

Présentation

- <**julien.breyault@cyberedu.fr**>
- **Enseignant en cyberdéfense**
et responsable de la formation continue cyber
à l'école d'ingénieurs  **ensibs:**
Université Bretagne Sud
- **Conseiller pédagogique** : spécialisation dans la gestion des compétences, la FTLV (FC, FA, VAE, VAPP...) et l'enseignement à distance
- **Vice-président** de  **CyberEdu**
La sécurité par l'enseignement supérieur des NTIC

ANSSI/Talents du numérique, FIC 2019: constat

"L'enjeu formation est décisif dans un domaine en croissance à 17%, avec des objets connectés qui se multiplient et des recrutements difficiles"

- Ces dernière années **en France** :
 - une hausse des effectifs de 6%/an
 - 1 400 créations nettes d'emplois/an
(dans un domaine qui en compte déjà 24 000, dont 7/10 en IDF)
 - **Seulement 1/4 des postes pourvus**
 - plusieurs dizaines de milliers d'emplois dans les prochaines années.

<https://talentsdunumerique.com/communiqués-presse/competences-et-cybersecurite-2019>

ANSSI/Talents du numérique, FIC 2019 + OPIIEC/EY : compétences

<https://www.fafiec.fr/85-l-observatoire-opiiec/etudes-transversales/459-formations-competences-france-cybersecurite.html>
<https://www.ssi.gouv.fr/administration/formations/panorama-des-metiers-de-la-cybersecurite/>

- **Compétences techniques :**

- sécurisation des applications,
- gestion des accès et des identités / protection des informations
- audit de sécurité / supervision/ gestion de la continuité d'activité
- infrastructure et réseaux
- programmation et cryptographie,

- **Les compétences transversales (« softskills ») jouent également un rôle important :**

- adaptabilité/flexibilité et réactivité,
- respect des règles de confidentialité,
- curiosité (veille),
- capacité d'analyse, d'anticipation,
- communication orale/écrite fluide,
- pratique de l'anglais (pro.),
- culture générale en matière de géopolitique et d'intelligence économique,
- maîtrise des enjeux juridiques (non limités au RGPD) – une matière dans laquelle des lacunes sont souvent identifiées chez les étudiants.

ANSSI/Talents du numérique, FIC 2019 + OPIIEC: évolutions

- **Intégrer le sujet « cybersécurité »** à tous les cursus supérieurs, même généralistes
- **Accompagner la mobilité professionnelle et la montée en compétences des salariés**

La commission recommande aux établissements de formation de s'intéresser

- au programme **CyberÉdu** (pour les étudiants du numérique **non spécialistes**) et à la labellisation pour les responsables de formation,
- et de demander le label **SecNumedu** (pour les formations de **spécialistes**)

- **Une alerte néanmoins : le secteur souffre d'un déficit d'attractivité...**
Des actions de communication d'envergure, notamment vers les jeunes et le grand public, sont indispensables.

Trop souvent **réduite à son aspect technique, la cybersécurité ne séduit pas.**

- **Catégorie 1 : Hygiène numérique**
 - BTS, IUT, licences ou diplômes d'informatique non spécialisés en cybersécurité,
 - personnels des administrations et des entreprises,
 - plus largement tous ceux qui utilisent des moyens numériques dans leur emploi.
- **Catégorie 2 : Formation complémentaire**
 - Personnels des systèmes d'informations et des communications,
 - pour acquérir ou de mettre à jour des connaissances et compétences nécessaires à leurs métiers.
- **Catégorie 3 : Formation à la cybersécurité**
 - Formations pour les spécialistes des systèmes d'information à la cyber-protection, à la cyberdéfense et à la cyber-résilience .
- **Catégorie 4 : Experts techniques**
 - ... et responsables spécialisés de haut niveau dans les disciplines de pointe, telles par exemple la cryptologie, le forensic (investigation numérique) ou le pentest (test d'intrusion),...
 - pouvant aller jusqu'à des certifications.
- **Catégorie 5 : Conduite des opérations cyber**
 - Formations pratiques, pour des généralistes de la conduite des opérations « cyber »
 - pouvant aller jusqu'à la gestion des crises : le Mastère spécialisé Gestion des crises cyber que propose Saint-Cyr Coëtquidan, ou le diplôme d'ingénieur Cyberdéfense de l'ENSIBS par exemple.

