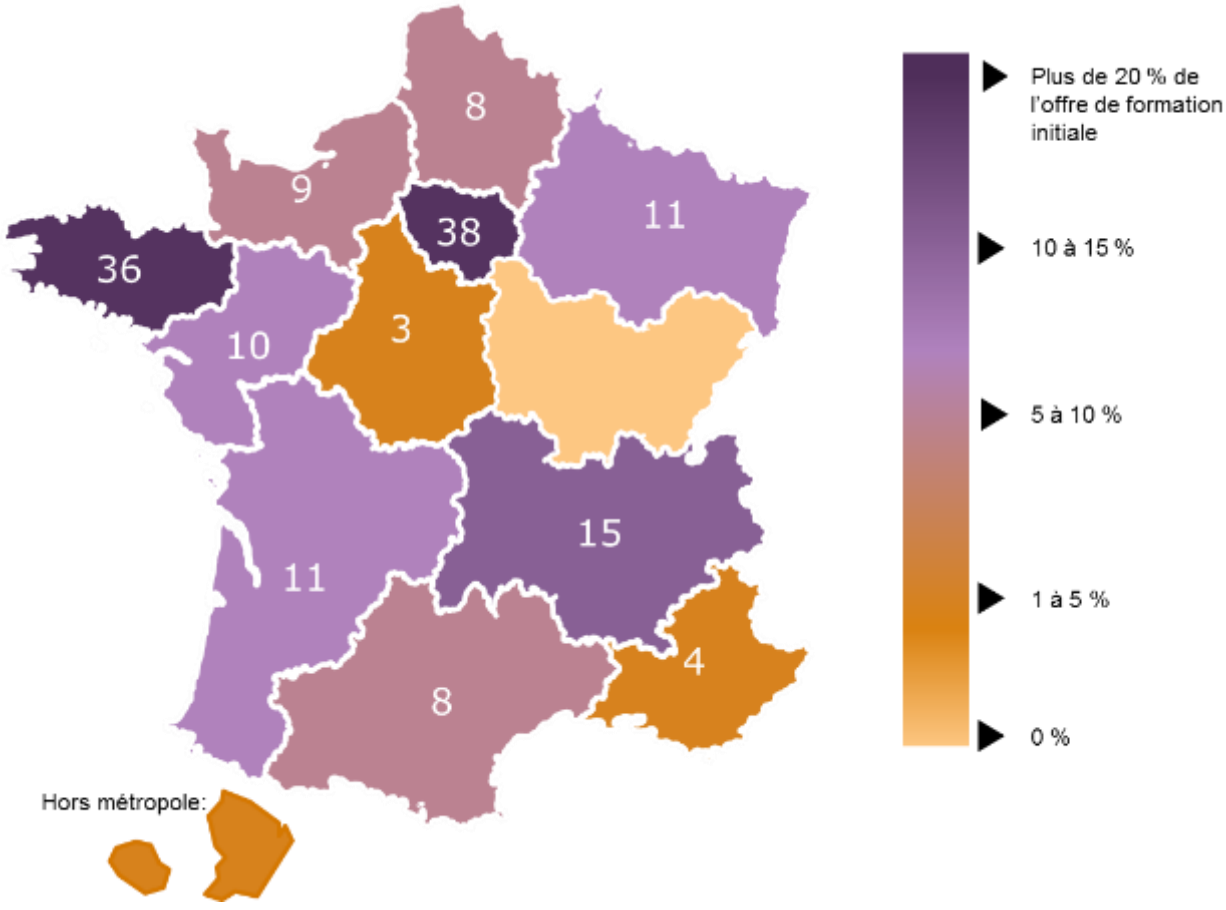
❖ *Répartition géographique*

Les établissements d'enseignement supérieur proposant une formation en cybersécurité couvrent quasiment l'ensemble des régions françaises. Cette répartition n'est pas homogène sur le territoire, avec trois régions qui concentrent plus de la moitié de l'offre de formation longue dispensée par les établissements d'enseignement supérieur :

- L'Ile-de-France concentre 25% de l'offre de formation
- La Bretagne 23%
- La région Auvergne-Rhône-Alpes 10%.

Avec plus de 30 formations proposées, la Bretagne joue un rôle particulièrement moteur pour la formation en France en cybersécurité. Un Pôle d'Excellence Cyber (PEC) s'est constitué, initié par le ministère de la Défense avec l'appui du Conseil Régional. L'ensemble des opérateurs de formation sont ainsi mobilisés pour le développement de la filière, promouvant la recherche, la formation et le développement du tissu industriel.

La carte ci-dessous donne la répartition régionale des formations longues identifiées :



REPARTITION GEOGRAPHIQUE DES FORMATIONS LONGUES IDENTIFIEES

❖ *Messages clés*

- **Une offre de formation qui se développe**

L'offre de formation est importante avec des enseignements dispensés partout en France. Il y a à la fois une forte diversité des types de formations longues, avec des formations historiques ainsi que des formations nouvellement créées.

> *« Dans le domaine de la cybersécurité et de la sécurité de l'information, des concepts devenus de fait, à la pointe de l'actualité, les formations initiales se multiplient : on ne compte plus le nombre de Masters ou de Mastères, de Licences Professionnelles qui se créent chaque année dans ces secteur »*[71]

- **Un taux de remplissage moyen de 83% des formations**

Si certaines formations en cybersécurité affichent un taux de remplissage important[72], elles ne sont pas en état de saturation. Il convient de s'interroger sur l'attractivité de ces formations auprès des étudiants.

> *« Très souvent, il y a moins d'élèves que de places disponibles : cela pose question ! Sur l'attractivité des formations ? Sur le niveau des élèves retenus ?... »*[73]

Ces places restantes non attribuées ne signifient pas forcément un manque de candidatures. Pour certaines formations notamment les mastères spécialisés, les dossiers de candidatures sont très nombreux. La sélection à l'entrée de ces cursus, souvent forte et exigeante au regard des enjeux de la filière, et le manque de prérequis de certaines candidatures expliquent que ces formations très demandées disposent de 17% de places à pourvoir.

> *« Nous recevons beaucoup de dossiers de candidature, parfois jusqu'à 75% de demandes de la part d'élèves étrangers. Mais dans ces dossiers, nous avons un manque de candidats qualifiés après la sélection des dossiers. » - Responsable de formation*

- **Les établissements d'enseignement supérieur s'ouvrent de plus en plus aux professionnels**

Une tendance s'observe sur le marché de la formation continue : les écoles prennent un rôle croissant en s'adressant directement aux professionnels du secteur.

> *« Les établissements d'enseignement supérieur se structurent pour offrir des formations qui répondent aux besoins du marché. »*[74]

[71] « Le challenge de la formation aux compétences SSI »Mag Sécurs, 2017
[72] Sur les 18 formations qui ont renseignées le nombre de places et d'étudiants.
[73] Expert du secteur
[74] « Cybersécurité : l'enseignement supérieur passe à l'attaque », L'étudiant, Septembre 2015

Des établissements d'enseignement supérieur ont développé, en plus d'une formation initiale en cybersécurité, des formations s'adressant aux professionnels déjà en poste. Cette offre peut prendre la forme de formations longues voire de formations courtes, constituées parfois en collaboration avec des entreprises.

Ces offres ont pour objectif de répondre aux besoins des entreprises sur tous les aspects multidimensionnels de la cybersécurité en proposant aussi bien des cursus experts, qui peuvent s'adapter au contexte de l'entreprise cliente, que des cours plus généraux, de sensibilisation.

- **Métiers ciblés après ces formations initiales**

L'ensemble des familles de métiers sont couverts par les formations suivantes :

- Les licences professionnelles préparent principalement aux familles de métiers suivantes : maintien en condition et conseil, audit et expertise en sécurité.
- Les formations de niveau master permettent aux étudiants de s'orienter vers des métiers de la famille du conseil, audit et expertise en sécurité, et la famille de pilotage, organisation de la sécurité et gestion des données.
- Les formations de type ingénieur ont tendance à former des professionnels pour les familles de métiers suivantes : management de projets de sécurité et cycle de vie de la sécurité ; conseil, audit et expertise en sécurité ; et pilotage, organisation de la sécurité et gestion des risques.
- Enfin, les mastères spécialisés sont des cursus permettant une orientation vers l'ensemble des métiers de la cybersécurité (dans une moindre mesure pour la famille de métiers : maintien en condition).

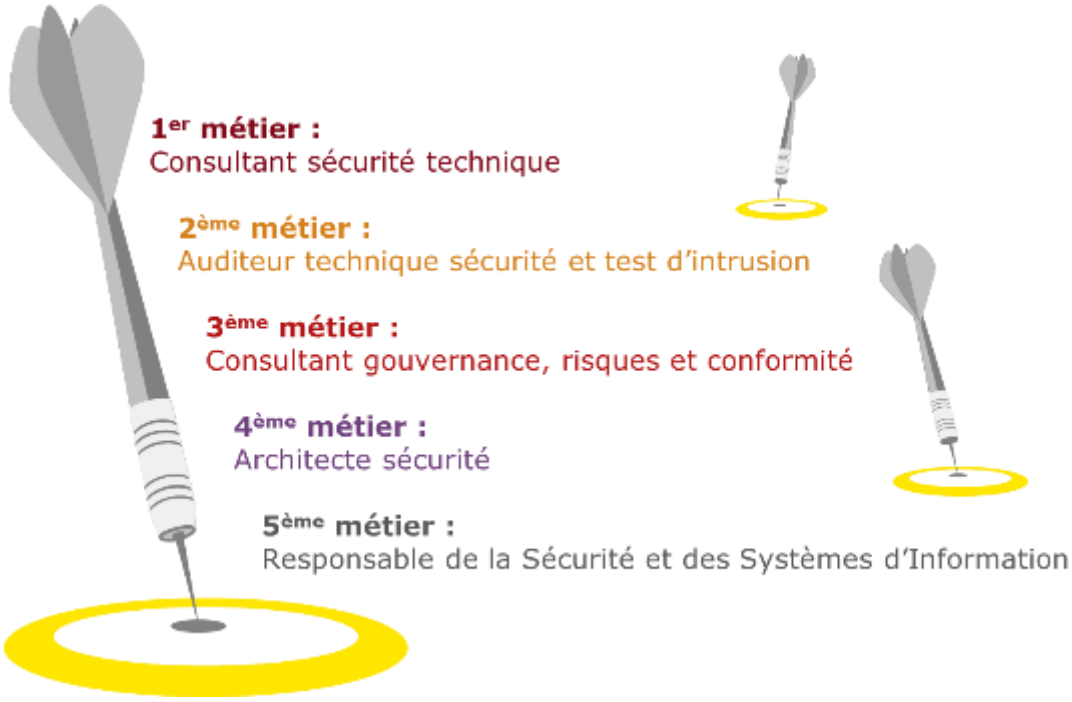
Lecture : 22% des licences professionnelles proposent des cursus permettant une orientation dans les métiers du pilotage, de l'organisation de la sécurité et de la gestion des risques.

Formations	Famille de métiers					Exemples de métiers :
	1. Pilotage, organisation de la sécurité et gestion des risques	2. Management de projets de sécurité et cycle de vie de la sécurité	3. Maintien en condition	4. Support et gestion des incidents de sécurité	5. Conseil, audit et expertise en sécurité	
Licences professionnelles (18)	22%	39%	50%	28%	56%	Technicien sécurité Intégrateur-développeur…
Master (12)	58%	33%	17%	25%	92%	Consultant sécurité technique…
Ingénieur (9)	56%	100%	0%	11%	89%	Architecte sécurité Consultant technique sécurité…
Mastère spécialisé (5)	60%	60%	20%	60%	100%	Consultant gouvernance, risques et conformité Auditeur organisationnel RSSI…

MATRICE DES FORMATIONS INITIALES PAR FAMILLE DE METIERS[75]

[75] Information collectée sur 44 formations, Principalement sur la labélisation SecNumEdu et pour les formations inscrites au RNCP de la CNCP.

La liste ci-dessous présente le top 5 des métiers les plus ciblés par les formations en termes de débouchés :



« TOP 5 » DES DEBOUCHES APRES LES FORMATIONS LONGUES[76]

Les sous-parties suivantes présentent de manière plus détaillée les formations dispensées par les établissements d'enseignement supérieur.

1.3. Les licences professionnelles en cybersécurité

Type de formation	Licences professionnelles
Nombre de formations recensées :	48
Formations enregistrées au répertoire de la CNCP :	37
Formations labélisées SecNumEdu :	8
Formation initiale / formation continue / VAE :	46 / 36 / 37
Exemples d'intitulés de formation : (liste complète fournie en annexe)	- Parcours « Réseaux Sans Fil et Sécurité » (RSFS) - Parcours « Administration et Sécurité des Réseaux » (ASUR) - Parcours « Administration et Sécurité des Systèmes et Réseaux » - …

[76] Données disponibles auprès de 28 formations sur les principaux métiers cibles.

Caractérisation des licences professionnelles labélisées par SecNumEdu

- 8 licences professionnelles labélisées SecNumEdu au 24.01.2017
- 10 ans d'ancienneté des formations en moyenne pour les licences professionnelles[77]
- 23 places par promotion en moyenne pour les licences professionnelles. Par rapport à d'autres types de formations (master, école d'ingénieur…), les licences professionnelles sont constituées de promotions plus réduites. Le nombre de places ne peut que difficilement évoluer, contraint par les équipements informatiques nécessaires et par le fonctionnement nécessaire en effectifs réduits.
- 160 places disponibles parmi 7 formations labélisées
- 152 élèves formés à la dernière année de promotion parmi 7 formations labélisées
- 94% de taux de remplissage moyen, avec des taux allant de 86% à 115%. Deux licences professionnelles ont rempli en totalité les places disponibles au sein de leur formation, présentant ainsi un taux de remplissage supérieur ou égal à 100% :
    - La licence professionnelle « Réseaux Informatiques, mobilité et sécurité » (LP RSFS-RIMS) de l'IUT de Saint Malo (115%)
    - La licence professionnelle « Administration et sécurité des systèmes et des réseaux » de l'IUT de la Roche-sur-Yon (100%)
- 4 mois d'expérience au sein d'une entreprise inclus dans le cursus (en alternance ou en stage).

[77] L'ancienneté des formations correspond au nombre de promotions de ce programme de formation. L'ancienneté peut être inférieure à celle de l'établissement si celui-ci a choisi de développer cette formation plus récemment. Ces informations ont notamment fait l'objet d'une déclaration pour la labélisation SecNumEdu. L'ancienneté est fondée sur des éléments déclaratifs. Aucun traitement des données n'a été réalisé.

1.4. Les masters en cybersécurité

Type de formation	Masters
Nombre total de formations recensées :	45
Formations enregistrées au répertoire de la CNCP :	17
Formations labélisées SecNumEdu :	7
Formation initiale / formation continue / VAE :	45 / 17 / 17
Exemples d'intitulés de formation : (liste complète fournie en annexe)	- Master « Management des risques et des systèmes d'information » (MRSI) - Master « Sécurité des systèmes d'information et de communication » (SSIC) - Master « Sécurité, audit, informatique légale » (SAFE) - …

Caractérisation des masters labélisés par SecNumEdu

- 7 masters labélisés SecNumEdu au 24.01.2017
- 20 ans d'existence moyenne de ces masters. La formation la plus ancienne identifiée par ce label est le Master Cryptis proposé à l'Université de Limoges considéré parmi les masters « historiques » de la filière car il forme depuis 30 ans des experts en sécurité informatique et en cryptologie.
- 37 places par promotion proposées en moyenne dans les masters, soit les promotions les plus nombreuses en cybersécurité avec les formations d'ingénieurs
- 219 places disponibles parmi 6 formations labélisées
- 176 élèves formés à la dernière année de promotion parmi 6 formations labélisées
- 78% de taux de remplissage moyen, avec des taux allant de 67% à 100%. Seul un master remplit en totalité les places disponibles pour la dernière promotion renseignée : le master de l'université de Lyon II intitulé « OPSIE : Organisation et Protection des Systèmes d'Information pour l'Entreprise ».
- 5 mois de stage inclus dans le cursus.

1.5. Les titres d'ingénieur en cybersécurité

Type de formation	Formations d'ingénieur
Nombre total de formations recensées :	37
Formations enregistrées au répertoire de la CNCP :	8
Formations labélisées SecNumEdu :	6
Formation initiale / formation continue / VAE :	37 / 7 / 6
Exemples d'intitulés de formation : (liste complète fournie en annexe)	- Ingénieur « Systèmes d'information sécurisés » (SIS) - Ingénieur « Sécurité des réseaux et des systèmes » - Ingénieur « Architecture et sécurité des réseaux » (ASR) - …

Caractérisation des formations d'ingénieur labélisées par SecNumEdu

- 6 formations d'ingénieur labélisées SecNumEdu au 24.01.2017
- 8 ans d'ancienneté en moyenne pour ces formations d'ingénieur. A titre d'illustration, l'Ecole Nationale Supérieure d'Ingénieurs de Bretagne Sud (ENSIBS) a nouvellement créé une spécialité cyberdéfense intégrée au cycle d'ingénieur avec 50 places. Après 1 an d'existence, cette formation a été labélisée SecNumEdu dès janvier 2017.
- 37 places en moyenne par promotion pour les options en sécurité au sein des écoles d'ingénieur. Cela constitue les promotions les plus grandes avec les masters.
- 199 places disponibles parmi 6 formations labélisées
- 132 élèves formés à la dernière année de promotion parmi 5 formations labélisées
- 76% de taux de remplissage moyen, avec des taux allant de 56% à 93%.
- 7 mois de stage inclus dans le cursus.

1.6. Les mastères spécialisés en cybersécurité

Type de formation	Mastères spécialisés
Nombre total de formations recensées :	15
Formations enregistrées au répertoire du CNCP :	0
Formations labélisées SecNumEdu :	5
Formation initiale / formation continue / VAE :	0 / 15 / 0
Exemples d'intitulés de formation : (liste complète fournie en annexe)	- MS « Architecture Cyber-Sécurité et Intégration » - MS « Sécurité de l'information et des systèmes (SIS) - MS « Technologies du Web et Cyber Sécurité » - …

Caractérisation des mastères spécialisés labélisés par SecNumEdu

- 5 mastères spécialisés labélisés SecNumEdu au 24.01.2017
- 10 ans d'ancienneté en moyenne pour ces mastères spécialisés
- 110 places disponibles pour ces 5 MS
- 46 élèves formés sur 3 MS qui offraient 66 places, soit un taux de remplissage moyen de 70%
- de 5 mois de stage en moyenne pour ces 5 MS
- 2 MS sur ces 5 proposant des certifications : Auditor ISO 27001, Lead auditor ISO 27001 et certification Stormshield
- Les principaux métiers auxquels s'adresses ces MS sont : consultant gouvernance, risques et conformité, consultant sécurité technique, auditeur technique sécurité et test d'intrusion et auditeur organisationnel

1.7. Autres formations

En complément des formations dispensées par les établissements d'enseignement supérieur, deux autres catégories ont été identifiées :

- **Les formations BADGE :**

L'ESIEA, forte de son expérience en sécurité informatique dans l'enseignement et la recherche, a développé deux formations BADGE, conçues et réalisées en partenariat avec l'entreprise Quarkslab : Badge Sécurité Offensive ; Badge Reverse Engineering. Ces formations de 230h dispensées en soirée et week-end sur 6 mois sont compatibles avec une activité professionnelle.

