Etude réalisée par le cabinet EY pour le compte de l'OPIIEC

Rapport de synthèse

Les formations et les compétences en France sur la cybersécurité

Mai 2017

Observatoire paritaire
Numérique
Ingénierie
Etudes et Conseil
Métiers de l'événement
OPIIEC
PROSPECTIVE MÉTIERS

Sommaire

1. Rappel des objectifs de l'étude et des moyens

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, cette dernière 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.

Objectifs de l'étude

- 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.
- Les objectifs de cette 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,
  - Etablir un plan d'actions pour mieux répondre aux attentes et aux besoins des entreprises en métiers et en compétence cybersécurité.

1. Rappel des objectifs de l'étude et des moyens

Méthodologie et moyens utilisés

Cette étude a été conduite en trois phases par le cabinet EY:

Enquête en ligne auprès des entreprises de la Branche

- Questionnaire mis en ligne en phase 1 de l'étude (de décembre 2016 à janvier 2017)
- 227 entreprises (dont 202 de la Branche) ont donné leur point de vue sur: leurs effectifs actuels en cybersécurité, les métiers représentés, les évolutions à venir, les compétences recherchées, le niveau de sensibilisation et l'offre de formation

Entretiens et groupes de travail

- Entretiens auprès d'entreprises spécialisées en cybersécurité (17 dont 12 auprès d'entreprises de la Branche) : phase 1
- Entretiens de formateurs et responsables de formation initiale ou continue en cybersécurité : phase 2
- Atelier de travail sur les formations initiales et continues : phase 2
- Atelier de travail sur les enjeux de la formation en cybersécurité et l'adéquation avec les besoins en termes de compétence, et proposition de plan d'actions : phase 3

Analyses quantitatives et qualitatives

- Revue des publications sectorielles en cybersécurité
- Relevé des offres d'emplois en ligne en cybersécurité
- Modélisation des emplois et prévision de recrutement en cybersécurité pour les entreprises de la Branche
- Revue des catalogues et plaquettes de formations
- Collecte de données en ligne pour les formations (SecNumEdu, CNCP…)

Sommaire

1. Rappel des objectifs de l'étude et des moyens
2. Analyse des besoins en recrutements et en compétences
3. Etat des lieux de l'offre de formation
4. Préconisations et plan d'actions

2. Analyse des besoins en recrutements et en compétences

La cybersécurité, une filière en plein développement

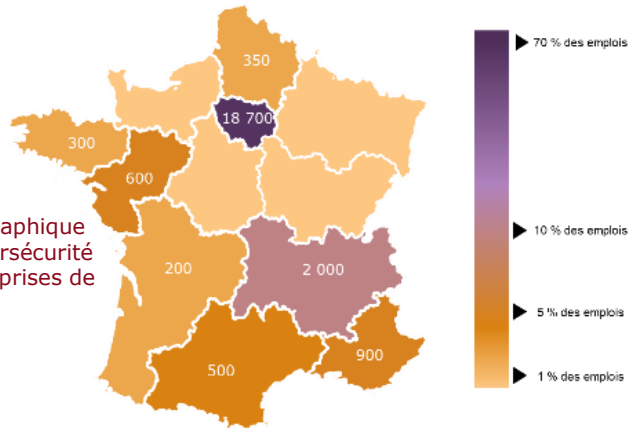
La branche et la cybersécurité : un panel riche d'activités au cœur de la stratégie des entreprises

- 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*.
- Tous les acteurs économiques et les administrations publiques sont aujourd'hui concernés par la cybersécurité, avec des degrés d'exposition au risque et une nécessité de sécurité différents.
- 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 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 de l'entreprises : données clients, secrets de fabrication, commerce en ligne…

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),…
- Avec plus de 24 000 emplois 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).

Répartition géographique des effectifs cybersécurité au sein des entreprises de la Branche



** Source: Sopra Steria, « Quand la sécurité devient un levier compétitif »*
*** Analyse EY pour l'estimation des effectifs en cybersécurité au sein des entreprises de la Branche*

**** Les emplois en cybersécurité, correspondant à une part des effectifs de la Branche, sont le nombre d'emplois salariés (base ETP). Source: modélisation EY 2017 des effectifs cybersécurité au sein de la Branche*

2. Analyse des besoins en recrutements et en compétences

La cybersécurité, une filière en plein développement

Une filière en croissance, et qui recrute !