- **Bac+2: Des techniciens supérieurs**
 - DUT Informatique ou réseaux et télécoms
 - BTS SIO (systèmes d'information des organisations) avec spécialités systèmes et réseau ou développementEt aussi:
 - BTS SN (systèmes numériques)
- **Bac+3: Le meilleur compromis niveau d'études/capacité d'insertion professionnelle**
 - Les LP apportent une plus-value professionnelle aux bac+2
 - Métiers de l'informatique : administration et sécurité des systèmes (et/ou réseaux), développement sécurisé,...
- **Pour missions de :**
 - management de projet : chef de projet, architecte de sécurité (bac +3 à +5) , développeur sécurité (bac +2 à +3)
 - maintien de la sécurité du système et du réseau : administrateur sécurité , technicien sécurité (bac +2 à +3)
 - support et gestion des incidents de sécurité : veilleur-analyste (bac +2 à +3)

<https://www.ssi.gouv.fr/entreprise/formations/secnumedu/>

- Formation initiale/en alternance:

- Licences pro ou Master pro (+3à+5)

<http://www.enseignementsup-recherche.gouv.fr/cid20181/la-licence-professionnelle.html>

<https://www.trouvermonmaster.gouv.fr/>

- Écoles d'ingénieurs (+5, recrutent à +2):

<http://www.cti-commission.fr/>

- Mastères spécialisés (+6): <http://www.cge.asso.fr/>

- Formation continue:

<https://www.ssi.gouv.fr/entreprise/formations/secnumedu-fc-labellisation-de-formatio ns-continues-en-cybersecurite/>

Et les qualification pro: <http://www.cncp.gouv.fr/>

...type DU pour non informaticiens: DU Droit de l'informatique par ex

- Pour profils plus généralistes en charge :
 - des relations internationales,
 - de la communication,
 - des questions juridiques,
 - ou encore des relations avec les industriels et les partenaires régionaux.
- Des juristes, par exemple, peuvent être formés et poursuivre de belles carrières dans la sécurité du numérique.
- Les RSSI sont pour une bonne partie des généralistes (et dépendent de la direction et non pas de la DSI)

- **Sécurité organisationnelle :**
 - CISSP, ISSAP, ISSEP, ISSMP (1/3 des pros de la sécu),
 - CCSP, CSSLP, SSCP,
 - ISO 27001, 27002, 27005,...
 - EBIOS-RM,
 - CISA, CISM, CRISK, CGEIT (ISACA ou AFAI),...
- **Sécurité technique :**
 - CISCO (CCNA sécu/cyberops, CCNP, SCYBER), Amazon, Huawei, Palo Alto, Microsoft,...
 - CEH (ou CNDA),
 - OWASP,
 - CISM, CIW, CompTIA Security+, GIAC,...
- **Processus souvent demandé :**
 - Passage examen, obtention d'attestation de réussite,
 - Envoi d'un dossier démontrant l'expérience acquise (2 à 5 ans d'expérience)
 - Engagement sur le respect d'un code de conduite,
 - Obtention du certificat
- *Les « formations aux examens » sont souvent nécessaires pour comprendre ce qui est demandé, le format des questions, types de réponses attendues... et la densité de questions (parfois 200 QCM en 3h!)*

Catégories de missions/métiers, ANSSI 2020/OPIIEC 2019

- **Pilotage, organisation et gestion des risques**
RSSI (PSSI), correspondant.e, responsable PCA
- **Conception de SI sécurisés**
architecte, directrice/eur, chef.fe de projet, dev.
- **Maintien en conditions de sécurité**
administratrice/eur, technicien.ne
- **Gestion des incidents et des crises**
analyste SOC, chargé.e réponse incidents
- **Conseil/formation, audit et expertise**
auditrice/eur, consultant.e, expert.e juridique, DPD, formatrice/eur

Métiers les plus recherchés, OPIIEC

<https://www.fafiec.fr/85-l-observatoire-opiiec/etudes-transversales/459-formations-competences-france-cybersecurite.html>

- consultant en cybersécurité,
- analyste/veilleur SOC (Security Operations Center)
- chef de projet sécurité,
- architecte sécurité
- administrateur sécurité

<https://www.cyberjobs.fr>



Responsable de la sécurité des systèmes d'information (RSSI)

< 100 offres

Administrateur systèmes et réseaux

> 500 offres

Ingénieur en cybersécurité

< 100 offres



(Source : Jobijoba)

PEC, offres et partenaires



20% offres autour le la bretagne (DGA, Thales, Airbus, Orange,...)