- **Le Certificat de Qualification Professionnelle**

Un certificat de Qualification Professionnelle (CQP) a été créé en juin 2016 par la Branche pour le Manager de la Sécurité et des Risques de l'Information (MSRI). Le MSRI est en charge de la définition de la politique de gestion des risques liés à l'information dans l'entreprise, du déploiement et de l'animation du dispositif de gestion des risques. Ce dispositif intègre des actions anticipatrices de pesée des vulnérabilités et des actions correctrices de défaut de sécurité de l'information.

Le CQP MSRI est composé de 5 blocs de compétences, évaluées à la remise du certificat :

1. Définir et organiser la gouvernance des risques liés à l'information
2. Définir et piloter le dispositif de maîtrise des risques liés à l'information
3. Définir et superviser le dispositif de gestion des incidents et des crises
4. Evaluer le dispositif de gestion des risques liés à l'information
5. Diffuser la culture de prévention des risques liés à l'information

Il s'adresse aux candidats titulaires d'un diplôme ou titre de niveau I (bac+5) issus d'un cursus scientifique, de commerce, de management ou juridique et avec une expérience professionnelle de 5 années minimum dans le domaine de la Sécurité (en tant que RRI, consultant SSI, Auditeur SSI, consultant en management et manager des risques).

La formation comprend 238h de cours et 126h d'études de cas organisée autour de :

- Des enjeux de la sécurité et des risques de l'information
- De la gouvernance de la sécurité et des risques de l'information
- De la gestion de la sécurité et des risques liés à l'information
- De la gestion des incidents et la gestion de crise
- Du contrôle interne et l'amélioration
- De la diffusion de la culture de prévention des risques…

III. Formations dispensées par des organismes de formation continue

Les formations s'adressent aux professionnels de la cybersécurité. Elles visent à apporter des compétences complémentaires aux personnes déjà en poste, des certifications, de nouveaux contenus, de la veille technologique ou une mise à jour sur des réglementations… Ces formations continues sont proposées aux professionnels souvent sous la forme de sessions courtes (usuellement 1 à 5 jours) compatible avec leurs activités professionnelles.

3.1 Les organismes de formation continue

Les organismes qui dispensent des formations continues peuvent être catégorisés selon deux types d'acteurs :

CATEGORIES D'ACTEURS DE LA FORMATION CONTINUE EN CYBERSECURITE

- **Des entreprises et organismes de formations spécialisés en cybersécurité**

Les entreprises et organismes de formations spécialisés en cybersécurité sont peu nombreux en France (9 organismes référencés en annexe du rapport). Le marché est concentré entre un petit nombre d'acteurs historiques et de professionnels à la fois prestataires de services et formateurs. Certains de ces organismes sont agréés par LSTI selon une procédure qui « assure de leur compétence et de leur savoir-faire à dispenser les formations en question »[78].

Certains de ces organismes spécialisés ont développé une expertise forte, leur permettant de s'adresser aux opérationnels avec des formations pointues sur des sujets innovants :

> *« Nous avons un positionnement d'expertise, à l'inverse des organismes généralistes. Notre activité de recherche et développement nous permet de créer des formations très pratiques et en avance de phase. » - Dirigeant d'un organisme spécialisé en cybersécurité*

[78] https://www.lsti-certification.fr/index.php/formations-agreees/les-organismes-de-formation.html

Des éditeurs de logiciels peuvent également dispenser directement des formations dédiées à leurs outils. La plupart s'adressent à ces organismes de formation spécialisés pour dispenser les modules spécifiques à leur solution.

- **Des organismes de formation généralistes**

De plus, des organismes de formation généralistes, avec des catalogues de formation très larges, proposent des formations dédiées en cybersécurité (6 organismes référencés en annexe de ce rapport).

« Nous formons chaque année 20 000 stagiaires tous domaines confondus.
La cybersécurité représente une part d'environ 15% de notre activité. »
- Dirigeant d'un organisme de formation généraliste

Ces formations répondent souvent à des problématiques plus transverses, mais ces organismes peuvent également dispenser des formations techniques en cybersécurité.

3.2 Caractérisation de cette offre de formation continue « courte »

❖ *Volume horaire des formations continues*

A travers ces différents organismes, plus de 400 formations continues ont pu être recensées. Elles sont principalement des formations de moins de 5 jours, parfois dispensées en plusieurs sessions en Ile-de-France et en province.

Le nombre d'heures des formations « courtes » a pu être identifié et analysé pour 98 formations[79] : ces dernières présentent en moyenne un contenu pédagogique enseigné sur 24 heures de cours, soit 3,5 jours.

« Au-delà de 35 heures (5 jours), c'est une formation dense de plus d'une semaine. Ce n'est que très rarement possible pour une entreprise de détacher un collaborateur plus d'une semaine. Et concrètement, pour une formation enseignée en Ile-de-France, il y a environ 50% des stagiaires qui viennent de la Région mais 50% viennent de province. Il leur faut une formation qui tient en une semaine ouvrée. » - Formateur

---

❖ *Modalités d'enseignements de ces formations continues*

Une part de ces formations peut être dispensée en ligne via des sessions de e-learning. Aujourd'hui cette part est relativement faible. Plusieurs organismes ont choisi de ne proposer leur formation qu'en présentiel afin de s'assurer du bon niveau de diffusion du savoir aux stagiaires. D'autres ont pour stratégie de développer leur offre de formation en ligne dans les années à venir :

« Dans notre stratégie, nous allons proposer des formations à distance. Beaucoup de nos clients nous le demandent, ne serait-ce que pour mieux s'adresser aux professionnels de province ou DOM TOM» - Dirigeants d'un organisme de formation spécialisé

La langue de formation est également un point de diversité entre ces formations. Elles peuvent être enseignées aussi bien en français qu'en anglais. Ce choix tient souvent de l'organisme de formation et de son champ d'action (France, pays francophones, Europe ou Monde), mais également du contenu de la formation.

« Nous avons fait le choix de donner la formation en français. Le contenu est suffisamment dense et le rythme soutenu. En anglais, il y a un vrai risque d'une perte de niveau et de compréhension des stagiaires » - Expert d'un grand organisme de formation continue

---

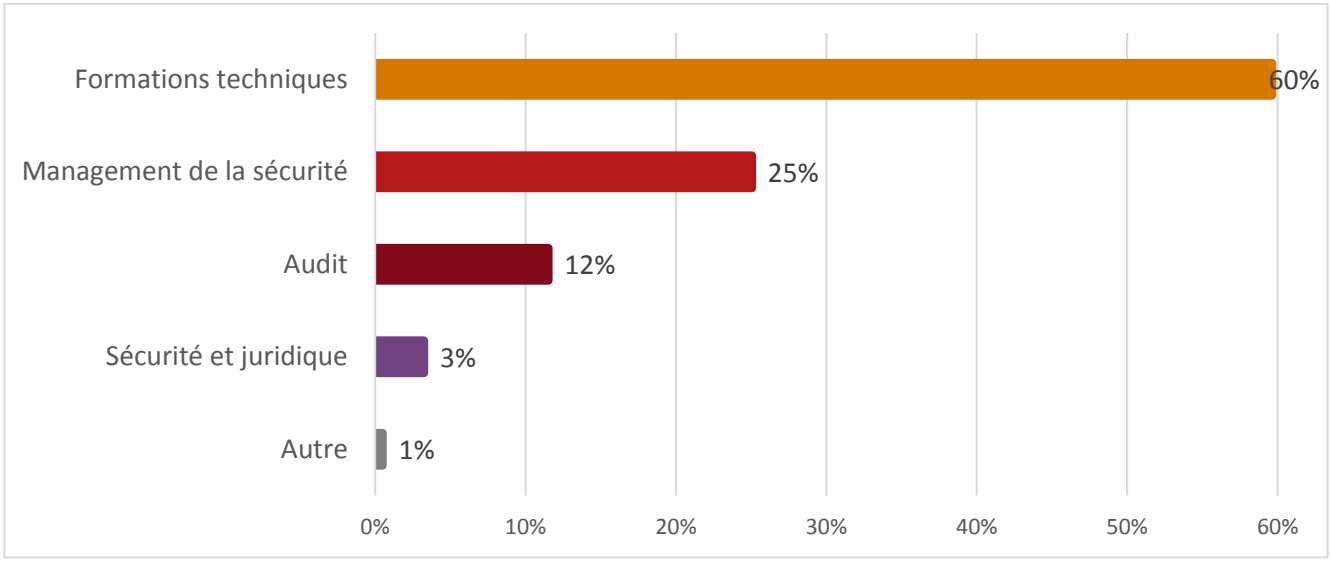
[79] Correspondant aux formations où l'information a pu être collectée en ligne entre janvier et février 2017.

❖ *Thématiques*

La diversité des thématiques de formations continues fait écho à la multiplicité des compétences demandées pour les professionnels en cybersécurité : compétences techniques, compétences fonctionnelles et capacités transverses.

Catégories:	Sous-catégories:
Formations techniques	Sécurité des Réseaux et des Infrastructures
	Sécurité des systèmes d'exploitation
	Cyber Défense
	Investigation numérique (Forensic) et réponses à incidents
	Test d'intrusion
	Sécurité des applications
	Sécurité des développements
Management de la sécurité	Management de la sécurité des systèmes d'information
	Management de la continuité d'activité
	Analyse des risques des systèmes d'information
Audit	Homologation à la sécurité des systèmes d'information (RGS, LPM, PSSIE…)
	Audit de sécurité des systèmes d'information
Sécurité et juridique	Les métiers du CIL et DPD
	Droit et sécurité des systèmes d'information

THEMATIQUES DES FORMATIONS CONTINUES EN CYBERSECURITE



PRINCIPALES THEMATIQUES DES FORMATIONS IDENTIFIEES

60% des formations sont dédiées à des compétences techniques : sécurité des réseaux et infrastructure, test d'intrusion, sécurité des applications, des développements, des systèmes d'exploitation… Après la dominante technique, près d'une formation sur trois concerne le management de la sécurité, faisant appel au développement et à une montée en compétence sur les compétences fonctionnelles (gestion des risques, plan de continuité…).

❖ *Certifications*

Certaines formations en cybersécurité font l'objet d'une certification. Les formations continues proposent principalement les certifications suivantes :

ISO 27005 Risk Manager

CISA (Certified Information Systems Auditor)

EBIOS Risk Manager

ISO 22301

ISO 27001 Lead Auditor

CISM (Certified Information Security Manager)

CISSO (Certified Information Systems Security Officer

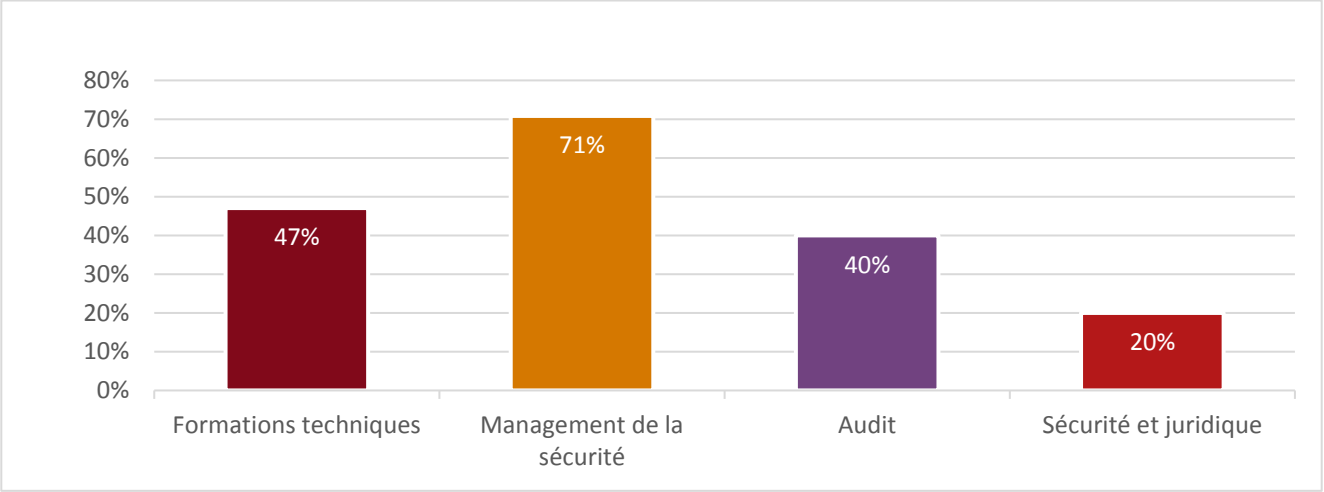
ISO 27001 Lead Implementer

CISSP (Certified Information Systems Security Professional)

PRINCIPALES FORMATIONS CONTINUES CERTIFIANTES

Les certifications internationales sont fortement demandées par les professionnels de la cybersécurité. Ces formations certifiantes représentent une part importante du marché des formations continues courtes.

Suivant les thématiques couvertes par ces formations, la part des formations certifiantes varie :



PART DES FORMATIONS CERTIFIANTES PAR CATEGORIE DE FORMATIONS CONTINUES[80]

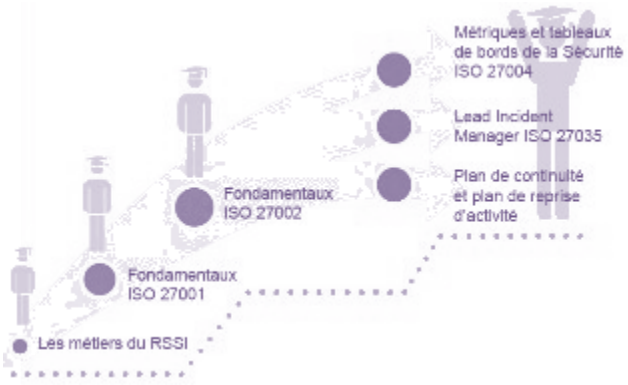
Ces certifications sont parfois requises pour l'exercice de certains métiers en cybersécurité, principalement pour les métiers de la 1ère famille de métiers (pilotage, organisation de la sécurité et gestion des risques) : CISSP, CISM, ISO 27001… C'est pour cette raison que ces formations certifiantes font l'objet d'une demande importante des entreprises et professionnels de la cybersécurité.

> *« Les formations certifiantes sont les plus demandées parmi notre catalogue de formation » - Dirigeant d'un organisme de formation spécialisé en cybersécurité*

[80] Sur les 98 formations continues où l'information a pu être collectée

❖ *Métiers auxquels les formations s'adressent*

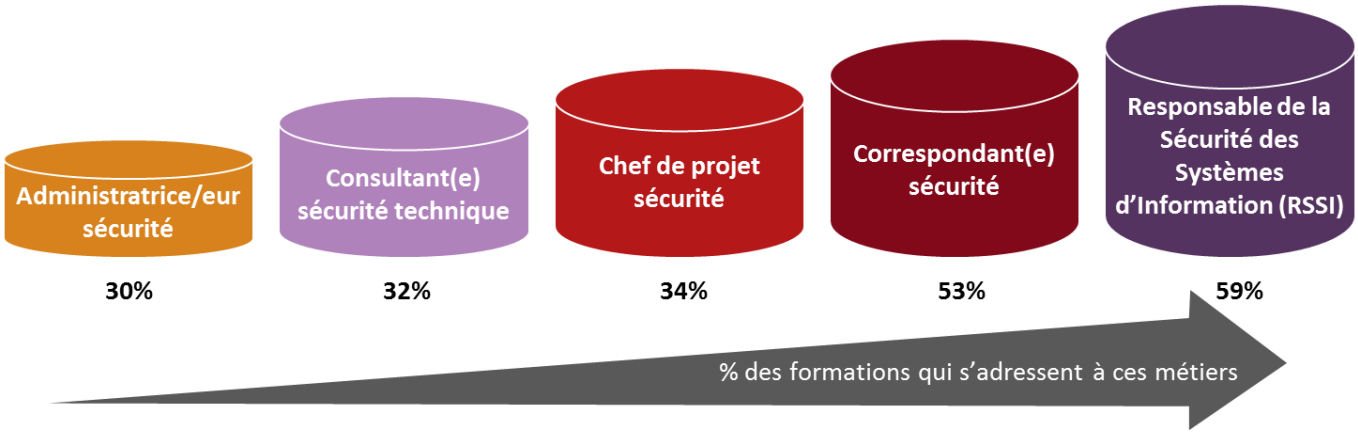
Pour s'adresser plus facilement aux professionnels de cybersécurité, les catalogues de formations identifient souvent les formations adaptées aux métiers. Les organismes de formation tendent à proposer des cursus ou parcours de formation en fonction des métiers :



EXEMPLE DE PARCOURS DE FORMATION CONTINUE DESTINE AUX RSSI

Ces cursus ne sont pas exclusifs les uns des autres, mais permettent ainsi aux professionnels de cybersécurité de progresser régulièrement à travers des formations différentes : des fondamentaux aux formations plus pointues. C'est également une manière de fidéliser les professionnels par une offre intégrée auprès d'un même organisme.

Le métier du RSSI est la cible du plus grand nombre de formations continues : deux fois plus nombreuses que pour le métier d'administrateur sécurité. Le champ d'activités et les responsabilités du RSSI nécessitent en effet des compétences nombreuses. Une maitrise des compétences techniques est toujours importante, engendrant des besoins réguliers en formation, et doit être complétée de connaissances grandissantes en management de la sécurité.



« TOP 5 » DES METIERS CONCERNES PAR LE PLUS GRAND NOMBRE DE FORMATION[81]

[81] Ces données reposent sur 98 formations continues où l'information « métiers auxquels s'adressent cette formation » a pu être récoltée.

IV. Autres initiatives en termes de formation en cybersécurité

Ces formations initiales et continues évoluent tout en s'inscrivant dans un schéma « classique » des formations en France. Le domaine du numérique et de la sécurité font appel à un rythme d'évolution important des programmes mais également des modes d'enseignements ou des partenariats nouveaux.

- **Une spécificité pour l'organisme de formation du personnel de l'administration française**

Des formations spécifiques pour le personnel de l'administration française

Focus sur le centre de formation à la sécurité des systèmes d'information (CFSSI)[82]

Le CFSSI intervient dans la définition et la mise en œuvre de la politique de formation à la sécurité des systèmes d'information. Il propose des formations dispensées par des experts de l'ANSSI sous la forme de stages courts et d'un cycle long permettant d'obtenir le titre d'expert en sécurité des systèmes d'information (ESSI).

En 2016, 83 sessions de formation ont été dispensées au profit de 1 699 personnes. Ces formations continues sont adressées aux personnels de l'administration française. Elles ne sont pas ouvertes à d'autres publics que le personnel de l'Etat, les collectivités territoriales et la fonction publique hospitalière. Le CFSSI propose ainsi 23 formations, allant du niveau « initiation » à « Perfectionnement ».Ces formations ont une durée moyenne de 4 jours.

❖ *La formation continue par l'école, accompagnée d'une meilleure sensibilisation à la cybersécurité*

Face à la demande toujours croissante des profils en cybersécurité, les formations se multiplient et se diversifient. La frontière entre formation initiale et continue tend à disparaître avec des acteurs proposant les deux.
En complément des formations techniques adressées aux profils expérimentés en cybersécurité, une offre complémentaire pour des profils « non experts » se structure :

« Les pouvoirs publics s'accordent à dire qu'il y a urgence à former tous les collaborateurs à la sécurité informatique, quelque que soit leur fonction. Le but est de pousser les salariés à la surveillance et de leur donner les bons réflexes »[83]

S'adaptant à la multiplicité des besoins des entreprises – de la start-up à la multinationale – certaines universités ou écoles, comme l'Université technologique de Troyes, complètent leurs offres de formation par des modules de sensibilisation, notamment adressés aux PME.