- La cybersécurité constitue une filière d'avenir. 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.*
- Les pratiques et la perception des problématiques de cybersécurité évoluent auprès de l'ensemble des entreprises et des administrations, mais aussi guidées par l'évolution des réglementations en cybersécurité.
- 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.
- A l'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 l'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 %.
- A l'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.

Une croissance portée notamment par les évolutions réglementaires

Des attaques: toujours plus nombreuses et sophistiquées

81 % des entreprises françaises ont été visées par une cyberattaque en 2015**

59 % des entreprises françaises ont augmenté leurs dépenses en cybersécurité en 2016**

Marqueurs législatifs: dynamiques françaises et internationales

- 2013 : préconisations du livre blanc sur la défense et la sécurité nationale, et Loi de Programmation Militaire (LPM)
- 2015 : décrets relatifs aux Organismes d'Importance Vitale (OIV) et à leurs SIIV
- 2016 et mise en application en 2018: Règlement Général sur la Protection des Données (RGPD)

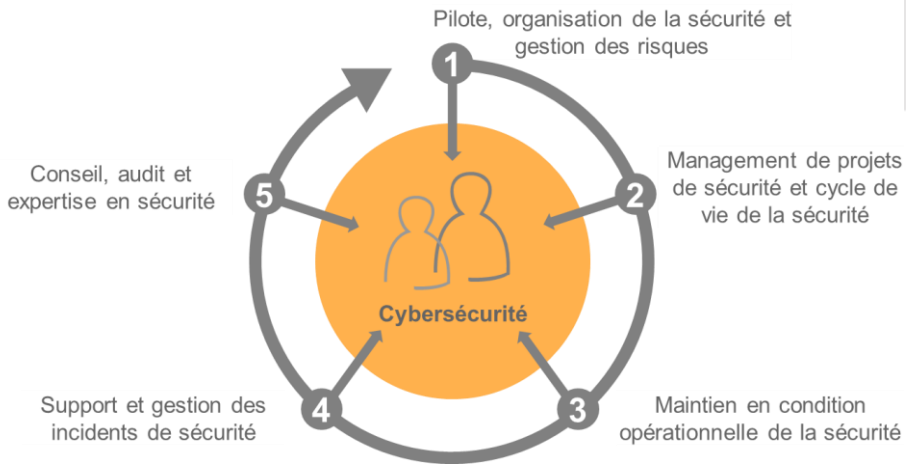
92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD**

* *Source:* BPI France, 2016, « La cybersécurité, une filière d'avenir pour l'offre française »

** *Sources:* Microsoft, Le Parisien Eco 2016, Symantec 2016….

2. Analyse des besoins en recrutements et en compétences

Un écosystème de métiers variés



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.

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.

2. Analyse des besoins en recrutements et en compétences

Cartographie des métiers en cybersécurité

- 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.
- Elle repose sur un premier travail d'analyse des référentiels existants (ANSSI, NIST…). Elle a également été testé et complété lors des entretiens et ateliers menés auprès d'entreprises en cybersécurité, l'ANSSI et organismes de formation initiale et continue.

1. Pilote, 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
Responsable de la Sécurité des Systèmes d'Information (RSSI)	Directrice/eur de programme sécurité	Administratrice/eur sécurité	Analyste SOC (Security Operations Center)	Consultant(e) et auditrice/auditeur gouvernance, risques et conformité
Correspondant(e) Sécurité	Chef de projet sécurité	Technicien(ne) sécurité	Chargé de la réponse aux incidents	Consultant(e) et auditrice/auditeur sécurité technique
Responsable du Plan de Continuité d'Activité (RPCA)	Développeuse/r sécurité			Evaluatrice/ évaluateur sécurité des systèmes et des produits
	Architecte sécurité			Cryptologue
				Expert(e) juridique en cybersécurité
				Délégué(e) à la Protection des Données (DPD)
				Formatrice/formateur en sécurité

- Dans le rapport complet de l'étude, cette liste des métiers présente également : les différentes appellations utilisées en France pour un même métier, une définition succincte de son rôle/ses activités, et le profil type en termes de formation.