- ministère des Armées et la Région Bretagne,
- douze grands groupes (Airbus Cyber Security, Atos-Bull, Bertin IT, Capgemini, DCI, EDF, La Poste, Naval Group, Nokia, Orange, Sopra Steria, Thales),
- des PME et plus d'une quinzaine de laboratoires, d'universités et d'écoles d'ingénieurs.

- +1000 recrutements/an en ce moment
- Jeunes diplômés, connectés, "geeks", ingénieurs en traitement du signal, experts du nucléaire ou de la balistique, cryptomathématiciens, linguistes maîtrisant des langues orientales ou rares telles que le persan ou le coréen...
- charte déontologique classée "secret-défense" portant comme acronyme LEDA pour " loyauté, exigence, discrétion, adaptabilité"
- affectation à l'étranger, après une cinquantaine de semaines de formation sur 5 à 6ans (enquêtes de sécurité et évaluations psychologiques tous les cinq ans).
- CDD de 1 à 3 ans (renouvelable pour une durée maximale de 6 ans au total, puis CDI) ; délai de recrutement d'environ 5 mois (le temps de passer tous les tests de sélection).
- rémunérés entre 33 000 et 35 000 euros bruts, suite à évaluations psychologiques, relationnelles, de furtivité...

Réserve opérationnelle cyber

<https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/la-reserve-de-cyberdefense>

- jusqu'à 30 jours par an
 - être de nationalité française,
 - âgé d'au moins 17 ans,
 - avoir satisfait aux obligations du service national,
 - avoir suivi la journée d'appel de préparation à la défense (JADP) ou la journée défense et citoyenneté (JDC),
 - avoir une bonne condition physique,
 - être apte moralement et psychologiquement
 - être détenteur du diplôme de gendarme adjoint de réserve (DGAR) obtenu à l'issue d'une préparation militaire encadrée par la gendarmerie.
- Chaque période d'activité fait l'objet d'une convocation qui ouvre droit à une rémunération journalière et, éventuellement, à des indemnités de déplacement et d'alimentation.

L'ANSSI recrute



- L'ANSSI comptait :
 - 120 ETP en 2009,
 - 500 en 2015,
 - 600 en 2018.
- a recruté plus de 140 personnes en 2017
- et prévoyait "un nombre d'embauches également « très significatif » pour 2018 et 2019 :
 - des ingénieurs en détection d'intrusion,
 - des ingénieurs réseau,
 - des administrateurs de réseau, des télécoms
 - et des analystes informatiques.

- Administration, système et réseau
- Architecture
- Audit
- Certification, labellisation
- Coordination et gestion de projets
- Détection
- Développement, Intégration et Test
- Expertise technique SSI
- Management
- Règlementation
- Réponses techniques aux attaques informatiques
- Support, autres
- Veille et analyse technique de la menace

<https://www.ssi.gouv.fr/recrutement/>

Sources/liens

<https://talentsdunumerique.com/sites/default/files/public/2019-01-note-tdn-competences-cybersecurite.pdf>

<https://www.fafiec.fr/85-l-observatoire-opiiec/etudes-transversales/459-formations-competences-france-cybersecurite.html>

<http://cigref.hr-ingenium.com/accueil.aspx>

<https://www.imt.fr/formation/debouches-et-metiers/barometre-metiers-numerique/>

<https://business.lesechos.fr/directions-numeriques/metier-et-carriere/parcours/0301348177395-les-femmes-boudent-toujours-la-cybersecurite-319154.php>

<https://theconversation.com/les-metiers-de-la-securite-du-numerique-sont-ils-reserves-aux-hommes-100696>

<https://www.capdigital.com/notre-vision/nos-ressources/>

<http://www.onisep.fr>

<http://www.enseignementsup-recherche.gouv.fr/cid20181/la-licence-professionnelle.html>

<https://www.trouvermonmaster.gouv.fr/>

<http://www.cti-commission.fr/>

<http://www.cge.asso.fr/>

<http://www.cncp.gouv.fr/>

<https://www.ssi.gouv.fr/entreprise/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/>

<http://www.data.gouv.fr/fr/datasets/referentiel-des-metiers-et-competences-des-systemes-dinformation-et-de-communication-sic/#resource-f933e725-e031-4f7b-ab41-be6e0fb9ac1d>

<https://infos.emploipublic.fr>

<https://www.ssi.gouv.fr/recrutement/>

<https://www.cyberjobs.fr>

<https://www.ssi.gouv.fr/administration/formations/panorama-des-metiers-de-la-cybersecurite/>

<https://www.ssi.gouv.fr/entreprise/formations/secnumedu/>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>

<https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

<https://www.cyberedu.fr>