[82] Source : site de l'ANSSI et catalogue formation du CFSSI.
[83] http://www.letudiant.fr/educpros/actualite/cybersecurite-l-enseignement-superieur-passe-a-l-attaque.html

❖ *La multiplication des évènements cybersécurité, contribuant à l'attractivité de la filière et constituant un autre processus de recrutement*

Sans être qualifiés de formation initiale ou continue, un certain nombre d'évènements participent à l'avènement et la reconnaissance des compétences et plus largement de la filière cybersécurité.
Encouragés par la volonté de se démarquer des promotions de diplômés et passionnés par le challenge intellectuel, de nombreux évènements de type « Ethical hacking » ou « Bug Bounty » attirent de plus en plus d'étudiants ou professionnels en cybersécurité.
A titre d'illustration, voici quelques initiatives récentes qui connaissent un succès important :

- **L'European Cyber Week (CEB)**, initiative lancée par le Pôle d'Excellence Cyber en Bretagne.

Cette semaine permet d'identifier les bonnes compétences en sécurité des systèmes d'information à travers un challenge essentiellement technique.

> *« Le but d'un challenge comme celui-ci est aussi d'attirer, avec des opérations originales, des profils que l'on n'arrive plus à capter avec des opérations de recrutement classiques »*

Cet évènement concentre les principaux acteurs référents en cybersécurité de France et d'Europe. Il permet également à la Bretagne de confirmer sa position de territoire à la pointe dans ce domaine.

- **La nuit du hack**, initiée dès 2003, inspirée par la Defcon de Las Vegas

Depuis 2010, cet évènement rassemble autour de conférences, ateliers et challenges des professionnels de la sécurité informatique et les hackers de tous niveaux de qualification.

- **Bounty Factory,** a rassemblé plus de **1800 participants en 2016.**

Ce système de bug bounty connait un fort succès. Les participants font l'objet d'un classement à chaque challenge – classement qui représente une forme de « concours » et intéresse les entreprises pour juger et recruter les candidats en fonction de leur performance.

PARTIE 3 : PRECONISATIONS ET PLAN D'ACTIONS

I. Synthèse de l'adéquation entre l'offre de formation avec les besoins des entreprises

Il ressort de cette étude que l'offre de formation en cybersécurité est adaptée aux besoins des entreprises d'un point de vue qualitatif. Les compétences développées correspondent aux attentes des entreprises, et les contenus des formations font l'objet d'actualisation aux nouveaux usages, nouvelles menaces et nouvelles réglementations. D'un point de vue quantitatif, les jeunes diplômés (issus de la formation initiale) ne semblent pas assez nombreux pour répondre aux demandes croissantes des entreprises. Cependant, la problématique principale ne se situe pas dans un nombre de places ou de formations insuffisant, mais dans l'attractivité des formations et de la filière plus globalement.

D'un point de vue quantitatif, l'offre de formation en cybersécurité est large et diversifiée :

- Près de 150 formations longues dispensées par les établissements d'enseignement supérieur (licences professionnelles, masters et formations d'ingénieur), représentant un nombre de places par promotion estimé à environ 2 500 places. Avec un taux de remplissage moyen de 83%, il est estimé chaque année que 2 100 élèves sont formés chaque année par des formations longues dispensées par les établissements d'enseignement supérieur
- Plus de 6 000 postes en cybersécurité sont actuellement non pourvus sont estimés pour l'ensemble de la filière cybersécurité en France, [84] - ces 6 000 postes correspondent souvent à des niveaux expérimentés (non directement issues de formations initiales)[85]. Par ailleurs, la phase 1 a mis en avant les besoins des entreprises de la Branche et leur croissance dans le domaine : 1 400 nouveaux postes créés à horizon 3 ans.
- La filière cybersécurité manque de personnes qualifiées mais pas d'un manque de formations. De plus, le facteur de pondération réside dans la formation continue dispensée aux salariés de la filière cybersécurité ou d'autres filières.

[84] JDD, 23 Avril 2017.

[85] Les entreprises recherchent le plus souvent des personnes directement opérationnelles sur des postes nécessitant plusieurs années d'expérience.

Le tableau suivant donne une appréciation générale d'adéquation des formations aux familles de métiers en cybersécurité tant d'un point de vue quantitatif que qualitatif (en termes de couverture des métiers, de contenu, des compétences…) :

Familles de métiers	Formations longues dispensées par les établissements d'enseignement supérieur		Formations courtes des organismes de formation	
	Adéquation	Commentaire	Adéquation	Commentaire
1. Pilotage, organisation de la sécurité et gestion des risques		Les niveaux Bac+5 et au-delà donnent un socle solide de compétences pour les métiers dits de pilotage comme RSSI. Ces derniers ne sont souvent accessibles qu'après plusieurs années d'expérience et des certifications complémentaires acquises en formation continue.		Tous les catalogues de formation proposent des parcours de formations destinées aux RSSI avec les principales certifications (ISO 27001, ISO 27002, ISO 27004, ISO 27035…).
2. Management de projets de sécurité et cycle de vie de la sécurité		Les formations pour cette famille de métier semblent correspondre en termes de contenu et de diversité de l'offre aux besoins des entreprises. Cependant les formations ne sont pas toutes saturées, soulevant la question de leurs attractivités.		25% des formations visent à développer les compétences en management de la sécurité (continuité d'activité, analyse des risques, management de la sécurité des systèmes d'information…)
3. Maintien en condition opérationnelle de la sécurité		Seules les licences professionnelles identifient les métiers de cette famille comme cible après la formation. Les licences professionnelles atteignent un taux de remplissage important (94% pour les formations labélisées SecNumEdu)		Les parcours de formations sont moins explicites pour des métiers comme l'administrateur sécurité ou technicien sécurité, qui ont la possibilité d'évoluer vers le manager en cybersécurité, vers l'expertise technique ou vers l'expertise en sécurité des données personnelles.
4. Support et gestion des incidents de sécurité		Cette famille de métiers semble moins connue ainsi que les formations associées. Une meilleure orientation vers ces formations est nécessaire.		Les évolutions réglementaires nécessitent une actualisation des contenus de formation et une anticipation des besoins en compétences : sécurité des applications, sécurité des systèmes d'exploitation.
5. Conseil, audit et expertise en sécurité		Les métiers de consultant / auditeur en sécurité technique ou organisationnelles sont les plus ciblées par les formations, et correspondent bien aux demandes les plus importantes des entreprises.		Les formations continues courtes sont nombreuses à s'adresser à cette famille de métiers.

Légende :

Sur le volet quantitatif : Nombre de formations et de places disponibles limitant ; Nombre de formations et de places disponibles en adéquation

Sur le volet qualitatif : Adéquation limitée, à fort enjeu ; Bonne adéquation, avec des possibilités d'ajustement ; Très bonne adéquation

Trois enjeux prioritaires ont été identifiés lors des précédentes phases de diagnostic :

- Comment accroitre l'attractivité et la visibilité de la filière cybersécurité pour les étudiants et les jeunes professionnels ?
- Comment faciliter l'orientation et l'accès des lycéens et étudiants aux formations en cybersécurité ?
- Comment accompagner la mobilité professionnelle et la montée en compétences des salariés vers les métiers de la cybersécurité ?

Chaque enjeu a été décliné en axes de travail, eux-mêmes déclinés en actions. Pour chaque action, le plan présente :

- Le contenu de l'action
- Les bénéficiaires-cibles
- Les acteurs impliqués
- Les points de vigilance associés
- Un indicateur de priorité
- Un indicateur de faisabilité

Tableau de synthèse des axes de travail :

Enjeux	Axes de travail
1. Accroitre l'attractivité et la visibilité de la filière cybersécurité	Structurer la filière cybersécurité
	Faire connaitre la filière et ses acteurs à un public plus large
	Valoriser les métiers de la cybersécurité auprès des lycéens et des étudiants
2. Faciliter l'orientation des lycéens et étudiants vers les formations en cybersécurité	Orienter les bons profils vers la formation initiale
	Développer des lieux d'échange pour faciliter l'accès à l'emploi
	Partager les initiatives en cybersécurité et bonnes pratiques locales
3. Accompagner la mobilité professionnelle et la montée en compétences des salariés	Actualiser les compétences des salariés en cybersécurité par la formation continue
	Sensibiliser les DRH aux métiers de la cybersécurité pour orienter les salariés vers les formations qualifiantes et certifiantes
	Renforcer la sensibilisation des dirigeants d'entreprises sur la cybersécurité

II. Enjeu 1 : Accroître l'attractivité et la visibilité de la filière cybersécurité

1.1. Constats

- **Une pénurie de candidats**

Les besoins en cybersécurité des entreprises sont en forte croissance. L'enquête de la phase 1 a mis en évidence les difficultés des entreprises à trouver des professionnels au sein de la filière avec les profils et les niveaux de maitrise de compétences attendus : en effet deux entreprises sur trois rencontrent des difficultés de recrutement sur les métiers de la cybersécurité[86].

- **Des carrières dans la cybersécurité encore peu connues vis-à-vis du grand public**

La cybersécurité apparaît comme une filière encore peu lisible et peu comprise des étudiants, et souffrant d'une image parfois négative faute de communication claire et coordonnée sur la réalité des métiers de la filière, les débouchés et les perspectives de carrière.

Pour un public plus large, il s'agit d'être en capacité de proposer des supports de communication et de promotion donnant une vision globale et simple de la filière pour aider à l'identification des principales formations et de leurs débouchés.

- **Des métiers méconnus et réduits à la dimension technique**

Les compétences recherchées aujourd'hui en cybersécurité dépassent largement la seule dimension technique, même si celle-ci reste bien entendu indispensable. Les acteurs de la cybersécurité doivent disposer de compétences organisationnelles, managériales, relationnelles, dites « aptitudes professionnelles », pour ne citer qu'elles, permettant de bien comprendre les enjeux stratégiques des entreprises, de communiquer et dialoguer avec les Directions Générales, de manager des projets complexes… Ces aspects sont encore trop peu connus et valorisés auprès d'un public non averti.

[86] Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité. (Phase 1)

1.2. Axes de travail et modalités de mise en œuvre

Les trois axes de travail suivants ont été identifiés :

- Structurer la filière cybersécurité
- Faire connaitre la filière et ses acteurs à un public plus large
- Valoriser les métiers de la cybersécurité auprès des lycéens et des étudiants

Axe de travail : Structurer la filière cybersécurité

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
1.A	Constituer un collectif « France Cybersécurité » qui se définit comme un collectif de professionnels en cybersécurité, comprenant une représentation de l'ANSSI, d'entreprises et de formateurs en cybersécurité. Ce groupe aura les objectifs suivants : • Structurer la filière à l'échelle de la France avec les besoins des entreprises • Etre le point de relais d'informations sur le marché de l'emploi (forums, salons spécialisés, associations et club de la cybersécurité, etc) • Maintenir à jour la liste des métiers recherchés et des compétences (RSSI, consultants cybersécurité, architectes / analyste en sécurité, etc)	NA	ANSSI Acteurs de la cybersécurité OPIIEC-FAFIEC (associé, non responsable ou financeur)	Définition des missions de ce collectif	★	⯪

Légende: Priorité ou complexité
☆ Faible ⯪ Moyen ★ Fort

Axe de travail : Faire connaitre la filière et ses acteurs à un public plus large

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
1.B	Créer un site portail "cyber" pour le grand public ou faire évoluer le site de l'ANSSI. Ce portail permettra de centraliser les informations suivantes : - référentiel des métiers et cartographie de l'offre de formation - communications sur les menaces et risques auxquelles sont exposées les entreprises - études existantes sur la cybersécurité - actualité (revue de presse sur la cybersécurité)	Acteurs de la cybersécurité Grand public	Collectif « France Cybersécurité » (en lien avec l'action 1.A)	- Portage et gouvernance du portail - Actualisation des informations - Référencement du portail cyber	★	⯪
1.C	Compléter la présente étude au niveau national pour l'ensemble de la filière cybersécurité. L'approche dépassera les entreprises de la Branche pour couvrir l'ensemble des secteurs concernés par la cybersécurité (la banque, la défense, la santé…) : Il s'agit de communiquer sur les différents secteurs et type d'entreprises concernées par les problématiques cybersécurité à un public plus large, à l'aide d'exemples simples, afin de donner des idées d'organisations où il est possible d'exercer les métiers de la cybersécurité	Grand Public Salariés	ANSSI Autres branches professionnelles	- Coût de prise en charge - Partage de l'étude	⯪	★

Légende: Priorité ou complexité

☆ Faible ⯪ Moyen ★ Fort

Axe de travail : Valoriser les métiers de la cybersécurité auprès des lycéens et des étudiants

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
1.D	Mettre en place une communication généraliste sur la cybersécurité auprès des lycéens et des étudiants : o Qu'est-ce que la cybersécurité ? o Qui sont les acteurs concernés ? o Quelles sont les problématiques rencontrées par les entreprises ? o Quels sont les métiers possibles et les débouchés ? o Quelles sont les formations ?	Collégiens Lycéens Etudiants	Collectif « France Cybersécurité » (en lien avec l'action 1.A) Acteurs de l'orientation (Onisep, Studyrama…) Presse étudiante (L'Etudiant)	- Adaptation de la communication aux publics visés - Aspect ludique et pédagogique des contenus	★	⯪
1.E	Mettre en place une communication spécifique auprès des lycéens et des étudiants sur les carrières et parcours professionnels possibles en cybersécurité : - mise en place d'une communication multicanale de parcours types, de belles histoires sur les carrières, débouchés et rémunérations de la filière (plaquettes, chaînes Youtube, stories Snapchat…) - information en ligne sur le portail cyber et/ou des articles dans la presse étudiante	Lycéens, étudiants	Collectif « France Cybersécurité » (en lien avec l'action 1.A) Acteurs de l'orientation (Onisep, Studyrama…) Presse étudiante (L'Etudiant) Conseillers d'orientation	- Adaptation de la communication aux publics visés - Coût et pilotage de la campagne	★	⯪

Légende: Priorité ou complexité
☆ Faible ⯪ Moyen ★ Fort

III. Enjeu 2 : Faciliter l'orientation des lycéens et étudiants vers les formations en cybersécurité

1.3. Constats

- **Un taux de remplissage des formations initiales qui questionne le niveau d'attractivité de la filière**

La phase 2 de cette étude a mis en avant une offre de formation large en France, probablement suffisamment grande et diversifiée pour couvrir le besoin actuel. Cependant, le nombre d'élèves formés n'atteint pas toujours le nombre de places ouvertes en formation, faute de candidats n'ayant pas le bagage technique requis. Cette inadéquation des candidatures fait que le taux de remplissage moyen des établissements d'enseignement supérieur[87] n'est que de 70%. Le nombre de places ouvertes pour ces formations n'est donc pas un critère limitant le nombre de personnes formées à la cybersécurité. La problématique se situe alors en amont, avant même l'entrée dans ces formations, au niveau de la capacité à orienter les bons profils vers les filières de formation cybersécurité.

- **Des canaux de recrutement divers**

Cette étude a mis en avant le besoin des entreprises en cybersécurité : 45% d'entre elles pensent que l'équipe cybersécurité sera amenée à se renforcer à l'horizon 3 ans[88]. Pour recruter, plus d'une entreprise sur deux utilise les réseaux professionnels en ligne et les prescripteurs d'annonces. Les sites sont variés et ne permettent pas toujours de réaliser simplement les recherches ciblées pour cette filière. C'est pourtant un point clé d'information dans ce contexte de pénurie des candidats et de croissance des besoins.

- **Des initiatives remarquables sur lesquelles capitaliser**

De nombreuses initiatives ont émergé en cybersécurité : de nouveaux types de formations, le phénomène Bug Bounty[89], la création de pôles d'excellence, de nouveaux partenariats entre entreprises et établissements d'enseignement supérieur… D'autres initiatives continueront de se constituer, surfant sur les nouveaux besoins des entreprises et l'évolution rapide des métiers afin de faciliter l'entrée dans la filière et de susciter des vocations.

[87] Lorsque l'information était disponible parmi les formations labelisées SecNumEdu
[88] Source : enquête en ligne EY auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité. (Phase 1)
[89] Programme de recherche de vulnérabilités qui récompense les chercheurs ayant trouvé des failles de sécurité dans un cadre préalablement défini par le programme de Bug Bounty et son périmètre (scope).

1.4. Axes de travail et modalités de mise en œuvre

Les axes de travail sont les suivants :

- Orienter les bons profils vers la formation initiale
- Développer des lieux d'échange pour faciliter l'accès dans la filière
- Valoriser les initiatives vertueuses et les bonnes pratiques

Axe de travail : Orienter les bons profils vers la formation initiale

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
2.A	Faire connaitre les pré-requis techniques pour candidater et postuler aux formations en cybersécurité : - liste des compétences recherchées avec des exemples concrets de taches - mise en avant des compétences non techniques via des communications sur le portail L'information pourra être détaillée pour les principales compétences recherchées en cybersécurité par les entreprises : - Sécurité des applications (mobile, web, tablettes, ERP, etc) - Audits de sécurité (technique, organisationnel, configuration, code source) - Protection de l'information (classification, mesures techniques ou organisationnelles) - Supervision sécurité (SOC, SIEM) - Plan de continuité d'activité (PRA, DRP, GC) - Gestion des accès et des identités	Etudiants Lycéens Professionnels	Collectif « France Cybersécurité » (en lien avec l'action 1.A) Acteurs de l'orientation (Onisep, Studyrama…) Presse étudiante (L'Etudiant)	Proposer des solutions d'orientation alternatives (formations complémentaires) pour ne pas décourager les candidats et leur permettre une mise à niveau	★	★
2.B	Assurer une présence de la filière cybersécurité sur les forums et salons étudiants avec : - la diffusion des contenus de communication "filière cybersécurité" aux établissements d'enseignement supérieur proposant une formation en cybersécurité et directement aux lycéens/étudiants à l'entrée - l'organisation de conférences / ateliers dédiés à la cybersécurité	Lycéens Etudiants	FIC Forum spécialisés en informatique OPPIEC, FAFIEC Etablissements d'enseignement supérieur Organisations professionnelles	Présence sur l'ensemble du territoire	★	★

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
2.C	Créer un outil d'information/orientation des formations en cybersécurité ou enrichir le site de SecNumEdu (ANSSI) permettant un usage simple. L'interface doit pouvoir proposer les formations accessibles en fonction des critères renseignés : région souhaitée, temps de la formation voulue, métiers visés, enseignements clés… Cet outil pourra être implémenté sur le site internet SecNumEdu ou sur une page du portail cybersécurité (en lien avec l'action 1.B). Par exemple, cet outil devra permettre aux étudiants de savoir : - Quelles formations possibles pour préparer au métier d'architecte sécurité ? - Quelles sont les compétences attendues d'un consultant en cybersécurité ? …	Lycéens Etudiants	ANSSI	- Actualisation des informations - Renseignement des sites de chaque formation pour poursuivre les recherches	★	⯪

Légende: Priorité ou complexité

☆ Faible ⯪ Moyen ★ Fort

Axe de travail : Développer des lieux d'échange pour faciliter l'accès à la filière

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
2.D	Créer sur le portail "cyber" une plateforme de "bourse à l'emploi", regroupant les annonces en ligne d'emploi sur la cybersécurité	Chercheurs d'emplois / stages Etudiants	Collectif « France Cybersécurité » (en lien avec l'action 1.A)	- Actualisation et alimentation des informations - Interface avec les entreprises (DRH et équipes cyber)	⯪	☆