2. Analyse des besoins en recrutements et en compétences

Les principaux métiers dans la Branche

- Les entreprises de la Branche se sont exprimées* sur les métiers les plus représentés au sein de leurs effectifs :

Les métiers en cybersécurité les plus présent au sein des entreprises de la Branche*

- En France, la plupart des entreprises met en exergue le manque de ressources et compétences dans le domaine de la cybersécurité : seulement 25% des besoins en recrutement dans le secteur sont couvert en 2015**.
- Les métiers de la cybersécurité sont nombreux et répondent à des besoins de compétences diverses. Cependant, les besoins en recrutement se concentrent sur une poignée de métiers. Les entreprises de la Branche* ont exprimé leur volonté actuelle de recruter des professionnels en cybersécurité :

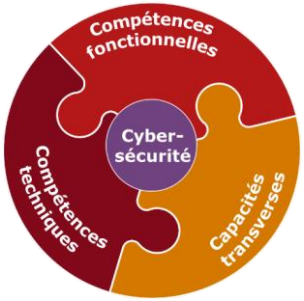
« Top 5 » des métiers que les entreprises de la branche recrutent actuellement*

** Source : enquête en ligne EY menée auprès des entreprises sur leurs effectifs et leurs besoins en cybersécurité*

*** Estimation ANSSI, Les Echos.fr, janvier 2016 « Cybersécurité : recherche candidats désespérément »*

2. Analyse des besoins en recrutements et en compétences

Cartographie des compétences en cybersécurité



- 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.

Compétences fonctionnelles
Analyse et cartographie des risques (EBIOS, MEHARI, ISO 27005, etc)
Normes de sécurité (ISO 2700x)
Elaboration des politiques et des procédures de sécurité
Gestion des incidents de sécurité (cyber crise)
Gestion du plan de continuité et de reprise d'activité
Sensibilisation et formation aux enjeux de la sécurité
Veille sur les évolutions règlementaires (LPM, NIS, RGS…)
Protection de la vie privée (data privacy)
Classification et protection des informations

Compétences techniques
Architecture de Sécurité (sondes, IDS, IPS…)
Sécurité des réseaux et des télécommunications
Sécurité des systèmes d'exploitation
Sécurité des applications
Cryptographie
Détection, réponse à incident de sécurité
Gestion des accès et des identités
Audit de sécurité (technique et organisationnel)
Tests d'intrusion
Sécurité liée aux nouveaux usages

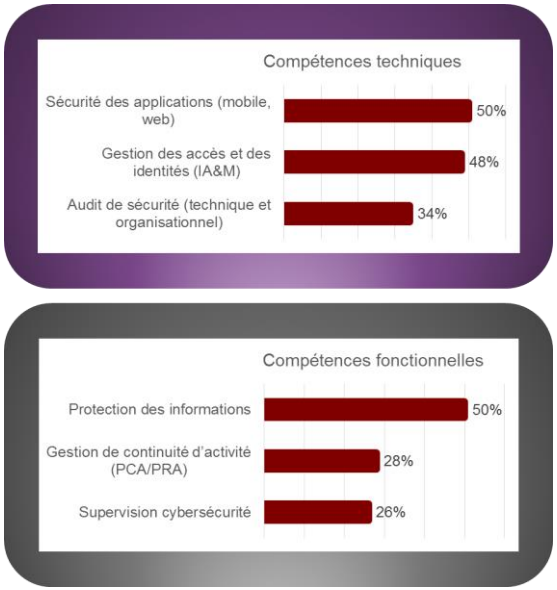
Capacités transverses	
Leadership et esprit d'entreprise	Rigueur et organisation
Adaptabilité et flexibilité	Sens relationnel
Analyse et synthèse	Travail en équipe et animation d'équipe
Communication orale et écrite	Anglais en contexte professionnel
Conviction et influence	Capacité d'écoute
Créativité et sens de l'innovation	Gestion du stress et des imprévus
Gestion de projet	Respect des règles de confidentialité
Gestion de la performance	Capacité d'anticipation
Orientation client	Curiosité intellectuelle / ouverture à d'autres environnements

- Le rapport complet précise par compétence la définition et les principaux métiers concernés.
  La matrice des métiers et des compétences est donnée en annexe du rapport.

2. Analyse des besoins en recrutements et en compétences

Principales compétences en cybersécurité recherchées par les entreprises de la Branche

- 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 compétences techniques et fonctionnelles attendues

- 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 capacités transversales recherchées par les entreprises de la Branche pour les professionnels de cybersécurité

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

Sommaire

1. Rappel des objectifs de l'étude et des moyens
2. Analyse des besoins en recrutements et en compétences
3. Etat des lieux de l'offre de formation
4. Préconisations et plan d'actions

3. Etat des lieux de l'offre de formation

Formations dispensées par les établissements d'enseignement supérieurs

Périmètre retenu pour l'offre de formation

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

Les niveaux de formation cartographiés

- 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.

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

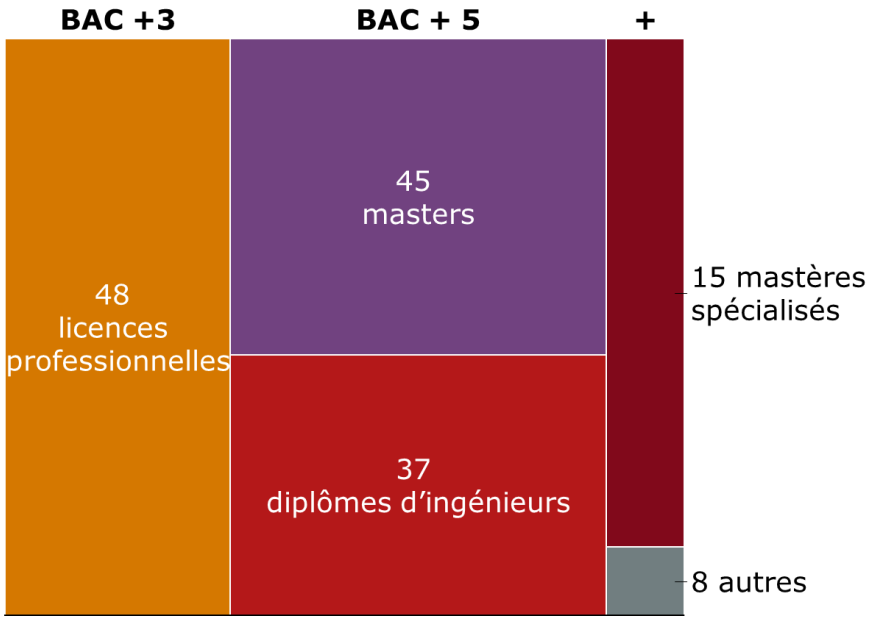
- L'ANSSI a réalisé un premier référencement (non exhaustif) des formations délivrant un titre reconnu par l'Etat de niveau équivalent à Bac+3 jusqu'à Bac+5, faisant état de 69 formations initiales : 24 licences professionnelles et 45 formations de niveau Bac+5.
- En 2016, l'ANSSI a souhaité améliorer le référencement des formations en sécurité du numérique par la mise en place d'un processus de labélisation 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, 26 formations. D'autres dossiers sont en cours d'instruction : des labélisations supplémentaires sont à prévoir.
- 26 formations ont été labélisées SecNumEdu:
  - ✓ 8 licences professionnelles
  - ✓ 7 masters
  - ✓ 6 formations d'ingénieur
  - ✓ 5 mastères spécialisés

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/
Le référentiel de labélisation SecNumEdu est disponible à l'adresse suivante :
https://www.ssi.gouv.fr/entreprise/formations/secnumedu/

3. Etat des lieux de l'offre de formation

Formations dispensées par les établissements d'enseignement supérieur

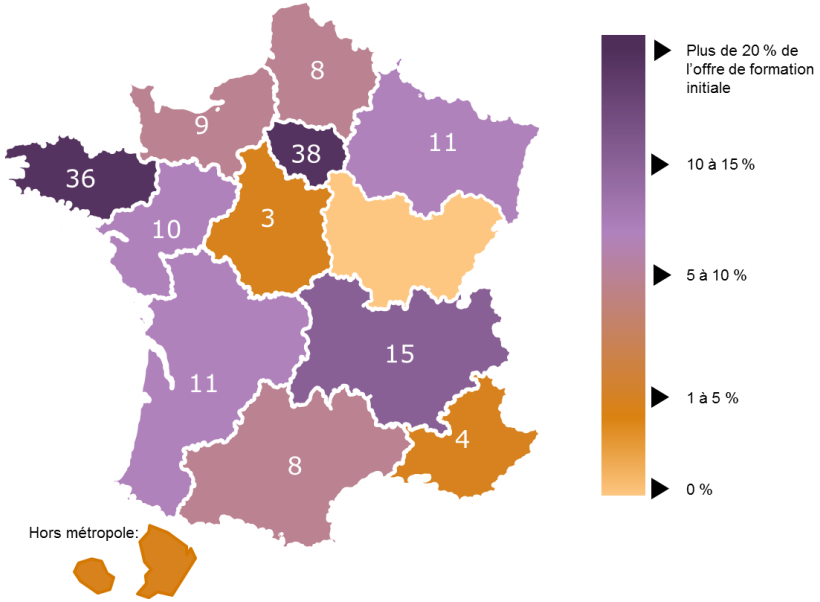
- Cette liste fait état de près de 150 formations aboutissant à des diplômes délivrés au niveau Bac+3 et Bac+5.