Axe de travail : Valoriser les initiatives vertueuses et les bonnes pratiques

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
2.E	Relayer les informations sur les évènements qui contribuent à faire connaitre la cybersécurité à un large public : - une page sur le portail "cyber" sur les prochains évènements en France - réalisation d'interviews des "lauréats" de ces évènements (profil, conseil pour rejoindre la filière, message aux jeunes...)	Grand public	Collectif « France Cybersécurité » (en lien avec l'action 1.A) Organisateurs des évènements		⯪	⯪
2.F	Dédier une page sur le site portail d'information sur les avancées territoriales de la filière cybersécurité (par exemple: le Pôle d'Excellence de Rennes, le collectif européen sur Lyon...). La cybersécurité devient un argument de marketing territorial : - pour les régions avec l'émergence de pôles associant formations et entreprises - pour les villes qui développent leurs propres évènements « cyber » : hackaton…	Grand public	Collectif « France Cybersécurité » (en lien avec l'action 1.A) Acteurs impliqués dans les initiatives remarquables	Actualisation des informations	★	⯪
2.G	Organiser des workshops et des cafés sur la formation en cybersécurité tous les trimestres avec des interventions d'experts ou de membres de la communauté cybersécurité. Le lieu pourra changer: àl'ANSSI, dans des établissements d'enseignement supérieur, au sein d'entreprises, dans des réunions d'associations...	Public sensibilisé Chercheurs d'emplois Professionnels	Collectif « France Cybersécurité » (en lien avec l'action 1.A)		⯪	⯪

Légende: Priorité ou complexité

☆ Faible ⯪ Moyen ★ Fort

Illustration de mise en œuvre possible ou exemple existants à l'étranger :

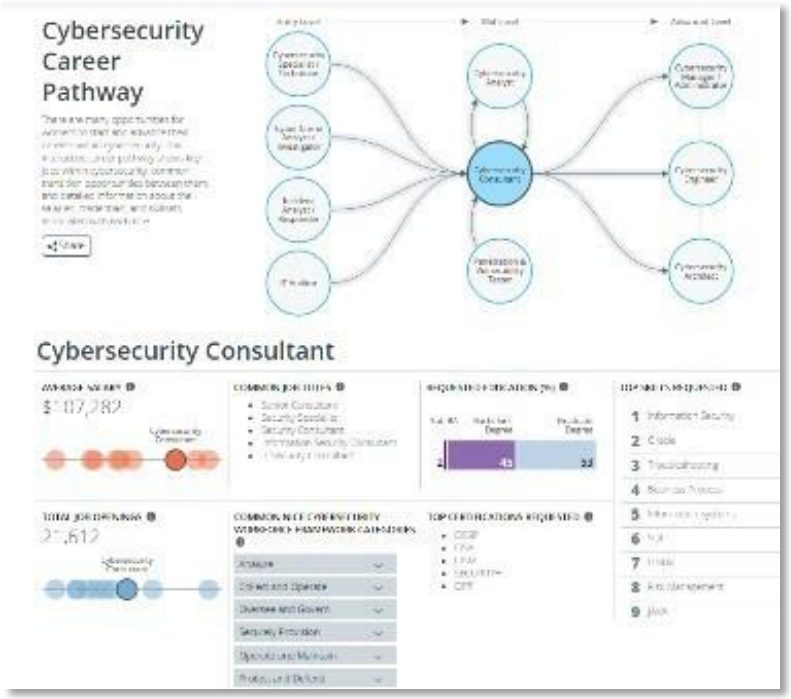


ILLUSTRATION D'UN PORTAIL CYBSERSECURITE AUX USA (http://cyberseek.org/pathway.html **)**

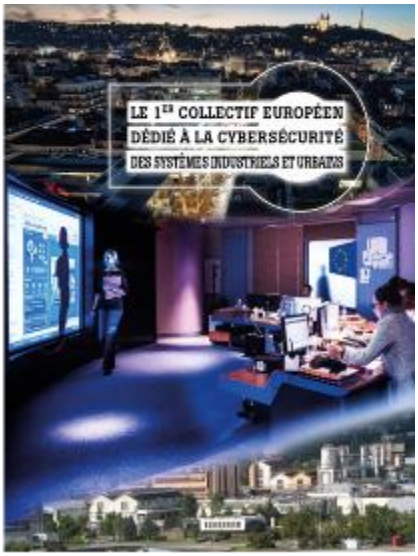


ILLUSTRATION DE COMMUNICATION DES TERRITOIRES EN TERMES DE CYBERSECURITE

IV. Enjeu 3 : Accompagner la mobilité professionnelle et la montée en compétences des salariés vers les métiers de la cybersécurité

3.1. Constats

- **L'évolution des compétences demandées par les entreprises**

La généralisation et le taux d'adoption exponentiels des solutions, « devices », des outils et des plateformes numériques (cloud computing, internet des objets, analytics, big data, mobilité, réseaux sociaux, etc.) augmentent la surface d'attaque des entreprises, augmentant leur vulnérabilité.

Les réglementations liées à la cybersécurité amènent les entreprises et les acteurs publics à se structurer pour protéger leur patrimoine informationnel ainsi que leurs traitements. Les métiers et les compétences en cybersécurité sont également impactés par la mise en œuvre de ces réglementations[90].

Le besoin en compétences pour ces nouveaux usages est important, allant des compétences techniques aux compétences fonctionnelles et transverses[91].

- **Une offre de formation en cybersécurité large mais peu lisible**

La cartographie des formations (phase 2) a montré qu'il existait un grand nombre de formations initiales ou continues, longues ou courtes, dispensées par des établissements d'enseignement supérieur ou des organismes de formation. L'offre de formation est large et semble couvrir l'ensemble des familles de métiers en cybersécurité. Plus de 150 formations longues dispensées par les établissements d'enseignement supérieur (de Bac+3 à Bac+5, des mastères spécialisés, des badges…) et plus de 400 modules de formations continues courtes ont été identifiées. Cette cartographie a été réalisée à partir de différentes sources d'information. En effet, les informations ne sont pas toujours centralisées, et il est difficile de s'y retrouver pour un non professionnel de la cybersécurité : Quel public cible ? Quel niveau de technicité ? Quels métiers cible ? Quelles certifications ? … Aujourd'hui, cette offre large manque de lisibilité pour deux raisons :

- un référencement dispersé (CNCP, SecNumEdu, catalogues de formations…)
- un manque d'indicateurs qualitatifs pour visualiser rapidement par exemple les principales certifications à avoir par métier, les organismes agréés…

- **Des difficultés de recrutement externes qui conduisent à renforcer les mobilités internes**

Les entreprises ont des besoins de recrutement et de renforcement de leurs équipes cybersécurité. Par ailleurs, elles ont souvent en interne des équipes plus grandes pour la filière IT. Les salariés de ces filières expriment parfois une appétence pour le domaine de la sécurité, posant la question du développement de passerelles vers les métiers de la cybersécurité pour les salariés souhaitant se réorienter dans leur carrière.

[90] Liste des principales réglementations liées à la cybersécurité présentée en annexe de cette étude.
[91] Liste des compétences en cybersécurité détaillée en partie 1 de cette étude.

- **<u>Une sensibilisation encore insuffisante des dirigeants d'entreprises</u>**

Les dirigeants des entreprises de la Branche se sont exprimés[92] lors de cette étude (phase 1) sur le niveau de sensibilité interne :

- Plus de la moitié des managers ont un niveau de sensibilisation aux problématiques cybersécurité jugé « moyen » ou « faible »
- Près de 2 opérationnels sur 3 (toutes fonctions confondues) ont un niveau de sensibilité jugé « moyen » ou « faible »

Les entreprises subissent pourtant des attaques de plus en plus nombreuses et sophistiquées. En ce sens, il y a un enjeu d'information des salariés concernant les risques d'attaques et les mesures à adapter concernant leurs usages numériques (mail, cloud…) pour une meilleure sécurité des informations de l'entreprise.

3.2. Axes de travail

Face à ces constats, il apparait nécessaire de renforcer les actions de communication au sein des entreprises pour mieux accompagner leurs salariés (assurant une fonction liée à la cybersécurité mais aussi au domaine IT, aux fonctions juridiques…).

Deux cibles sont ainsi particulièrement importantes, en raison de leur rôle d'impulsion et de relais pour la formation continue de leurs salariés : les Directions des Ressources Humaines (DRH) et les dirigeants d'entreprise.

Les axes de travail sont les suivants :

- Actualiser les compétences des salariés en cybersécurité par la formation continue
- Sensibiliser les DRH aux métiers de la cybersécurité pour orienter les salariés vers les formations qualifiantes et certifiantes
- Renforcer la sensibilisation des dirigeants d'entreprises sur la cybersécurité

[92] Source : enquête en ligne EY auprès des entreprises (périmètre : Branche et hors Branche)

Axe de travail : Actualiser les compétences des salariés en cybersécurité par la formation continue

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
3.A	Créer des Actions Collectives Nationales (ACN) sur la cybersécurité. Par exemple, deux axes pour lancer les ACN pourraient être privilégiés sur 1. Les parcours de formation au sein de la filière cybersécurité et 2. Les passerelles depuis la filière informatique :	Professionnels de la cybersécurité Professionnels en informatique (hors cybersécurité)	CPNE FP de la Branche FAFIEC		★	☆
	1. <u>Créer des parcours pour les professionnels de la cybersécurité :</u> - Information des salariés sur les possibilités de parcours professionnels et des formations certifiantes en cybersécurité - diffusion des évolutions possibles d'un métier à l'autre en cybersécurité (parcours de formation à renseigner sur le site portail) Par exemple, les parcours à identifier pourraient être : - Parcours 1 : Evolution vers le manager en cybersécurité (Analyste -> Consultant sécurité -> Chef de projet sécurité -> Directeur de programme sécurité -> RSSI) - Parcours 2 : Evolution vers l'expertise technique (Analyste SOC -> développeur sécurité -> auditeur sécurité -> Architecte de sécurité - Parcours 3 : évolution vers l'expertise en sécurité des données personnelles (Administrateur sécurité -> consultant sécurité -> délégué à la protection des données (DPO)					
	<u>2. Proposer des parcours de formation continue pour des professionnels de l'informatique vers la cybersécurité.</u> La démarche à lancer vis-à-vis des professionnels de l'informatique (hors métiers cybersécurité) pourrait être la suivante : - Evaluer l'intérêt des professionnels en informatique pour développer leurs compétences en cybersécurité - Identifier les principaux métiers en informatique qui pourraient être concernés par des passerelles vers les métiers de cybersécurité - Repérer les formations continues existantes qui conviendraient à ces passerelles entre l'informatique et la cybersécurité - Identifier les compétences sur lesquelles il conviendra de développer une offre de formation continue - Etudier le mode de financement de ces formations pour accéder aux métiers de la cybersécurité Par exemple, les passerelles pourraient être les suivantes : - Passerelle 1 : développeur informatique -> développeur sécurité - Passerelle 2 : Chef de projet informatique (MOA/MOE) -> chef de projet sécurité - Passerelle 3 : administrateur systèmes et réseaux -> analyste SOC ou CERT - Passerelle 4 : Directeur des Systèmes d'information (DSI) -> RSSI ou DPD - Etc					

Légende: Priorité ou complexité
☆ Faible ★ Moyen ★ Fort

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
3.B	Remettre à jour régulièrement les programmes de formations avec les éléments suivants : - Evolutions de la cybersécurité en termes de réglementations, nouveaux usages… - Référencement par l'ANSSI de ces nouveaux programmes (à intégrer sur SecNumEdu)	Etudiants	ANSSI Etablissements d'enseignement supérieur	- Actualisation des informations - Démarche partenariale	☆	★
3.C	Poursuivre un dialogue régulier (tous les ans) avec les organismes de formations continues pour : - Trouver des solutions de financement d'un plus grand nombre de formations - Accompagner les organismes dans les démarches d'éligibilité au financement : référencement Datadoc, inscription à l'inventaire…	Professionnels de la cybersécurité	OPIIEC-FAFIEC Certificateurs		★	☆

Légende: Priorité ou complexité
☆ Faible ⯪ Moyen ★ Fort

Axe de travail : Sensibiliser les DRH aux métiers de la cybersécurité pour orienter les salariés vers les formations qualifiantes et certifiantes

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
3.D	Communiquer auprès des DRH pour une meilleure connaissance des métiers et des besoins de compétences en cybersécurité en vue d'un meilleur accompagnement de la formation continue des salariés. Par exemple, créer un kit de communication didactique auprès des DRH contenant les informations suivantes : - Principaux métiers de la cybersécurité - Matrice simple des métiers-compétences - Principales tendances et évolutions de la filière	DRH	ANSSI Entreprises de la cybersécurité	Actualisation des informations	★	⯪
3.E	Lancer une évaluation qualitative des certifications et des formations pour une meilleure lisibilité de l'offre auprès des DRH. Par exemple, lister les formations et les certifications utiles pour le bon exercice de certains métiers de la cybersécurité :	DRH	OPIIEC-FAFIEC ANSSI …	Mobilisation des établissements et organismes de formation	⯪	★

	- RSSI : certifications CISSP, CISM, ISO 27005 Risk manager - Auditeur sécurité : ISO 27001 lead auditor, sécurité de l'infrastructure Analyste SOC : sécurité réseaux et des applications					
3.F	Encourager les entreprises à former en sécurité les salariés exerçant d'autres fonctions que la cybersécurité (Informatique, Juridique, Achats…)	Les salariés via les DRH d'entreprises	DRH des entreprises		★	★

Légende: Priorité ou complexité
☆ Faible ★ Moyen ★ Fort

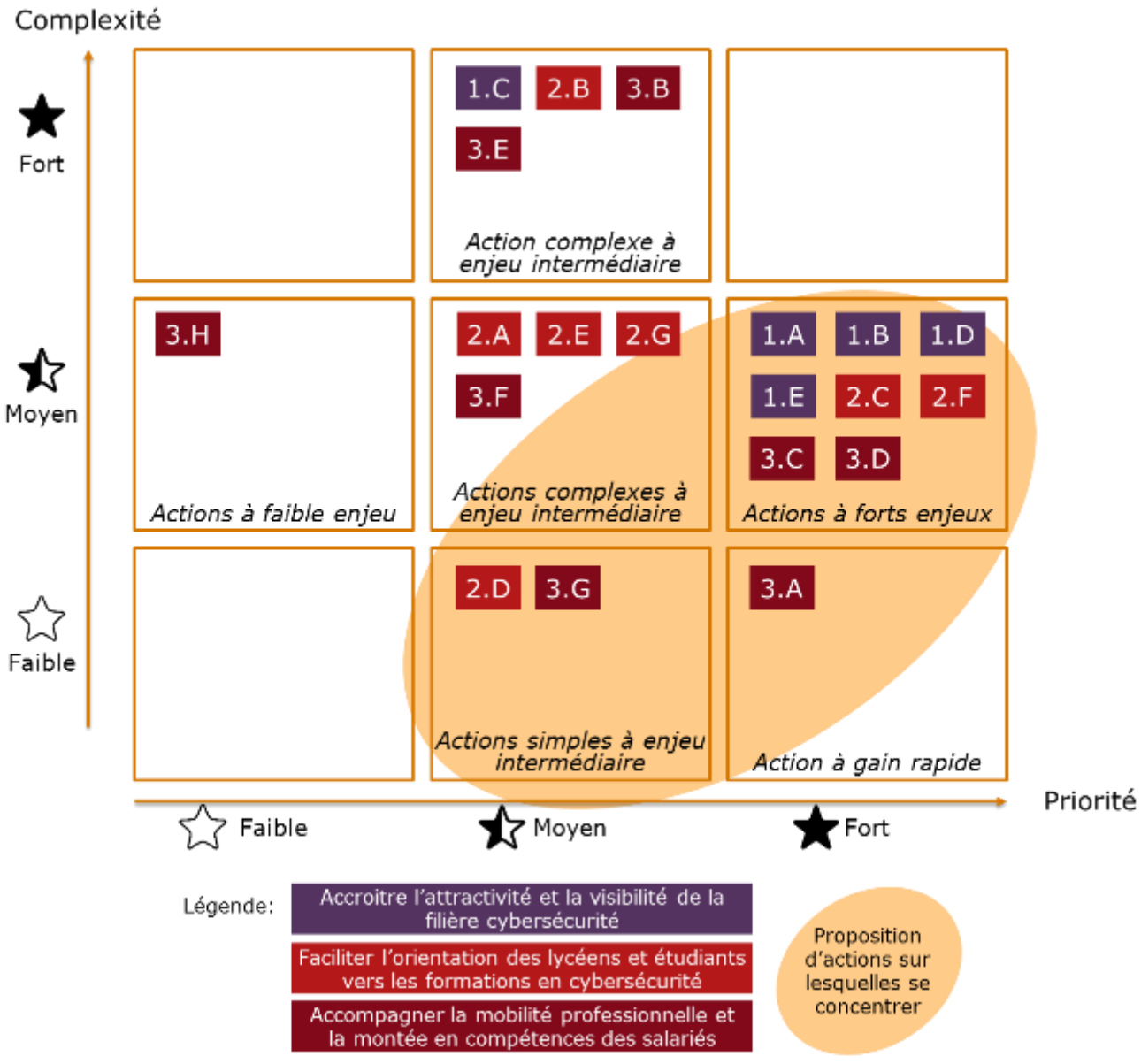
Axe de travail : Renforcer la sensibilisation des dirigeants d'entreprises sur la cybersécurité

#	Actions	Bénéficiaires	Acteurs impliqués	Points de vigilance	Indicateur de priorité	Indicateur de complexité
3.G	Diffuser la plaquette communicante de cette étude aux dirigeants d'entreprise	Dirigeants d'entreprise	OPIIEC Organisations professionnelles et syndicales de la Branche		★	☆
3.H	Missionner des « ambassadeurs » de la cybersécurité (experts et professionnels impliqués dans la filière et volontaires) pour élever le niveau de sensibilisation des managers: - Communication sur les initiatives prises par les entreprises du secteur - Diffusion aux entreprises de supports de communication et de sensibilisation en interne	Dirigeants d'entreprise	Collectif « France Cybersécurité » (en lien avec l'action 1.A) Entreprises et organismes de formation volontaires		☆	★

Légende: Priorité ou complexité
☆ Faible ★ Moyen ★ Fort

V. Synthèse du plan d'actions

Les recommandations se composent de 20 actions. Chacune d'elles a été classée par niveau de priorité (faible, moyen et fort) et niveau de complexité pour sa mise en œuvre (en fonction du nombre d'acteurs à mobiliser, du besoin de financement…).