Répartition des formations longues en cybersécurité

- La liste des formations est placée en annexe du rapport complet avec : le nom de l'organisme, l'intitulé de la formation, le type de formation (master, licence professionnel…), la localisation, l'accès par la formation initiale/formation continue/VAE, l'enregistrement au RNCP, la labélisation SecNumEdu.

- 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%.



Répartition géographique des formations en cybersécurité

3. Etat des lieux de l'offre de formation

Formations dispensées par les établissements d'enseignement supérieur

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 et des formations nouvellement créées.
- Plus de 40% des formations sont accessibles pour la formation continue (64 formations enregistrées au RNCP).

Un taux de remplissage moyen de 83% des formations*

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

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

- 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.

** Source: Formations labélisées SecNumEdu*

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 (50%) et conseil, audit et expertise en sécurité (56%)
- Les formations de niveau master permettent aux étudiants de s'orienter vers des métiers de la famille du conseil, audit et expertise en sécurité (92%) et la famille de pilotage, organisation de la sécurité et gestion des données (58%)
- 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 (100%) ; conseil, audit et expertise en sécurité (92%) ; et pilotage, organisation de la sécurité et gestion des risques (56%)
- 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 : 56% des licences professionnelles proposent des cursus permettant une orientation dans les métiers du conseil, de l'audit et de l'expertise en sécurité. Information collectée sur 44 formations, Principalement sur la labélisation SecNumEdu et pour les formations inscrites au RNCP de la CNCP.

3. Etat des lieux de l'offre de formation

Formations courtes 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.

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 recensés en annexe du rapport complet). 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 ».
- 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.
- 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 formations généralistes

- De plus, des organismes de formation généralistes, avec des catalogues de formation très larges, proposent des formations dédiées en cybersécurité (6 organismes recensés en annexe du rapport complet).
- Ces formations répondent souvent à des problématiques plus transverses, mais ces organismes peuvent également dispenser des formations techniques en cybersécurité.

3. Etat des lieux de l'offre de formation

Formations courtes dispensées par des organismes de formation continue

Volume horaire des formations continues

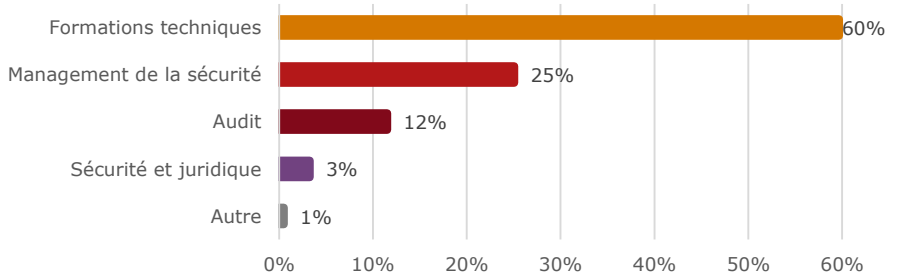
- A travers ces différents organismes, plus de 400 formations continues ont pu être recensées. Elles correspondent principalement à des formations de moins de 5 jours, parfois dispensées en plusieurs sessions en Ile-de-France et en province. Les formations «courtes»* présentent en moyenne un contenu pédagogique enseigné sur 24 heures de cours, soit 3,5 jours.

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.
- 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 (niveau de technicité).

Thématiques des formations courtes

- 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.



Principale thématique des formations identifiées**

- 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…).

** Source: Information collectée en ligne sur les catalogues de formation des organismes, pour 98 formations, entre janvier et février 2017.*

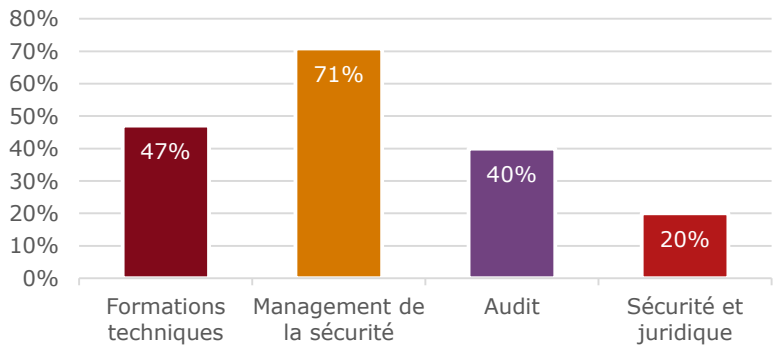
*** Source: Information collectée en ligne sur les catalogues de formation, pour 405 formations.*

3. Etat des lieux de l'offre de formation

Formations courtes dispensées par des organismes de formation continue

Certifications

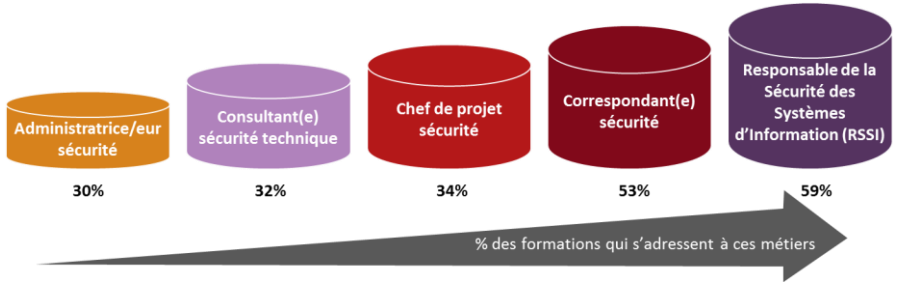
- Les certifications internationales sont fortement demandées par les professionnels de la cybersécurité. Ces formations certifiantes représentent une part importante du marché des formations continues courtes.
- Ces certifications sont parfois requises pour l'exercice de certains métiers en cybersécurité, principalement pour les métiers de la 1ère famille de métiers (pilotage, organisation de la sécurité et gestion des risques) : CISSP, CISM, ISO 27001…



Part des formations certifiantes par catégorie de formations continues*

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. 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 plus pointues.



« Top 5 » des métiers concernés par le plus grand nombre de formation*

- 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.

** Source: Information collectée en ligne sur les catalogues de formation des organismes, pour 98 formations, entre janvier et février 2017.*

3. Etat des lieux de l'offre de formation

Autres initiatives et modes d'enseignement 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

- Le Centre de Formation à la Sécurité des Systèmes d'Information (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.

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

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

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.
  - La nuit du hack, initiée dès 2003, inspirée par la Defcon de Las Vegas
  - Bounty Factory, a rassemblé plus de 1800 participants en 2016.

Sommaire

1. Rappel des objectifs de l'étude et des moyens
2. Analyse des besoins en recrutements et en compétences
3. Etat des lieux de l'offre de formation
4. Préconisations et plan d'actions

4. Préconisations et plan d'actions

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) sont assez nombreux pour répondre aux demandes des entreprises en termes de professionnels débutant. La problématique principale ne se situe pas dans un nombre de places ou de formations (initiale ou continue) insuffisant, mais dans l'attractivité des formations et de la filière plus globalement.

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'ajustements
  - Très bonne adéquation

4. Préconisations et plan d'actions

- 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.

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

4. Préconisations et plan d'actions

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

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.

- **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.

Modalités de mise en œuvre :

5 actions composent ces axes de travail. Ci-dessous le détail de 2 actions :

Action 1A	Constituer un collectif « France Cybersécurité » qui se définit comme 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 ?
Bénéficiaires	Collégiens Lycéens Etudiants

Action 1E	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
Bénéficiaires	Lycéens Etudiants

La liste complète et détaillée des actions est présentée dans le rapport de l'étude.

4. Préconisations et plan d'actions

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

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 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. 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, 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.

Modalités de mise en oeuvre:

7 actions composent ces axes de travail. Ci-dessous le détail d'une action:

Action 2B	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
Bénéficiaires	Lycéens Etudiants

La liste complète et détaillée des actions est présentée dans le rapport de l'étude.

4. Préconisations et plan d'actions

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

Constats:

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

Les réglementations liées à la cybersécurité amènent les entreprises et les acteurs publics à se structurer pour protéger leur patrimoine informationnel. Les métiers et les compétences en cybersécurité sont également impactés par la mise en œuvre de ces réglementations et le développement des outils/plateformes numériques. Le besoin en compétences pour ces nouveaux usages est important, allant des compétences techniques aux compétences fonctionnelles et transverses.