MATRICE PRIORITE-COMPLEXITE DES ACTIONS

#	Actions
1.A	Constituer un collectif « France Cybersécurité »
1.B	Créer un site portail "cyber" pour le grand public ou faire évoluer le site de l'ANSSI
1.C	Compléter la présente étude au niveau national pour l'ensemble de la filière cybersécurité
1.D	Mettre en place une communication généraliste sur la cybersécurité auprès des lycéens et étudiants
1.E	Mettre en place une communication spécifique sur les carrières et parcours professionnels possibles en cybersécurité
2.A	Faire connaitre les pré-requis techniques pour candidater et postuler aux formations en cybersécurité
2.B	Assurer une présence de la filière cybersécurité sur les forums et salons étudiants
2.C	Créer un outil d'information / orientation des formations en cybersécurité ou enrichir le site de SecNumEdu (ANSSI)
2.D	Créer sur le portail « cyber » une plateforme de « bourse à l'emploi »
2.E	Relayer les informations sur les évènements qui contribuent à faire connaitre la cybersécurité à un large public
2.F	Dédier une page sur le portail « cyber » d'information sur les avancées territoriales de la filière cybersécurité
2.G	Organiser des workshops et des cafés sur la formation en cybersécurité
3.A	Lancer des Actions Collectives Nationales (ACN) sur la cybersécurité
3.B	Remettre à jour régulièrement les programmes de formations
3.C	Organiser des échanges réguliers et individualisés avec les organismes de formations continues
3.D	Communiquer auprès des DRH en vue d'un meilleur accompagnement de la formation continue des salariés
3.E	Lancer une évaluation qualitative des certifications et des formations
3.F	Encourager les entreprises à former en sécurité les salariés d'autres fonctions que la sécurité
3.G	Diffuser la plaquette communicante de cette étude aux dirigeants d'entreprise
3.H	Missionner des « ambassadeurs » de la cybersécurité pour élever le niveau de sensibilisation des managers

: Proposition d'actions sur lesquelles se concentrer

ANNEXES

ANNEXE 0 : Glossaire

ANNEXE 1 : Panel d'entreprises rencontrées

ANNEXE 2 : Bibliographie

ANNEXE 3 : Questionnaire de l'enquête en ligne

ANNEXE 4 : Codes NAF de référence pour la Branche

ANNEXE 5 : Matrice des métiers et leurs compétences

ANNEXE 6 : Guide d'entretien pour la phase 2 « état des lieux de l'offre de formation »

ANNEXE 7 : Cartographie de l'offre de formation dispensée par les établissements d'enseignement supérieur

ANNEXE8 : Cartographie des organismes de formations privées pour la formation continue « courte » en cybersécurité (liste non exhaustive)

ANNEXE 9 : Tableau des réglementations (et illustration de certaines normes) et impacts sur les métiers en cybersécurité

Annexe 0 – Glossaire

ACN : Action Collective Nationale

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ASR : Architecture et Sécurité des Réseaux

ASUR : Administration et SécUrité des Réseaux

BADGE : Bilan d'Aptitude Délivré par les Grandes Ecoles

CEB : European Cyber Week

CISM : Certified Information Security Manager, certification délivrée par l'ISACA

CISO : Chief Information Security Officer

CQP : Certificat de Qualification Professionnelle

CRO : Correspondant Risques Opérationnels

CSSI : Correspondant Sécurité des Systèmes d'Information

CDD : Contrat à Durée Déterminée

CDI : Contrat à Durée Indéterminée

CFSSI : Centre de Formation à la Sécurité des Systèmes d'Information

CIL : Correspondant Informatique et LibertésCGE : Conférence des Grandes Ecoles

CERT : Computer Emergency Response Team

COMEX : COMité EXécutif

CNIL : Commission Nationale de l'Informatique et des Libertés

CNAM : Conservatoire National des Arts et Métiers

CNCP : Commission Nationale de la Certification Professionnelle

CPNEFP : Commission Paritaire Nationale de l'Emploi et de la Formation Professionnelle

CTI : Commission des Titres d'Ingénieurs

DPD : Délégué à la Protection des Données

DPO : Data Protection Officer

DRH : Direction des Ressources Humaines

ESSI : Expert en Sécurité des Systèmes d'Information

FIC : Forum International de la Cybersécurité

GdC : Gestion de Crise

IAM : Gestion des Identités et des Accès (Identity and Access Management)

IT : Information Technology

IUT : Institut Universitaire de Technologie

LMP : Loi de Programmation Militaire

MRSI : Manager des Risques des Systèmes d'Information

MS : Mastère Spécialisé

NCWF : NICE Cybersecurity Workforce Framework

NIST : National Institute of Standards and Technology

OIV : Opérateur d'Importance Vitale

OPCA : Organisme Paritaire Collecteur Agréé

OPIIEC : Observatoire Paritaire de l'Informatique, de l'Ingénierie, des Etudes et du Conseil

PCA : Plan de Continuité d'Activité

PEC : Pôle d'Excellence Cyber

PME : Petites et Moyennes Entreprises

PMO : Project Management Office

PRA : Plan de Reprise d'Activité

RIMS : Réseaux Informatiques, Mobilité et Sécurité

RGPD : Règlement Général sur la Protection des Données

RNCP : Répertoire National de la Certification Professionnelle

RPCA : Responsable du Plan de Continuité d'Activité

RSFS : Réseaux Sans Fil et Sécurité

RSSI : Responsable de la Sécurité des Systèmes d'Information

SAFE : Sécurité, Audit, Informatique lEgale

SIIV : Systèmes d'Information d'Importance Vitale

SIS : Systèmes d'Information Sécurisés

SSI : Sécurité des Systèmes d'Information

SSIC : Sécurité des Systèmes d'Information et de Communication

SOC : Security Operations Center ou Centre des Opérations de Sécurité (COS)

TPE : Très Petite Entreprise

Annexe 1 – Panel d'entreprises et organismes rencontrés dans le cadre de cette étude

Entreprise / Organisme	
Accenture	IBM France
Amossys	Informatique CDC
ANSSI	ISEP
Beijaflore	Microsoft
Cap Gemini	Orange Cyberdéfense
Centrale Supélec	Sanofi
DGSIC - Ministère de la Défense	Sekoia
Dictis	Société Générale
ESIEA	Sogeti
EPITA	Université de Limoges
Fidens	Université de Valenciennes
Formind	Telecom ParisTech
Global Knowledge	Wallix
HSC by Deloitte	Wavestone

Annexe 2 – Bibliographie

ANSSI, Février 2011, « Défense et sécurité des systèmes d'informations, Stratégie de la France »

CEIS, « Quelles sont les évolutions possibles de la gestion du personnel de défense pour lutter efficacement dans le cyberespace ? »

CEIS, Décembre 2014, « Quel référentiel pour les métiers de la cybersécurité ? »

Cigref, Octobre 2016, Le « collaborateur 2020 » son profil, ses compétences Quelle politique pour l'attirer et le garder ?

EY, 2015, « Cybersécurité : créer les conditions de la confiance dans le monde digital »

EY, Janvier 2015, « Cyberattaques : Prenez de l'avance sur les cybercriminels »

EY & LinkedIn, 2014, La Révolution des Métiers « Nouveaux métiers, nouvelles compétences : quels enjeux pour l'entreprises ? »

IBM Institute for Business Value, Février 2016, « La Cybersécurité et les dirigeants »

NIST, Novembre 2016, NICE Cybersecurity Workforce Framework (NCWF)

PAC, 2015, Cybersécurité "Investissements, opportunités et challenges pour les entreprises françaises »

Sopra Steria, 2016, Avis d'expert « Quand la sécurité devient un avis levier compétitif »

Xerfi, Juin 2015, « Le marché de la cybersécurité en France et dans le monde »

Wavestone, Novembre 2016, « Opérateur d'importance vitale, cybersécurité et conformité LPM »

Annexe 3 - Questionnaire de l'enquête en ligne

Test Cybersécurité

Quelle place pour la cybersécurité dans votre entreprise ?

Le saviez-vous ?

- **81%** des entreprises françaises ont été visées par une cyberattaque en 2015
- Se remettre d'un incident de sécurité coûte en moyenne **800 000 €**
- **9 semaines** sont nécessaires pour réparer les dégâts causés par une cyberattaque

Et vous ? Nous vous permettons d'exprimer les besoins de votre entreprise en termes de protection et de ressources en cybersécurité.

Participez à l'enquête « Quelle place pour la cybersécurité dans votre entreprise ? »

L'**OPIIEC**, l'observatoire Paritaire des métiers du numérique, de l'ingénierie, des études et du conseil et des métiers de l'événement, lance une étude sur les compétences et les besoins des entreprises en France sur la **cybersécurité**, qui paraîtra en mai 2017. L'OPIIEC a mandaté **EY** pour la conduite de cette étude.

Cette enquête, adressée à un échantillon de dirigeants, recruteurs et responsables cybersécurité a pour objectif de mieux comprendre les besoins de recrutement de professionnels de la sécurité, de mettre en évidence les compétences recherchées chez les candidats et de comprendre si les formations y répondent à vos besoins.

10 minutes de votre temps seulement !

Totalement confidentiel, le temps de remplissage du questionnaire est estimé à 10 minutes seulement.

Aidez-nous à mieux comprendre vos attentes, afin de mieux orienter les étudiants et professionnels du secteur et d'aider à l'évolution des formations initiales et continues.

Merci par avance,

L'équipe projet de l'étude (OPIIEC et EY)

- A propos de vous

1. Quel est le nom de votre entreprise?

* 2. Quelle est votre fonction au sein de l'entreprise?

- Présidence / Direction générale
- Direction financière
- Direction des ressources humaines
- Direction des systèmes d'information
- Autre (veuillez préciser)

3. Quelle est la taille de votre entreprise (effectifs salariés)?

De 1 à 9 personnes | De 10 à 49 personnes | De 50 à 500 personnes | Plus de 500 personnes

* 4. Quel est le nombre de personnes travaillant dans la cybersécurité au sein de votre entreprise?

1 personne | De 2 à 10 personnes | De 11 à 20 personnes | Plus de 20 personnes

5. Où sont situées vos équipes cybersécurité?
(possibilité de cocher plusieurs cases)

Auvergne-Rhône-Alpes	Hauts-de-France	Pays-de-la-Loire
Bourgogne-Franche-Comté	Ile-de-France	Provence-Alpes-Côte d'Azur
Bretagne	Nouvelle-Aquitaine	Corse
Centre-Val-de-Loire	Normandie	A l'étranger
Grand Est	Occitanie	

* 6. Selon vous, quelle va être l'évolution des effectifs de l'équipe cybersécurité dans les années à venir (horizon 3 ans)?

- En croissance
- Stable
- En diminution

7. Pourriez-vous nous donner les raisons de cette évolution?

- Les métiers de cybersécurité dans votre entreprise

8. Quels sont les métiers les plus représentés dans votre entreprise ?
(possibilité de cocher plusieurs cases)

- ☐ Responsable de la Sécurité des Systèmes d'Information (RSSI)
- ☐ Responsable d'exploitation informatique
- ☐ Chef de projet SSI
- ☐ Architecte sécurité
- ☐ Intégrateur
- ☐ Administrateur sécurité
- ☐ Responsable centre de supervision (SOC)
- ☐ Autre (veuillez préciser)
- ☐ Analyste cybersécurité
- ☐ Ingénieur chargé d'analyse en détection d'intrusions
- ☐ Consultant cybersécurité
- ☐ Auditeur technique
- ☐ Pen testeur
- ☐ Expert en cybersécurité

9. A horizon 5 ans, quels facteurs externes vont faire évoluer ces métiers?

- ☐ Transformation numérique
- ☐ Evolutions réglementaires
- ☐ Evolution des usages (cloud, BYOD...)
- ☐ Nouvelles menaces (phishing, fraude au président...)
- ☐ Autre (veuillez préciser)

10. A horizon 5 ans, quels nouveaux métiers sont susceptibles d'émerger?

11. Comment qualifieriez-vous le niveau de sensibilisation aux problématiques de cybersécurité suivant les niveaux suivants:

	Faible	Moyen	Fort
Au niveau de la direction générale	○	○	○
Au niveau des salariés	○	○	○

- Les compétences recherchées en cybersécurité

* 12. Quelles sont les compétences les plus recherchées aujourd'hui pour vos équipes en cybersécurité ?
(possibilité de cocher plusieurs cases)

- ☐ Protection des informations
- ☐ Gestion et analyse des risques (méthodologies telles que EBIOS, MEHARI)
- ☐ Gestion de continuité d'activité (PCA/PRA)
- ☐ Gestion des accès et des identités (IAM)
- ☐ Sécurité des applications (mobile, web)
- ☐ Autre (veuillez préciser)
- ☐ Audit de sécurité (technique et organisationnel)
- ☐ Adaptabilité et flexibilité
- ☐ Anglais en contexte professionnel
- ☐ Curiosité intellectuelle / ouverture à d'autres environnements

13. A horizon 5 ans, quelles seront les compétences les plus recherchées?

- Le recrutement en cybersécurité

* 14. Quels sont les canaux de recrutement que vous utilisez en cybersécurité ?
(possibilité de cocher plusieurs cases)

- ☐ Annonces sur le site internet de l'entreprise
- ☐ Annonces sur les réseaux professionnels
- ☐ Recours à des cabinets de recrutement
- ☐ Autre (veuillez préciser)
- ☐ Directement auprès des écoles (forum...)
- ☐ Réseau interne (bouche à oreille)

15. Quels sont les métiers sur lesquels vous recrutez aujourd'hui?

16. Si vous rencontrez des difficultés de recrutement, quelles sont les raisons ?
(possibilité de cocher plusieurs cases)

- ☐ Manque de candidats
- ☐ Inadéquation des formations aux besoins métiers
- ☐ Attractivité salariale
- ☐ Autre (veuillez préciser)
- ☐ Difficultés géographiques
- ☐ Attractivité / image de l'entreprise
- ☐ Pas de difficulté de recrutement

* 17. Quels sont les métiers où vous rencontrez des difficultés ?
(possibilité de cocher plusieurs cases)

- ☐ Pas de difficulté de recrutement
- ☐ Responsable de la Sécurité des Systèmes d'Information (RSSI)
- ☐ Responsable d'exploitation informatique
- ☐ Chef de projet SSI
- ☐ Architecte sécurité
- ☐ Intégrateur
- ☐ Administrateur sécurité
- ☐ Autre (veuillez préciser)
- ☐ Responsable centre de supervision (SOC)
- ☐ Analyste cybersécurité
- ☐ Ingénieur chargé d'analyse en détection d'intrusions
- ☐ Consultant cybersécurité
- ☐ Auditeur technique
- ☐ Pen testeur
- ☐ Expert en cybersécurité

18. Souhaitez-vous ajouter des précisions sur ces difficultés de recrutement ?

- Adéquation de l'offre de formations en cybersécurité avec vos besoins

* 19. Selon vous, l'offre en formation initiale couvre-t-elle de manière adéquate vos besoins en cybersécurité?

○ Oui, tout à fait ○ Oui, plutôt ○ Plutôt non ○ Non, pas du tout

* 20. Et la formation continue de vos salariés en cybersécurité ?

○ Oui, tout à fait ○ Oui, plutôt ○ Plutôt non ○ Non, pas du tout

21. L'inadaptation de l'offre en formation aux besoins en compétences cybersécurité de votre entreprise que vous signalez est-elle liée à :

- ☐ des thématiques de formation non couvertes
- ☐ un problème de qualité ou de niveau des formations
- ☐ un mode d'apprentissage inadapté
- ☐ d'autres facteurs

22. Pourriez-vous préciser ces autres facteurs ?

23. Souhaiteriez-vous apporter des précisions ou faire une remarque sur ce questionnaire et cette étude ?

Nous vous remercions pour le temps que vous aurez bien voulu consacrer à ce questionnaire.

Annexe 4 - Codes NAF de références pour la Branche

CHAMP D'APPLICATION				
Activités	**NAF**	**libellé**	**NAF rév 2**	**libellé**
NUMERIQUE	721Z	Conseil en systèmes informatiques	6202A	Conseil en systèmes et logiciels informatiques
	722A	Edition de logiciels (non personnalisés)	5821Z	Édition de jeux électroniques
			5829A	Édition de logiciels système et de réseau
			5829B	Edition de logiciels outils de développement et de langages
			5829C	Edition de logiciels applicatifs
	722C	Autres activités de réalisation de logiciels	6201Z	Programmation informatique
			6202A	Conseil en systèmes et logiciels informatiques
			6202B	Tierce maintenance de systèmes et d'applications informatiques
			6209Z	Autres activités informatiques
	723Z	Traitement de données	6203Z	Gestion d'installations informatiques
			6311Z	Traitement de données, hébergement et activités connexes
	724Z	Activités de banques de données	5812Z	Édition de répertoires et de fichiers d'adresses
			5821Z	Édition de jeux électroniques
			5829A	Édition de logiciels système et de réseau
			5829B	Edition de logiciels outils de développement et de langages
			5829C	Edition de logiciels applicatifs
			6201Z	Programmation informatique
			6311Z	Traitement de données, hébergement et activités connexes
			6312Z	Portails Internet
CONSEIL	741E	Études de marché et sondages	7320Z	Études de marché et sondages
CONSEIL	741G	Conseil pour les affaires et la gestion	7022Z	Conseil pour les affaires et autres conseils de gestion
			7490B	Activités spécialisées, scientifiques et techniques diverses
			7021Z	Conseil en relations publiques et communication
INGE	742C	Ingénierie, études techniques	7112B	Ingénierie, études techniques
			7490B	Activités spécialisées, scientifiques et techniques diverses
	743B	Analyses, essais et inspections techniques	7120B	Analyses, essais et inspections techniques
CONSEIL	745A	Sélection et mise à disposition de personnel	7810Z	Activités des agences de placement de main-d'œuvre
			7830Z	Autre mise à disposition de ressources humaines
Traduction	748F	Secrétariat et traduction	7430Z	Traduction et interprétation
Métiers de l'évenement	748J	Organisation de foires et salons	8230Z	Organisation de salons professionnels et congrès
			43.32C	agencement de lieux de vente, montage de stands
			25.11Z	fabrication de structures métalliques et éléments modulaires pour Exposition.
			90.04Z	gestion de salles de spectacles **(uniquement dans le cadre des foires et salons).**
			68.32A	administration d'immeubles et autres bien immobiliers **(uniquement dans le cadre des foires et salons).**
			68.20B	location de terrains et autres biens immobiliers : halls d'exposition, salles de conférence, de réception, de réunion. **(uniquement dans le cadre des foires et salons).**

Annexe 5 – Matrice des métiers et leurs compétences

4 degrés de maitrise des compétences correspondant aux niveaux attendus:
D'une maîtrise partielle ... à complète

- Compétences fonctionnelles

Intitulé Métier	Analyse et cartographie des risques (EBIOS, MEHARI, ISO 27005,etc)	Normes de sécurité (ISO 2700x)	Elaboration des politiques et des procédures de sécurité de l'information	Gestion des incidents de sécurité (cyber crise)	Gestion du plan de continuité et de reprise d'activité (PCA/PRA)	Sensibilisation et formation aux enjeux de la sécurité	Veille sur les évolutions réglementaires (LPM, NIS, RGS, RGPD, etc.)	Protection de la vie privée (Data privacy)	Classification et protection des informations
Responsable de la Sécurité des Systèmes d'Information (RSSI)	●	●	●	◕	◕	●	◕	●	●
Correspondant Sécurité	◕	◕	◕	◕	◕	●	●	●	●
Responsable du Plan de Continuité d'Activité (RPCA)	◕	◕	◕	●	●	◑	◑	◑	◕
Directeur de programme sécurité	◕	◕	◕	◑	◕	◕	◕	●	●
Chef de projet sécurité	◕	◕	◕	◑	◕	●	◕	●	●
Développeur sécurité	◑	◑	◔	◔	◕	◕	◔	◕	◕
Architecte sécurité	◔	◑	◔	◑	◕	◕	◔	●	●
Administrateur sécurité	◔	◑	◑	◕	◕	◕	◑	◕	◕
Technicien sécurité	◔	◑	◑	◕	◕	◕	◑	◕	◕
Analyste SOC (Security Operations Center)	◑	◑	◔	●	●	◔	◑	◕	◕
Chargé de la réponse aux incidents	◑	◑	◔	●	●	◑	◑	◕	◕
Consultant/auditeur gouvernance, risques et conformité	●	◕	◕	◕	◕	◕	◕	◕	◕
Consultant/auditeur sécurité technique	◑	◑	◔	◑	◔	◕	◔	◑	◕
Evaluateur sécurité des systèmes et des produits	◑	◑	◔	◔	◕	◕	◔	◕	◕
Cryptologue	◔	◑	◔	◑	◔	◑	◑	◕	◕
Expert juridique en cybersécurité	◑	◑	◑	◑	◑	◕	●	◕	◑
Délégué à la Protection des Données (DPD)	◑	◑	◑	◑	◑	◕	◕	●	◑
Formateur en sécurité	◕	◕	◕	◕	◕	◕	◕	◕	◕

4 degrés de maitrise des compétences correspondant aux niveaux attendus:

D'une maîtrise partielle ... à complète

- Compétences techniques

Intitulé métier	Architecture de sécurité (sondes, IDS/IPS, firewalls…)	Sécurité des réseaux et des télécommunications	Sécurité des systèmes d'exploitation (Windows, UNIX, etc.)	Sécurité des applications (mobile, web, langage de programmation)	Cryptographie	Détection, réponse à incident et Forensics	Gestion des accès et des identités (IA&M)	Audit de sécurité (technique et organisationnel)	Tests d'intrusion	Sécurité liée aux nouveaux usages (Cloud Computing, BYOD, objets connectés,etc)
Responsable de la Sécurité des Systèmes d'Information (RSSI)	◑	◑	◑	◑	◑	◑	◑	◑	◑	◑
Correspondant Sécurité	◑	◑	◑	◑	◑	◑	◑	◑	◑	◑
Responsable du Plan de Continuité d'Activité (RPCA)	◕	◕	◕	◕	◑	◕	◑	◑	◑	◑
Directeur de programme sécurité	◕	◕	◕	◕	◕	◕	◕	◑	◑	◕
Chef de projet sécurité	◕	◕	◕	◕	◕	◕	◕	◑	◑	◕
Développeur sécurité	◕	◕	◕	●	◕	◔	◕	◑	◕	◕
Architecte sécurité	●	●	◕	◕	◕	◕	◕	◑	◑	●
Administrateur sécurité	◕	◕	◑	◑	◑	◕	◑	◔	◔	◕
Technicien sécurité	◕	◕	◑	◑	◑	◕	◑	◔	◔	◕
Analyste SOC (Security Operations Center)	◑	◑	◑	◑	◑	◑	◕	◑	◑	◑
Chargé de la réponse aux incidents	◑	◑	◑	◑	◑	◑	◑	◑	◑	◕
Consultant/auditeur gouvernance, risques et conformité	◕	◕	◕	◕	◕	●	◕	◕	●	◕
Consultant/auditeur sécurité technique	◕	◕	◑	◑	◕	◕	◑	◑	◕	◕
Evaluateur sécurité des systèmes et des produits	◕	◕	◕	●	◕	◔	◕	◑	◕	◕
Cryptologue	◑	◑	◑	◑	◑	◔	◑	◕	◑	◕
Expert juridique en cybersécurité	◕	◕	◕	◕	●	◔	◑	◑	◑	◕
Délégué à la Protection des Données (DPD)	◑	◑	◑	◑	◑	◑	◑	◑	◑	◑
Formateur en sécurité	◑	◑	◑	◑	◑	◑	◑	◑	◑	◑

4 degrés de maitrise des compétences correspondant aux niveaux attendus:

D'une maîtrise partielle ... à complète

- Capacités transverses (1/2)

Intitulé Métier	Leadership et esprit d'entreprise	Adaptabilité et flexibilité	Analyse et synthèse	Communication orale et écrite	Conviction et influence	Créativité et sens de l'innovation	Gestion de projet	Gestion de la performance
Responsable de la Sécurité des Systèmes d'Information (RSSI)	●	◕	●	●	●	●	◕	◕
Correspondant Sécurité	◑	◕	●	●	●	◕	◕	◕
Responsable du Plan de Continuité d'Activité (RPCA)	●	●	●	●	●	◑	◑	◕
Directeur de programme sécurité	●	◕	◕	●	●	◕	●	●
Chef de projet sécurité	●	◕	●	●	●	◕	●	●
Développeur sécurité	◑	●	◕	◕	◑	●	◑	◔
Architecte sécurité	●	◕	●	●	●	◕	◕	◕
Administrateur sécurité	◑	◕	◕	◕	◑	◑	◑	●
Technicien sécurité	◔	●	◕	◕	◔	◔	◑	◕
Analyste SOC (Security Operations Center)	●	◕	●	●	◕	◔	◔	●
Chargé de la réponse aux incidents	●	◕	●	●	◕	◔	◔	●
Consultant/auditeur gouvernance, risques et conformité	◕	●	●	●	●	◕	◕	◑
Consultant/auditeur sécurité technique	◕	●	◕	●	◕	◕	◕	◑
Evaluateur sécurité des systèmes et des produits	◑	●	◕	◕	◑	●	◑	◔
Cryptologue	◑	◑	◕	◕	●	●	◑	◑
Expert juridique en cybersécurité	◑	●	●	●	●	◔	◔	◔
Délégué à la Protection des Données (DPD)	◕	◕	◕	●	●	◔	◔	◔
Formateur en sécurité	◔	◕	◕	●	●	◔	◑	◔

4 degrés de maitrise des compétences correspondant aux niveaux attendus:

D'une maîtrise partielle ... à complète

- Capacités transverses (2/2)

Intitulé Métier	Orientation client	Rigueur et organisation	Sens relationnel	Travail en équipe et animation d' équipe	Anglais en contexte professionnel	Capacité d'écoute	Gestion du stress et des imprévus	Respect des règles de confidentialité	Capacité d'anticipation	Curiosité intellectuelle / ouverture à d'autres environnements
Responsable de la Sécurité des Systèmes d'Information (RSSI)	●	◕	●	●	●	●	◑	●	●	●
Correspondant Sécurité	●	●	●	●	◕	●	◕	●	◕	●
Responsable du Plan de Continuité d'Activité (RPCA)	●	◕	◕	◕	●	◕	◑	◕	●	◑
Directeur de programme sécurité	●	●	●	●	●	◕	◑	●	●	●
Chef de projet sécurité	●	●	●	●	●	◕	●	●	◑	◑
Développeur sécurité	●	◕	◑	●	◕	◕	◕	◕	◕	●
Architecte sécurité	●	●	◕	◕	●	◕	◑	◕	◑	●
Administrateur sécurité	●	●	◕	●	●	●	●	●	◕	◔
Technicien sécurité	●	●	◕	●	●	●	●	●	◑	◑
Analyste SOC (Security Operations Center)	◕	◕	◕	●	●	◕	●	●	◑	◕
Chargé de la réponse aux incidents	◕	◕	◕	●	●	◕	●	●	◑	◕
Consultant/auditeur gouvernance, risques et conformité	●	◕	●	◕	●	●	◑	●	◕	◕
Consultant/auditeur sécurité technique	●	◕	◕	◕	●	●	◕	●	◕	◕
Evaluateur sécurité des systèmes et des produits	●	◕	◑	●	◕	◕	◕	◕	◕	●
Cryptologue	◑	●	◑	●	●	◑	◑	◕	●	●
Expert juridique en cybersécurité	◕	●	●	◑	◕	●	●	●	●	◑
Délégué à la Protection des Données (DPD)	◑	●	◕	◑	◑	◕	◕	●	◕	◑
Formateur en sécurité	◑	◕	●	●	◕	●	◑	◔	◑	●

Annexe 6 : Guide d'entretien pour la phase 2 « état des lieux de l'offre de formation »

ETUDE SUR LES FORMATIONS ET LES COMPETENCES EN FRANCE SUR LA CYBERSECURITE

Guide d'entretien

1. Présentation de l'étude

L'OPIIEC, l'observatoire Paritaire des métiers du numérique, de l'ingénierie, des études et du conseil et des métiers de l'événement, lance une étude sur les compétences et les besoins des entreprises en France sur la cybersécurité, qui paraîtra en mai 2017. L'OPIIEC a mandaté EY pour la conduite de cette étude.

L'objectif est de :

- Dresser un état des lieux qualitatif et quantitatif des métiers et des compétences en matière de cybersécurité
- Cartographier l'offre de formation initiale et continue existante en France notamment dans l'enseignement supérieur

Cet entretien a vocation à ouvrir avec les acteurs du secteur une discussion sur l'évolution des métiers et des compétences de la cybersécurité, et d'identifier leurs attentes vis-à-vis des professionnels de la filière.

2. Questionnaire

Présentation de l'offre de formation

1. Quelle est l'offre de formation (initiale ou continue) proposée en cybersécurité dans votre établissement ?
2. Quel est le public cible pour ces formations ? (Bac, étudiants Bac +3, jeunes professionnels…)
3. Pour vos principales filières de formation, quelle est la capacité annuelle maximum de formation ? Cette capacité est-elle atteinte ?
4. Sur les 5 dernières années, quel a été le rythme de croissance des demandes d'inscriptions ? De l'ouverture de places de formation ?
5. Selon vous, quel va être le taux de croissance des demandes d'inscription dans vos cursus dans les 5 prochaines années ?
6. Rencontrez-vous des difficultés à recruter dans vos cursus de formation ?
7. Où est dispensée géographiquement cette formation ? Y a-t-il des cours à distance/en ligne ?
8. Quelles sont les certifications diplômantes / certifiantes proposées par votre établissement ?
9. Quels sont les débouchés ? (poursuite des études, suite des parcours, métiers-cibles…)
10. Quels sont les contenus pédagogiques les plus stratégiques pour le marché aujourd'hui ?

Adéquation de l'offre de formation aux besoins actuels et évolutions à venir

Parmi les résultats de la phase 1 sur les métiers et les compétences recherchées en cybersécurité :
Les principales compétences recherchées par les entreprises dans les années à venir sont :

- Compétences techniques : sécurité des applications, gestion des accès et des identités, audit de sécurité
- Compétences fonctionnelles : protections des informations, gestion de continuité d'activité, supervision cybersécurité
- Capacités transversales : adaptabilité/flexibilité, respect des règles de confidentialité, curiosité intellectuelle

Les principaux métiers que les entreprises souhaitent recruter actuellement sont : consultants en cybersécurité, administrateur système réseau, chef de projet cybersécurité, architecte sécurité, administrateur sécurité

11. Votre offre de formation permet-elle de répondre à ces attentes en termes de développement et enrichissement de compétences ?
12. Quelles sont vos pistes et priorités pour l'actualisation des contenus des programmes pédagogiques ?
13. Quelles sont les attentes du marché de l'emploi vis-à-vis de vos diplômés ? Quelles pistes pourraient être envisagées pour continuer, ou mieux répondre, aux attentes du marché ?

Visions prospectives

14. Comment intégrez-vous les évolutions réglementaires à venir (RGPD…) dans votre contenu pédagogique ?
15. Selon vous, comment est-il possible d'innover sur la formation des personnes en cybersécurité ?
16. A quoi pourrait ressembler l'école de la Cybersécurité de demain (sur la formation initiale et continue) ?

Annexe 7 : Cartographie de l'offre de formation dispensée par les établissements d'enseignement supérieur

A noter que les informations sur les voies d'accès (formation initiale, formation continue, VAE) sont issues des fiches du RNCP.

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
ISIMA (Institut supérieur d'informatique, de modélisation et de leurs applications)	Ingénieur en informatique. Filière : Réseau et sécurité informatique	Ingénieur	Auvergne Rhône Alpes	X	X		X		Oui
IUT Cézeaux Aubière	Licence MRIT Métiers des Réseaux Informatiques et des Télécommunications. Parcours : Administration Et Sécurité des Réseaux	Licence pro	Auvergne Rhône Alpes	X					Oui
IUT Cézeaux Aubière	Licence MRIT Métiers des Réseaux Informatiques et des Télécommunications. Parcours : Réseaux Sans Fil et Sécurité	Licence pro	Auvergne Rhône Alpes	X					Oui
IUT d'Annecy – Université Savoie Mont Blanc	Licence Professionnelle MI-ASSR (Métiers de l'Informatique mention Administration et Sécurité des Systèmes et Réseaux)	Licence pro	Auvergne Rhône Alpes	X	X	X	X		Oui
Mines Saint Etienne	Sécurité des systèmes intégrés et applications SISA	Mastère spécialisé	Auvergne Rhône Alpes		X				
Université de Clermont-Ferrrand 1	« Administration et Sécurité des Réseaux »	Licence pro	Auvergne Rhône Alpes		X	X	X		
Université de Grenoble Joseph Fourier	« Réseaux Sans Fil et Sécurité »	Licence pro	Auvergne Rhône Alpes	X	X	X	X		
Université de Grenoble Pierre Mendès France	« Administration et Sécurité des réseaux »	Licence pro	Auvergne Rhône Alpes	X	X	X	X		
Université de Lyon 1	Master SAFIR, parcours « Sécurité des systèmes informatiques en finance et en assurance - S2IFA »	Master	Auvergne Rhône Alpes	X					
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cybersecurité »	Master	Auvergne Rhône Alpes	X					
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cryptologie, sécurité et codage de l'information »	Master	Auvergne Rhône Alpes	X					
Université Grenoble Alpes	Master « Sécurité, audit, informatique légale - SAFE »	Master	Auvergne Rhône Alpes	X					

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
Université Joseph Fourier Grenoble I	Licence Professionnelle Réseaux et télécommunications spécialité Administration et sécurité des réseaux	Licence pro	Auvergne Rhône Alpes	X	X	X	X		
Université Lyon 2	Master 2 OPSIE : Organisation et Protection des Systèmes d'Information pour l'Entreprise	Master	Auvergne Rhône Alpes	X	X	X	X		Oui
Université Pierre Mendès France Grenoble II (UPMF)	Licence Professionnelle Mention Systèmes Informatiques et Logiciels Spécialité Métiers de l'administration et de la sécurité des systèmes d'information (MESSI)	Licence pro	Auvergne Rhône Alpes		X	X	X		
Centrale Supélec - Mines-Télécom	Mastère spécialisé en CyberSécurité	Mastère spécialisé	Bretagne		X				Oui
Cnam Bretagne	« Analyste en Sécurité des Systèmes Télécoms Réseaux et Informatiques » ASSTRI	Licence pro	Bretagne	X	X	X	X		
Ecole nationale supérieure d'ingénieurs de Bretagne-Sud	Ingénieur diplômé de l'école nationale supérieure d'ingénieurs de Bretagne-Sud de l'université de Bretagne-Sud spécialité sécurité des systèmes d'information en partenariat avec l'ITII Bretagne	Ingénieur	Bretagne	X					
ENSIBS	Ingénieur ENSIBS Spécialité Cyberdéfense	Ingénieur	Bretagne	X					Oui
ENSIBS	Diplôme d'ingénieur des systèmes de confiance	Ingénieur	Bretagne	X					Oui
ENSIBS	Ingénieur « Management et Ingénierie de sécurité des systèmes - cyberdéfense »	Ingénieur	Bretagne	X					
IUT St Malo – Université Rennes I	LP RSFS-RIMS (Réseaux informatiques, mobilité et sécurité)	Licence pro	Bretagne	X					Oui
Centrale Supélec (Rennes)	Ingénieur « Systèmes d'information sécurisés » SIS	Ingénieur	Bretagne	X					
TELECOM Bretagne	Technologies du Web et Cyber Sécurité (TWCS)	Mastère spécialisé	Bretagne		X				
IUT St Malo – Université Rennes I	« Administration et Sécurité des Réseaux »	Licence pro	Bretagne	X	X	X	X		
Université Rennes I	Master informatique, spécialité « Sécurité des Systèmes d'Information - ISTIC »	Master	Bretagne	X					
Université Rennes I	Master mathématiques de l'information, cryptographie	Master	Bretagne	X	X	X	X		Oui
IUT St Malo – Université Rennes I	Licence Professionnelle Réseaux et télécommunications, spécialité : Réseaux sans fil et sécurité	Licence pro	Bretagne	X	X	X	X		

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
Université Rennes I	MASTER Sciences, technologie, santé, mention informatique, spécialité Sécurité des Systèmes d'Information (SSI)	Master	Bretagne	X	X	X	X		
IUT de Lannion	Licence professionnelle: Administration et gestion des systèmes et réseaux informatiques	Licence pro	Bretagne	X					
IUT de Lannion	Licence professionnelle: Intégration	Licence pro	Bretagne	X					
Cnam Bretagne	Formation d'analyste en sécurité des systèmes télécommunications, réseaux et informatique	Licence pro	Bretagne	X					
ENSIBS	Diplôme universitaire - Gestion de cybercrise	Ingénieur	Bretagne	X					
ENSIBS	Diplôme universitaire - Ingénierie de solutions de sécurité	Ingénieur	Bretagne	X					
Université Rennes I	Master informatique, spécialité recherche en informatique	Master	Bretagne	X	X	X	X		
Université Rennes I	Master électronique, télécommunications et réseaux de l'information, cryptographie	Master	Bretagne	X	X	X	X		
Université Rennes I	Master électronique, télécommunications et réseaux. Spécialité: télécommunications et réseaux	Master	Bretagne	X					
Université Rennes I	Master professionnel: sécurité défense intelligence stratégique SE-DEFIS	Master	Bretagne	X					
Université Rennes I	Master sciences, technologies, santé mention informatique spécialité ingénierie des réseaux	Master	Bretagne	X	X	X	X		
Université Rennes I	Licence Professionnelle Réseaux et télécommunications, spécialité : Réseaux sans fil et sécurité	Licence pro	Bretagne	X	X	X	X		
État-major des Écoles de Sous officiers et militaires du rang	Cursus de l'armée de l'air certifiée élémentaire 8220.22. Réseaux informatiques et sécurité des systèmes d'information et de communications	Ingénieur	Bretagne	X					
État-major des Écoles de Sous officiers et militaires du rang	Cursus de l'armée de l'air certifiée supérieur 8220.45. Réseaux informatiques et sécurité des systèmes d'information et de communications	Ingénieur	Bretagne	X					
École Navale BCRM Brest	Voie d'approfondissement: systèmes d'information et modélisation	Ingénieur	Bretagne	X					
ENSSAT Lannion	Ingénieur télécom et technologies émergentes	Ingénieur	Bretagne	X					
ENSTA Bretagne	Diplôme d'ingénieur de l'ENSTA Bretagne Option systèmes, perception, information, décision (SPID)	Ingénieur	Bretagne	X					