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

La cartographie des formations 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. 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 ? Quelles certifications ? …

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

Les entreprises ont des besoins de recrutement et 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.

- **Une sensibilisation encore insuffisante des DRH et des dirigeants d'entreprises**

Les entreprises subissent 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.

Modalité de mise en œuvre:

8 actions composent ces axes de travail. Ci-dessous le détail de 2 actions:

Action 3A	Créer des Actions Collectives Nationales (ACN) sur la cybersécurité. Par exemple, deux axes pour lancer les ACN pourraient être privilégiés : 1. Créer des parcours pour les professionnels de la cybersécurité: 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) 2. Proposer des parcours de formation continue pour des professionnels de l'informatique vers la cybersécurité
Bénéficiaires	Professionnels de la cybersécurité Professionnels en informatique (hors cybersécurité)

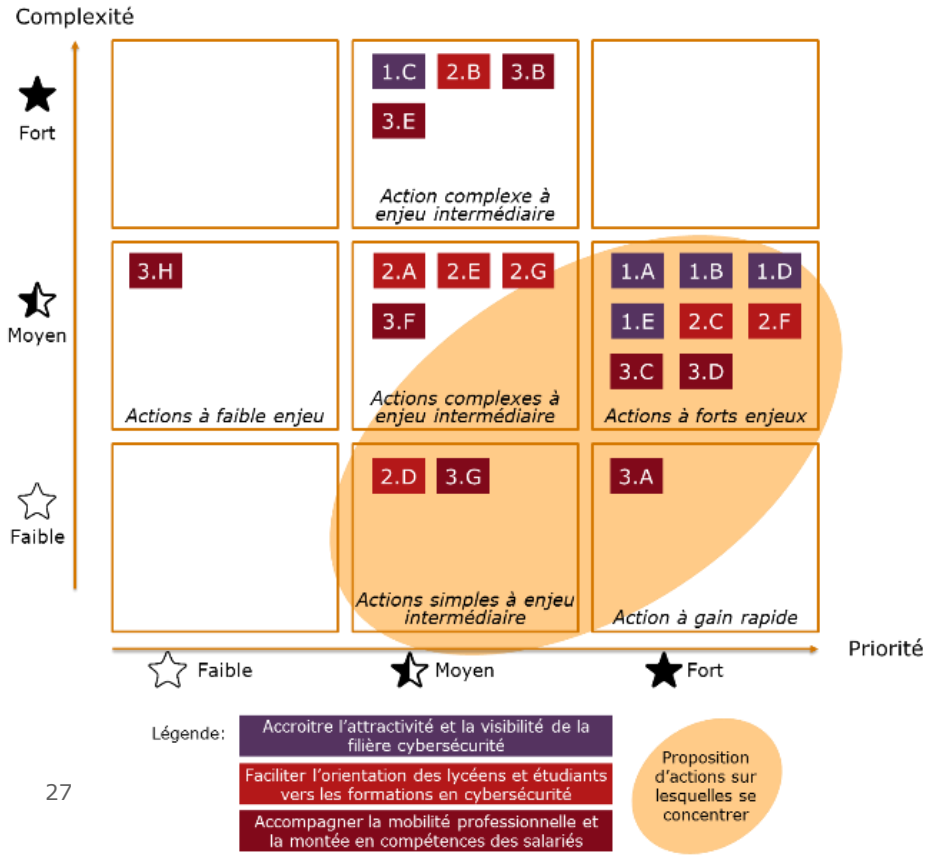
Action 3 F	Encourager les entreprises à former en sécurité les salariés exerçant d'autres fonctions que la cybersécurité (Informatique, Juridique, Achats…)
Bénéficiaires	Les salariés via les DRH d'entreprises

La liste complète et détaillée des actions est présentée dans le rapport de l'étude.

4. Préconisations et plan d'actions

Synthèse du plan d'actions

Les recommandations se composent de 20 actions. Chacune d'elles ont été classées 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…).



#	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

Pour toute demande d'information veuillez contacter:

Monica OKHKIAN

Chef de projets

Mail: opiiec@opiiec.fr

Observatoire paritaire
Numérique
Ingénierie
Etudes et Conseil
Métiers de l'évènement
OPIIEC
PROSPECTIVE MÉTIERS