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
INSA Rennes	Diplôme d'ingénieur en informatique option sécurité	Ingénieur	Bretagne	X					
Télécom Bretagne	Formation d'ingénieur généraliste (FIG)	Ingénieur	Bretagne	X					
Télécom Bretagne	Formation d'ingénieur spécialisé en informatique parcours réseaux et télécommunications (FIP)	Ingénieur	Bretagne	X					
Télécom Bretagne	Architecture en cybersécurité	Certificat d'Etudes Spécialisées	Bretagne					X	
ENSTA Bretagne	Mastère spécialisé Architecture des systèmes d'information	Mastère spécialisé	Bretagne		X				
Écoles de Saint-Cyr Coëtquidan	Mastère spécialisé conduite des opérations et gestion des crises en cyberdéfense	Mastère spécialisé	Bretagne		X				
INSA Centre Val de Loire	Ingénieur « Sécurité et technologies informatiques »	Ingénieur	Centre Val-de-Loire	X					
Université de Poitiers	Master « Management des risques informationnels et industriels »	Master	Centre Val-de-Loire	X	X	X	X		
Université de Poitiers	Master Domaine : SCIENCES, TECHNOLOGIES et SANTE Mention : Gestion des Risques Spécialité : Management des Risques et des Systèmes d'information (MRSI)	Master	Centre Val-de-Loire	X	X	X	X		
Université de Tours	« Qualité - Sécurité des Systèmes d'Information »	Licence pro	Centre Val-de-Loire	X	X	X	X		
Ecole nationale supérieure d'ingénieurs de Bourges	Ingénieur diplômé de l'école nationale supérieure d'ingénieurs de Bourges spécialité sécurité et technologies informatiques	Ingénieur	Grand Est	X	X	X	X		
Mines Nancy	Sécurité des systèmes informatiques	Mastère spécialisé	Grand Est		X				
Université de Haute-Alsace	« Administration et Sécurité des réseaux »	Licence pro	Grand Est	X	X	X	X		
Université de Lorraine	« Réseaux Sans Fil et Sécurité »	Licence pro	Grand Est	X	X	X	X		
Université de Lorraine (Mines Nancy, Telecom Nancy, ENSEM)	Master « Security of Computer Systems »	Master	Grand Est	X					
Université de Lorraine	Master « Services, sécurité des systèmes et des réseaux »	Master	Grand Est	X	X	X	X		
Université de Lorraine	Master « Sécurité des systèmes d'information et de communication - SSIC »	Master	Grand Est	X					
Université de Reims Champagne-Ardenne	Master Informatique, Dominante Administration et Sécurité des Réseaux	Master	Grand Est	X					Oui

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
Université de Technologie de Troyes	Mastère Spécialisé « Expert Forensic et Cybersécurité »	Mastère spécialisé	Grand Est		X				Oui
Université Technologique de Troyes	Master « Sécurité des systèmes d'information »	Master	Grand Est	X					
Université de Technologie de Troyes	Ingénieur spécialité "Systèmes, Réseaux et Télécommunications"	Ingénieur	Grand Est	X	X	X	X		
Université des Antilles et de la Guyane	« Administration et Sécurité des Réseaux »	Licence pro	Guyane	X					
TELECOM Lille	Ingénierie de la Cybersécurité (Cybersecurity Engineering)	Mastère spécialisé	Hauts de France		X				Oui
Télécom Lille	Ingénieur « Sécurité des réseaux et des systèmes »	Ingénieur	Hauts de France	X					
Université d'Artois	« Systèmes informatiques et logiciel - Sécurité informatique »	Licence pro	Hauts de France	X					
Université de Valenciennes et du Hainaut Cambrésis	Master Informatique : Parcours Ingénierie des Réseaux COmmunications Mobiles et Sécurité – IRCOMS	Master	Hauts de France	X					Oui
Université de Valenciennes et du Hainaut Cambrésis	« Collaborateur de Défense et Anti Intrusion des Systèmes Informatiques (CDAISI) »	Licence pro	Hauts de France	X	X	X	X		
Université de Valenciennes et du Hainaut Cambrésis	Master « Cyber-défense et sécurité de l'information - CDSI »	Master	Hauts de France	X					
Université de Valenciennes et du Hainaut Cambrésis	Master « Informatique, réseaux et sécurité - IRS »	Master	Hauts de France	X					
Université de technologie de Compiègne	Master Sciences, Technologies, Santé Mention Ingénierie des Services et des Systèmes (ISS) Spécialité Ingénierie des Systèmes d'Information (ISI)	Master	Hauts de France	X	X	X	X		
Ecole supérieure d'électricité (ESE SUPELEC)	Master sciences, technologies, santé mention informatique spécialité services, sécurité des systèmes et des réseaux	Master	Ile-de-France	X					
ENSTA	Architecture et sécurité des systèmes d'information	Mastère spécialisé	Ile-de-France		X				
EPITA	Ingénieur Epita, Majeure « Systèmes, Réseaux et Sécurité »	Ingénieur	Ile-de-France	X					Oui
ESGI	Mastère « Sécurité informatique »	Ingénieur	Ile-de-France	X					
ESIEA	Mastère Spécialisé « Sécurité de l'Information et des Systèmes » de l'ESIEA (MS-SIS)	Mastère spécialisé	Ile-de-France		X				Oui

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
ETNA-Alternance	Ingénieur « Architecte système réseaux et sécurité »	Ingénieur	Ile-de-France	X	X	X	X		
Institut des sciences et technologies de Paris (ParisTech)	Master sciences et technologies spécialité communications et sécurité informatique	Master	Ile-de-France	X					
IONIS-STM	Master « Ingénierie informatique & Management : Sécurité informatique »	Master	Ile-de-France	X					
ISEP Formation Continue	Architecture Cyber-Sécurité et Intégration	Mastère spécialisé	Ile-de-France		X				Oui
ISEP Formation Continue	Management et protection des données à caractère personnel	Mastère spécialisé	Ile-de-France		X				
ISEP	Praticien Légal a la Protection des Données Personnelles	Badge	Ile-de-France						
ISEP	Praticien Technique à la Protection des Données Personnelles	Badge	Ile-de-France						
TELECOM ParisTech	Architecte réseaux et cybersécurité (ARC)	Mastère spécialisé	Ile-de-France		X				
TELECOM ParisTech	Cybersécurité et cyberdéfense	Mastère spécialisé	Ile-de-France		X				
Telecom SudParis	Sécurité des systèmes et des réseaux	Mastère spécialisé	Ile-de-France		X				
Télécom SudParis	Ingénieur « Sécurité des systèmes et des réseaux »	Ingénieur	Ile-de-France	X					
Université de Paris 8, en partenariat avec Paris Diderot (Paris 7)	Master « Mathématiques fondamentales et protection de l'information »	Master	Ile-de-France	X					
Université de Paris Sud	« Sécurité des Réseaux et Systèmes informatiques »	Licence pro	Ile-de-France	X	X	X	X		
Université de Paris-Diderot (Paris 7) - en partenariat avec Paris 8	Master « Mathématiques, Informatique et applications à la Cryptologie - MIC »	Master	Ile-de-France	X	X	X	X		
Université de Paris-Est Créteil (Paris 12)	Master « Sécurité des systèmes informatiques »	Master	Ile-de-France	X					
Université de Versailles Saint-Quentin	« Administration et Sécurité des Réseaux »	Licence pro	Ile-de-France	X	X	X	X		
Université de Versailles-Saint-Quentin	Master « Sécurité des contenus, des réseaux, des télécommunications et des systèmes - SeCReTS »	Master	Ile-de-France	X					

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
Université d'Evry-Val-d'Essonne	Licence Professionnelle Réseaux et télécommunications - Spécialité Réseaux et sécurité pour les télécommunications dans l'entreprise	Licence pro	Ile-de-France	X	X	X	X		
Université Paris 13	« Administration et Sécurité en Réseaux »	Licence pro	Ile-de-France	X	X	X	X		
Université Paris Descartes - Paris 5	MASTER SCIENCES, TECHNOLOGIES, SANTE, à finalité PROFESSIONNELLE ET RECHERCHE, Mention INFORMATIQUE, spécialité RESEAUX ET SECURITE	Master	Ile-de-France	X	X	X	X		
Université Paris Est Créteil Val de Marne	« Réseaux informatiques, mobilité, sécurité (RIMS) »	Licence pro	Ile-de-France	X					
Université Paris-Est Créteil Val-De-Marne	Licence Professionnelle Domaine : Sciences, technologie, santé Licence professionnelle Réseaux et télécommunication Spécialité Administration et sécurité des réseaux	Licence pro	Ile-de-France	X	X	X	X		
Université Paris-Est Créteil Val-De-Marne	Licence Professionnelle Domaine : Sciences, technologie, santé Licence professionnelle Réseaux et télécommunication Spécialité Réseaux sans fil et sécurité	Licence pro	Ile-de-France	X	X	X	X		
Université Pierre et Marie Curie (Paris 6) - avec l'AFTI	Master « Informatique, spécialité SFPN, filière sécurité informatique - MSI »	Master	Ile-de-France	X					
Université Paris 2 Panthéon-Assas	Master 2 Expertise Économique et Juridiques des Systèmes d'Information	Master	Ile-de-France	X					
Ecole Polytechnique	Piloter une démarche de cybersécurité	Autre	Ile-de-France					X	
Université Paris 1 Panthéon Sorbonne	MASTER Mention Droit public et administration publique Spécialité Droit du numérique - Administration - Entreprises	Master	Ile-de-France	X	X	X	X		
INGETIS	Expert en système informatique	Autre	Ile-de-France	X	X	X	X		
ECTEI (Ecole centrale des techniques de l'environnement industriel)	Responsable de la sécurité des systèmes d'information et des réseaux	Master	Ile-de-France	X	X	X	X		
ESIEA	BADGE " Sécurité Offensive / Pentest "	Badge	Ile-de-France		X				
ESIEA	BADGE « Reverse Engineering »	Badge	Ile-de-France		X				
ESIEA	Ingénieur des technologies du numérique option cyber défense/sécurité	Ingénieur	Ile-de-France & Pays de la Loire	X					Oui

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
ESIEA	Ingénieur parcours « Fundamentals of Security (SEC) »	Ingénieur	Ile-de-France & Pays de la Loire	X					
ENSICAEN	Ingénieur « Monétique et sécurité des systèmes »	Ingénieur	Normandie	X					
ESIGELEC	Ingénieur « Architecture et sécurité des réseaux - ASR »	Ingénieur	Normandie	X					
Université de Basse Normandie	Master « Réseaux et sécurité des systèmes informatiques »	Master	Normandie	X					
Université de Caen Normandie	Licence Professionnelle Système informatiques et logiciels spécialité Audit et sécurité des réseaux et des systèmes d'information	Licence pro	Normandie	X	X	X	X		
Université de Caen Normandie	Licence Professionnelle Management des organisations spécialité Qualité-Sécurité-Environnement	Licence pro	Normandie	X	X	X	X		
Université de Rouen	« Administration Sécurité des Réseaux »	Licence pro	Normandie	X	X	X	X		
Université de Rouen	Master « Sécurité des Systèmes Informatiques (SSI) »	Master	Normandie	X	X	X	X		
INSA Rouen	Ingénieur diplômé de l'Institut National des Sciences Appliquées de Rouen, spécialité Architecture des Systèmes d'Information	Ingénieur	Normandie	X	X	X	X		
Université du Havre	Master « Systèmes informatiques, Réseaux et Sécurité - MATIS »	Master	Normandie	X					
ENSEIRB-MATMECA (Bordeaux INP)	cybeR-sécurité, Systèmes et Réseaux (RSR)	Ingénieur	Nouvelle Aquitaine	X					Oui
ENSEIRB-MATMECA et l'Institut Polytechnique de Bordeaux	ingénieur diplômé de l'Institut polytechnique de Bordeaux, École Nationale Supérieure d'électronique, informatique, télécommunications, mathématique et mécanique de Bordeaux, spécialité « Réseaux et Systèmes d'Information"	Ingénieur	Nouvelle Aquitaine	X	X		X		
IUT de La Rochelle	Licence Professionnelle MRIT (Métiers des Réseaux Informatiques et des Télécommunications), spécialité ASUR (Administration et SécUrité des Réseaux)	Licence pro	Nouvelle Aquitaine	X	X	X	X		Oui
IUT des Pays de l'Adour (Mont de Marsan) - UPPA	Licence Professionnelle MRIT (Métiers des Réseaux Informatiques et des Télécommunications), spécialité ASUR (Administration et SécUrité des Réseaux)	Licence pro	Nouvelle Aquitaine	X	X	X	X		Oui

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
Université de Bordeaux	Master en Cryptologie et Sécurité Informatique	Master	Nouvelle Aquitaine	X	X	X	X		Oui
Université de Bordeaux 1	« Administration et Sécurité des Réseaux »	Licence pro	Nouvelle Aquitaine	X	X	X	X		
Université de Limoges	Master Informatique Parcours Cryptis	Master	Nouvelle Aquitaine	X					Oui
Université de Limoges	Master Mathématiques Parcours Cryptis	Master	Nouvelle Aquitaine	X					Oui
Université de Limoges	Master « Sécurité de l'Information et Cryptologie - CRYPTIS »	Master	Nouvelle Aquitaine	X	X	X	X		
Ecole nationale de l'aviation civile (ENAC)	MASTER Sciences, technologie, santé, mention informatique, spécialité Sécurité des Systèmes d'Information (SSI)	Master	Occitanie	X					
Toulouse Ingénierie	Ingénieur « TLS-SEC »	Ingénieur	Occitanie	X					
Université de Perpignan Via Domitia	Licence Professionnelle Sciences , technologies, santé ; Mention Métiers de l'informatique : administration et sécurité des systèmes et des réseaux ; Spécialité Administrateur de systèmes	Licence pro	Occitanie	X	X	X	X		
Université de Toulouse 2	« Réseaux Sans Fil et Sécurité »	Licence pro	Occitanie	X	X	X	X		
Université Paul Sabatier - Toulouse 3	Licence Professionnelle Systèmes informatiques et logiciels spécialité Sécurité des réseaux et des systèmes	Licence pro	Occitanie	X		X	X		
Université Sciences et techniques du Languedoc Montpellier II	Licence Professionnelle Réseaux et télécommunications spécialité Réseaux sans fil et sécurité	Licence pro	Occitanie	X	X	X	X		
Université Sciences et techniques du Languedoc Montpellier II	Licence Professionnelle Réseaux et télécommunications spécialité Administration et sécurité des réseaux	Licence pro	Occitanie	X	X	X	X		
Université de Montpellier, IUT de Béziers	Licence professionnelle Administration et SécUrité et des Réseaux (ASUR)	Licence pro	Occitanie & Guyane	X	X	X	X		Oui
Ecole supérieure Angevine d'informatique et de productique (ESAIP)	Titre ingénieur diplômé de l'Ecole Supérieure Angevine d'Informatique et de Productique, spécialité «Sécurité et Prévention des Risques»	Ingénieur	Pays de la Loire	X		X	X		
EPSI	Programme Ingénierie informatique - option Sécurité Informatique	Ingénieur	Pays de la Loire	X					
ESAIP	Ingénieur « Informatique et réseaux, spécialité cybersécurité »	Ingénieur	Pays de la Loire	X					

Nom de l'organisme	Nom de la formation	Type de formation	Région	Formation initiale	Formation continue	VAE	CNCP (répertoire)	CNCP (inventaire)	Labélisé SecNumEdu
IIA Laval	Manager en ingénierie informatique (M2I) option « Management de la sécurité des systèmes d'information (MSSI) »	Master	Pays de la Loire	X					
IUT de La Roche-sur-Yon	Licence Professionnelle administration et sécurité des systèmes et des réseaux	Licence pro	Pays de la Loire	X					Oui
Université de Nantes	« Administration et sécurité des réseaux »	Licence pro	Pays de la Loire	X	X	X	X		
Université d'Orléans	Master « Informatique Nomade, intelligence et sécurité »	Master	Pays de la Loire	X	X	X	X		
Université du Maine - Le Mans	Licence Professionnelle Activités juridiques option droit et sécurité des nouvelles technologies de l'information et de la communication	Licence pro	Pays de la Loire	X					
EURECOM	Ingénieur de spécialisation en « sécurité des systèmes informatiques et des communications »	Ingénieur	Provence Alpes Côte d'Azur	X	X	X	X		
Université d'Aix-Marseille	« Administration et sécurité des réseaux d'entreprises »	Licence pro	Provence Alpes Côte d'Azur	X	X	X	X		
Université de Nice Sophia Antipolis	Ingénieur « Cryptographie, Sécurité, et vie Privée dans les Applications et Réseaux »	Ingénieur	Provence Alpes Côte d'Azur	X					
Université Nice Sophia Antipolis	Licence Professionnelle Sciences, Technologies, Santé - Mention : Réseaux et télécommunications - Spécialité : Réseaux sans fil et sécurité	Licence pro	Provence Alpes Côte d'Azur	X	X	X	X		
Université de la Réunion	« Réseaux Sans Fil et Sécurité »	Licence pro	Réunion	X	X	X	X		
Université de la Réunion	Licence Professionnelle Domaine : SCIENCES, TECHNOLOGIES, SANTE Mention : MÉTIERS DES RÉSEAUX INFORMATIQUES ET TÉLÉCOMMUNICATIONS Parcours : ADMINISTRATION ET SÉCURITÉ DES RÉSEAUX	Licence pro	Réunion	X	X	X	X		

❖ *Formations dispensées par les établissements d'enseignement supérieur, ayant renseignées les familles de métiers cibles*

Nom de l'organisme	Nom de la formation	Type de formation	Région	1. Pilotage, organisation de la sécurité et gestion des risques	2. Management de projets de sécurité et cycle de vie de la sécurité	3. Maintien en condition opérationnelle de la sécurité	4. Support et gestion des incidents de sécurité	5. Conseil, audit et expertise en sécurité
ISIMA	Ingénieur en informatique. Filière : Réseau et sécurité informatique	Ingénieur	Auvergne Rhône Alpes		Architecte sécurité			
IUT Cézeaux Aubière	Licence MRIT Métiers des Réseaux Informatiques et des Télécommunications. Parcours : Administration Et Sécurité des Réseaux	Licence pro	Auvergne Rhône Alpes		Architecte sécurité	Technicien sécurité	Analyste SOC	Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
IUT Cézeaux Aubière	Licence MRIT Métiers des Réseaux Informatiques et des Télécommunications. Parcours : Réseaux Sans Fil et Sécurité	Licence pro	Auvergne Rhône Alpes		Architecte sécurité	Technicien sécurité		Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
IUT d'Annecy – Université Savoie Mont Blanc	Licence Professionnelle MI-ASSR (Métiers de l'Informatique mention Administration et Sécurité des Systèmes et Réseaux)	Licence pro	Auvergne Rhône Alpes			Technicien sécurité		Consultant/auditeur sécurité technique
Université de Grenoble Pierre Mendès France	« Administration et Sécurité des réseaux »	Licence pro	Auvergne Rhône Alpes					Consultant/auditeur sécurité technique
Université Lyon 2	Master 2 OPSIE : Organisation et Protection des Systèmes d'Information pour l'Entreprise	Master	Auvergne Rhône Alpes	RSSI Responsable du Plan de Continuité d'Activité (RPCA)	Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
CentraleSupélec Mines-Télécom	Mastère spécialisé en CyberSécurité	Mastère spécialisé	Bretagne	RSSI				Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
ENSIBS	Ingénieur ENSIBS Spécialité Cyberdéfense	Ingénieur	Bretagne	RSSI Responsable du Plan de Continuité d'Activité (RPCA)	Architecte sécurité		Analyste SOC	Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique

Nom de l'organisme	Nom de la formation	Type de formation	Région	1. Pilotage, organisation de la sécurité et gestion des risques	2. Management de projets de sécurité et cycle de vie de la sécurité	3. Maintien en condition opérationnelle de la sécurité	4. Support et gestion des incidents de sécurité	5. Conseil, audit et expertise en sécurité
ENSIBS	Diplôme d'ingénieur des systèmes de confiance	Ingénieur	Bretagne	RSSI	Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
IUT St Malo – Université Rennes I	LP RSFS-RIMS (Réseaux informatiques, mobilité et sécurité)	Licence pro	Bretagne			Technicien sécurité		Formateur en sécurité
IUT St Malo – Université Rennes I	Licence Professionnelle Réseaux et télécommunications, spécialité : Réseaux sans fil et sécurité	Licence pro	Bretagne					Consultant/auditeur sécurité technique
INSA Centre Val de Loire	Ingénieur « Sécurité et technologies informatiques »	Ingénieur	Centre Val-de-Loire	Correspondant Sécurité	Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
Université de Poitiers	Master « Management des risques informationnels et industriels »	Master	Centre Val-de-Loire					Consultant/auditeur sécurité technique
Université de Poitiers	Master Domaine : SCIENCES, TECHNOLOGIES et SANTE Mention : Gestion des Risques Spécialité : Management des Risques et des Systèmes d'information (MRSI)	Master	Centre Val-de-Loire	RSSI				Consultant/auditeur gouvernance, risques et conformité
Université de Lorraine	Master « Services, sécurité des systèmes et des réseaux »	Master	Grand Est	RSSI				
Université de Reims Champagne-Ardenne	Master Informatique, Dominante Administration et Sécurité des Réseaux	Master	Grand Est			Administrateur sécurité		Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
Université de Technologie de Troyes	Mastère Spécialisé « Expert Forensic et Cybersécurité »	Mastère spécialisé	Grand Est	RSSI Responsable du Plan de Continuité d'Activité (RPCA)	Architecte sécurité	Technicien sécurité	Analyste SOC	Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique Formateur en sécurité
Université de Technologie de Troyes	Ingénieur spécialité "Systèmes, Réseaux et Télécommunications"	Ingénieur	Grand Est		Chef de projet sécurité			Consultant/auditeur sécurité technique

Nom de l'organisme	Nom de la formation	Type de formation	Région	1. Pilotage, organisation de la sécurité et gestion des risques	2. Management de projets de sécurité et cycle de vie de la sécurité	3. Maintien en condition opérationnelle de la sécurité	4. Support et gestion des incidents de sécurité	5. Conseil, audit et expertise en sécurité
TELECOM Lille	Ingénierie de la Cybersécurité (Cybersecurity Engineering)	Mastère spécialisé	Hauts de France					Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique Formateur en sécurité
Université de Valenciennes et du Hainaut Cambrésis	Master Informatique : Parcours Ingénierie des Réseaux COmmunications Mobiles et Sécurité - IRCOMS	Master	Hauts de France	RSSI	Architecte sécurité		Analyste SOC	Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
EPITA	Ingénieur Epita, Majeure « Systèmes, Réseaux et Sécurité »	Ingénieur	Ile-de-France	RSSI	Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
ESIEA	Mastère Spécialisé « Sécurité de l'Information et des Systèmes » de l'ESIEA (MS-SIS)	Mastère spécialisé	Ile-de-France		Chef de projet sécurité			Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
ISEP Formation Continue	Architecture Cyber-Sécurité et Intégration	Mastère spécialisé	Ile-de-France		Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité
Université de Paris Sud	« Sécurité des Réseaux et Systèmes informatiques »	Licence pro	Ile-de-France	RSSI				Consultant/auditeur sécurité technique
Université de Paris-Diderot (Paris 7) - en partenariat avec Paris 8	Master « Mathématiques, Informatique et applications à la Cryptologie - MIC »	Master	Ile-de-France					Consultant/auditeur sécurité technique Cryptologue
Université d'Evry-Val-d'Essonne	Licence Professionnelle Réseaux et télécommunications - Spécialité Réseaux et sécurité pour les télécommunications dans l'entreprise	Licence pro	Ile-de-France	RSSI				
Université Paris-Est Créteil Val-De-Marne	Licence Professionnelle Domaine : Sciences, technologie, santé Licence professionnelle Réseaux et télécommunication Spécialité Réseaux sans fil et sécurité	Licence pro	Ile-de-France		Architecte sécurité			

Nom de l'organisme	Nom de la formation	Type de formation	Région	1. Pilotage, organisation de la sécurité et gestion des risques	2. Management de projets de sécurité et cycle de vie de la sécurité	3. Maintien en condition opérationnelle de la sécurité	4. Support et gestion des incidents de sécurité	5. Conseil, audit et expertise en sécurité
ESIEA	Ingénieur des technologies du numérique option cyber défense/sécurité	Ingénieur	Ile-de-France & Pays de la Loire	RSSI Responsable du Plan de Continuité d'Activité (RPCA)	Architecte sécurité			Consultant/auditeur sécurité technique
Université de Caen Normandie	Licence Professionnelle Système informatiques et logiciels spécialité Audit et sécurité des réseaux et des systèmes d'information	Licence pro	Normandie			Administrateur sécurité		
Université de Rouen	« Administration Sécurité des Réseaux »	Licence pro	Normandie		Architecte sécurité	Administrateur sécurité		
Université de Rouen	Master « Sécurité des Systèmes Informatiques (SSI) »	Master	Normandie		Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité
ENSEIRB-MATMECA (Bordeaux INP)	cybeR-sécurité, Systèmes et Réseaux (RSR)	Ingénieur	Nouvelle Aquitaine		Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
IUT des Pays de l'Adour (Mont de Marsan) - UPPA	Licence Professionnelle MRIT (Métiers des Réseaux Informatiques et des Télécommunications), spécialité ASUR (Administration et SécUrité des Réseaux)	Licence pro	Nouvelle Aquitaine	RSSI	Architecte sécurité			Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
Université de Bordeaux	Master en Cryptologie et Sécurité Informatique	Master	Nouvelle Aquitaine	RSSI				Consultant/auditeur sécurité technique
Université de Limoges	Master Informatique Parcours Cryptis	Master	Nouvelle Aquitaine	RSSI				Consultant/auditeur gouvernance, risques et conformité Consultant/auditeur sécurité technique
Université de Limoges	Master Mathématiques Parcours Cryptis	Master	Nouvelle Aquitaine					Consultant/auditeur sécurité technique Formateur en sécurité
Université de Limoges	Master « Sécurité de l'Information et Cryptologie - CRYPTIS »	Master	Nouvelle Aquitaine	RSSI	Architecte sécurité	Administrateur sécurité		Cryptologue
Université de Montpellier, IUT de Béziers	Licence professionnelle Administration et SécUrité et des Réseaux (ASUR)	Licence pro	Occitanie & Guyane			Technicien sécurité		Consultant/auditeur sécurité technique

Nom de l'organisme	Nom de la formation	Type de formation	Région	1. Pilotage, organisation de la sécurité et gestion des risques	2. Management de projets de sécurité et cycle de vie de la sécurité	3. Maintien en condition opérationnelle de la sécurité	4. Support et gestion des incidents de sécurité	5. Conseil, audit et expertise en sécurité
IUT de La Roche-sur-Yon	Licence Professionnelle administration et sécurité des systèmes et des réseaux	Licence pro	Pays de la Loire			Administrateur sécurité Technicien sécurité		
EURECOM	Ingénieur de spécialisation en « sécurité des systèmes informatiques et des communications »	Ingénieur	Provence Alpes Côte d'Azur		Chef de projet sécurité			Consultant/auditeur gouvernance, risques et conformité
Université de la Réunion	« Réseaux Sans Fil et Sécurité »	Licence pro	Réunion		Architecte sécurité			
Université de la Réunion	Licence Professionnelle Domaine : SCIENCES, TECHNOLOGIES, SANTE Mention : MÉTIERS DES RÉSEAUX INFORMATIQUES ET TÉLÉCOMMUNICATIONS Parcours :ADMINISTRATION ET SÉCURITÉ DES RÉSEAUX	Licence pro	Réunion		Architecte sécurité	Administrateur sécurité		

Annexe 8 : Cartographie des organismes de formations continue « courte » en cybersécurité (liste non exhaustive)

❖ *Principaux organismes de certification en cybersécurité*

Organismes de certification	Description	Site web
GIAC	Accrédité à l'ANSI aux USA, pour les formations SANS	www.giac.org
LSTI	Accrédité au COFRAC en France, pour les formations aux normes ISO27001, ISO22301, ISO27005, et EBIOS, RSSI et CIL	www.lsti-certification.fr
ISC2	Accrédité à l'ANSI aux USA, pour CISSP	www.isc2.org
LPI	Pour Expert Sécurité Linux	www.lpi.org
Information Assurance Certification	Pour la sécurité SCADA	www.iacertification.org
Cloud Security Alliance	Pour la sécurité cloud	www.cloudsecurityalliance.org

❖ *Principaux organismes de formation en cybersécurité*

Société	Description	Site web
Auditware	Propose des formations en sécurité de l'information, cloud computing security, continuité d'activité et management des risques	www.auditware.fr
Byward	Accompagne les entreprises et administrations dans le management de la sécurité de leurs systèmes d'informations, et dispense à ce titre 5 formations en cybersécurité	www.byward.eu
Fidens	Offre des prestations de conseil et d'audit, et également organisme référencé de formation. Fidens est agréé par LSTI depuis 2006.	www.fidens.fr
HSC By Deloitte	Propose à la fois des formations en sécurité technique, en sécurité organisationnelle et en continuité d'activité. HSC est agréé par LSTI depuis 2005.	www.hsc-formation.fr
IBM	Propose 10 formations, référencées pour le Compte Professionnel de Formation (CPF).	www.ib-formation.fr
SANS Institute	Centre de formation en cybersécurité dans toute l'Europe et au Moyen Orient.	www.sans.org
Sekoia	Forme depuis 2008 les professionnels de la gestion des risques en entreprise, RSSI, Risk Manager, RPCA, auditeurs…	www.sekoia.fr
Sysdream	Propose des formations en sécurité informatique depuis 2004.	www.sysdream.com
The Duquesne Group	Propose des formations couvrant les aspects de la continuité d'activité, agréé par LSTI depuis 2012	www.duquesnegroup.com

❖ *Principaux organismes généralistes proposant de formations en cybersécurité*

Société	Description	Site web
Afnor compétences	Agréé par LSTI depuis 2010	www.afnor.org
Capgemini Institut	Agréé par LSTI depuis 2013 100 séminaires en 2017 dont une partie dédiée « Sécurité et gestion des risques ».	www.institut.capgemini.fr
Demos	Spécialiste de la formation proposant plus de 1300 formations interentreprises en France dont 25 spécifiques à la cybersécurité	www.demos.fr
Global Knowledge	Centre de formation professionnelle en information et management. Environ 15% de son activité correspond à des formations en cybersécurité.	www.globalknowlegde.fr
M2I	2ème centre de formation sur le marché français dans la formation professionnelle informatique et management	www.m2iformation.fr
Orsys	Agréé par LSTI depuis 2008. Spécialiste de la formation professionnelle et continue avec une part dédiée à des formations « réseaux et sécurité ».	www.orsys .com

❖ *Principales formations proposant une certification en cybersécurité*

Description	Nom de la certification	Organisme de certification	Inventaire CNCP
Fondamentaux et principes de la sécurité des systèmes d'information	SANS SEC401- GSEC	GIAC	
Sécuriser Windows	SANS SEC505 - GCWN	GIAC	
Expert Sécurité Linux 303	LPIC-3	LPI	
Investigations inforensiques – Windows	SANS FOR408 - GCFE (GIAC Certified Forensic Examiner)	GIAC	
Analyse inforensique avancée et réponse aux incidents	SANS FOR508 - GCFA (GIAC Certified Forensic Analyst)	GIAC	
Analyse et investigation numérique avancées dans les réseaux	SANS FOR572 - GNFA	GIAC	
Investigations inforensiques avancée sur équipements mobiles	SANS FOR585 - GMOB	GIAC	
Rétroingénierie de logiciels malfaisants : Outils et techniques d'analyse	SANS FOR610 - GREM (GIAC Reverse Engineering Malware)	GIAC	
Techniques de hacking, exploitation de failles et gestion des incidents	SANS SEC504 - GCIH (Certified Incident Handler)	GIAC	
Exploitation et Surveillance de la Sécurité	SANS SEC511	GIAC	
Tests d'intrusion des applications web et hacking éthique	SANS SEC542 - GWAPT	GIAC	
Tests d'intrusion avancés des applications web et hacking éthique	SANS SEC642 - GXWAP	GIAC	
Tests d'intrusion et hacking éthique	SANS SEC560 – GPEN	GIAC	X
Tests d'intrusion avancés, exploitation de failles et hacking éthique	SANS SEC660 – GXPN	GIAC	
Protéger les applications web	SANS DEV522 - GWEB (Certified Web Application Defender)	GIAC	
Essentiels juridiques pour gérer la SSI	Certification ESSJUR	LSTI	

Description	Nom de la certification	Organisme de certification	Inventaire CNCP
Correspondant informatique et libertés, formation labellisée par la CNIL	Certification CIL	LSTI	
Formation CISSP	Certified Information Systems Security Professional (CISSP)	ISC2	
Formation RSSI	Certification RSSI	LSTI	
Sécurité du Cloud Computing	Certification CCSK (Certificate of Cloud Security Knowledge)		
Audit des Systèmes de Management de la Sécurité de l'Information	ISO 27001 Lead Auditor	LSTI	
Implémentation des Systèmes de Management de la Sécurité de l'Information	ISO 27001 Lead Implementer	LSTI	X
Gestion des risques en sécurité de l'information avec ISO27005	ISO 27005 Risk Manager	LSTI	X
Gestion des risques en sécurité de l'information avec EBIOS	EBIOS Risk Manager	LSTI	
Audit des Systèmes de Management de la Continuité d'Activité	ISO 22301 Lead Auditor	LSTI	X
Implémentation des Systèmes de Management de la Continuité d'Activité	ISO 22301 Lead Implementer	LSTI	X

Annexe 9 : Tableau des réglementations (et illustration de certaines normes) et des impacts sur les métiers en cybersécurité

Cadre réglementaire en cybersécurité	Principaux métiers concernés	Impacts sur les compétences demandées
Le RGPD (Règlement Général sur la Protection des Données) unifie les règlementations de protection des données existantes dans les pays de l'Union Européenne sous une législation unique, en introduisant des directives sur la manière dont les entreprises devront gérer des informations personnellement identifiables. Il sera applicable à toutes les entreprises ayant des activités en Europe, que les données personnellement identifiables qu'elles gèrent soient stockées dans le périmètre de l'Union Européenne, ou non. Le RGPD demande la nomination obligatoire d'un délégué à la protection des données (Data Protection Officer en anglais) pour les organismes publics ou privés dont « les activités de base [...] exigent un suivi régulier et systématique à grande échelle des personnes concernées » (article 37). Il doit être associé à toutes les questions de protection des données à caractère personnel. Ses principales missions sont de contrôler le respect du règlement, de conseiller le responsable des traitements sur son application et de faire office de point de contact avec l'autorité de contrôle.	- Délégué à la protection des données (DPD) - Responsable de la Sécurité des Systèmes d'Information (RSSI)	- Chiffrement, contrôle d'accès, gestion des logs, - Analyse de risques, politiques de sécurité et formation sécurité
La Loi de Programmation Militaire (LPM) s'impose aux 248 OIV (Opérateurs d'Importance Vitale) identifiés en France et dont la liste est tenue secrète, ont été répartis en 12 secteurs d'activité (télécoms, transports, finances, énergie etc.) afin de pouvoir leur appliquer des règles sur-mesure et adaptées. Les règles qui devront concrètement s'appliquer aux SIIV sont celles rédigées par l'ANSSI en concertation avec les OIV. Elles verront le jour sous la forme d'arrêtés sectoriels, applicables à compter du 1er juillet 2016. Les actions en cours actuellement chez les OIV visent à identifier les écarts de conformités et à budgéter les chantiers requis.	- Responsable de la Sécurité des Systèmes d'Information (RSSI) - Directeur de programme sécurité - Architecte de sécurité - Administrateur sécurité	- Analyse de risques, politiques de sécurité et formation sécurité
La directive de « cybersécurité » NIS (Sécurité des Réseaux et de l'Information) oblige un large éventail d'entreprises du secteur privé à se conformer à de nouvelles exigences de sécurité et de signalement d'incidents. Elle stipule également que les « opérateurs d'infrastructures critiques, » c'est-à-dire les entreprises de services publics, les transports et les entreprises de services financiers, doivent déployer des mesures appropriées pour gérer les risques de sécurité et signaler les incidents graves à une autorité nationale ou à l'équipe d'intervention informatique d'urgence.	- Responsable de la Sécurité des Systèmes d'Information (RSSI) - Analyste CERT	- Supervision et détection des incidents de sécurité

Cadre réglementaire en cybersécurité	Principaux métiers concernés	Impacts sur les compétences demandées
La suite ISO/CEI 27000 (aussi connue sous le nom de Famille des standards SMSI ou ISO27k) comprend les normes de sécurité de l'information publiées conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI, ou IEC en anglais). La suite ISO 2700X contient des recommandations des meilleures pratiques en management de la sécurité de l'information, pour l'initialisation, l'implémentation ou le maintien de systèmes de management de la sécurité de l'information (SMSI, ou ISMS en anglais), ainsi qu'un nombre croissant de normes liées au SMSI.	- Responsable de la Sécurité des Systèmes d'Information (RSSI) - Consultant / auditeur sécurité	- Analyse de risques, politiques de sécurité et formation sécurité
Le Référentiel Général de Sécurité (RGS), a pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives et s'impose ainsi à elles comme un cadre contraignant tout en étant adaptable et adapté aux enjeux et besoins de tout type d'autorité administrative.	- Responsable de la Sécurité des Systèmes d'Information (RSSI) - Consultant / auditeur sécurité	- Compétences techniques (chiffrement, contrôle d'accès, gestion des logs,
La Politique de sécurité des systèmes d'information (PSSIE), portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014, s'applique à tous les systèmes d'information des administrations de l'État : ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'État et autorités administratives indépendantes. Ces administrations sont dénommées « entités » dans le texte. La PSSIE concerne l'ensemble des personnes physiques ou morales intervenant dans ces systèmes d'information, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers agissant au nom et pour le compte des administrations de l'État (prestataires ou sous-traitants) et de leurs employés.	- Responsable de la Sécurité des Systèmes d'Information (RSSI)	- Compétences techniques (chiffrement, contrôle d'accès, gestion des logs
La norme **PCI DSS (Payment Card Industry Data Security Standard)** a été développée par le PCI Security Standards Council qui réunit les grands réseaux émetteurs de cartes (Visa, MasterCard, American Express, Discover, JCB) dans le but de renforcer la sécurité des données des titulaires de cartes et de faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale. En effet, les compromissions de données se sont multipliées au cours de la première décennie du siècle, supportées financièrement par le « domaine émetteur » et il devenait donc nécessaire de renforcer la sécurité dans le « domaine acquéreur » (commerçants et fournisseurs de services de paiements monétiques). Il ne s'agit pas d'une obligation réglementaire stricto sensu, mais d'une obligation contractuelle incontournable compte tenu de la place prise par les réseaux émetteurs.	- Développeur sécurité - Responsable de la Sécurité des Systèmes d'Information (RSSI)	- Sécurité des applications - Sécurité des infrastructures

Cadre réglementaire en cybersécurité	Principaux métiers concernés	Impacts sur les compétences demandées
Le règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE. L'ANSSI est l'un des organismes nationaux chargés de la mise en œuvre de ce règlement.	- Responsable de la Sécurité des Systèmes d'Information (RSSI) - Développeur sécurité - Cryptologue	- Sécurité des applications - Sécurité des infrastructures
La **Loi pour la Confiance dans l'Economie Numérique (LCEN)** contient des dispositions relatives à la cryptologie dans ses articles 29 à 40. L'article 30 de la LCEN libéralise totalement la seule utilisation des moyens de cryptologie.	- Responsable de la Sécurité des Systèmes d'Information (RSSI) - Développeur sécurité - Cryptologue	- Sécurité des applications - Sécurité des infrastructures

Et, de façon générale, toute autre législation ou réglementation actuelle ou à venir ayant un impact sur la sécurité des processus informatisés ou des échanges électroniques et potentiellement applicable aux entreprises.

.

FIN