RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ONISEP

ZOOM SUR LES MÉTIERS DE LA CYBERSÉCURITÉ

www.onisep.fr / https://evolution.campuscyber.fr/

FRANCE 2030

CAMPUS CYBER

ZOOM SUR LES MÉTIERS DE LA CYBERSÉCURITÉ

Les métiers de la cybersécurité allient analyse et innovation technologique pour concevoir et mettre en œuvre des solutions de protection des systèmes d'information face à la menace croissante de cyberattaques. De l'identification des risques à la mise en place de dispositifs de sécurité, en passant par les tests d'intrusion ou la réponse aux incidents, de nombreux professionnels interviennent pour garantir la fiabilité, la conformité et la résilience des infrastructures numériques.

Les entreprises du secteur, de la PME au grand groupe, recrutent une diversité de profils en analyse SOC, en ingénierie, en contrôle et tests de systèmes de sécurité, en cryptographie, mais également dans la recherche, le commercial et le juridique appliqués à la cybersécurité.

Des métiers d'avenir, exigeants et en perpétuelle évolution, sont accessibles via des formations généralistes ou plus pointues, du bac+2 au bac+8, et offrent des rémunérations qui peuvent être très attractives.

Ce guide, réalisé en partenariat avec TAL-CYB : Talents Cyber (coordonnée par le Campus Cyber), est un outil de découverte pour les jeunes et leurs familles ainsi qu'un support pour les équipes éducatives. Il favorise l'approche et la connaissance de la cybersécurité. Il s'appuie sur la réalité du terrain et s'inscrit dans le cadre de la découverte des métiers et du parcours Avenir, qui accompagne les élèves, au collège et au lycée, dans leur exploration du monde professionnel.

Anne de Rozario,
Directrice générale de l'Onisep par intérim

Joffrey Célestin-Urbain,
Président du Campus Cyber

SOMMAIRE

CAMPUS CYBER

ONISEP

Office national d'information sur les enseignements et les professions, établissement public sous tutelle du ministère de l'Éducation nationale et du ministère de l'Enseignement supérieur, de la Recherche et de l'Espace • Publication de l'Onisep© Onisep décembre 2025, avec la collaboration de TalCyb: Talents Cyber (coordonné par le Campus Cyber); ce travail a bénéficié d'une aide de l'État gérée par l'Agence nationale de la recherche au titre de France 2030 portant la référence ANR-23-CMAS-0020 • Directrice de la publication: Anne de Rozario • **Directeur des ressources éditoriales transmédias:** Michel Maurel • **Cheffe du service éditions transmédias et responsable éditoriale:** Laurence Congy • **Rédactrice en chef:** Séverine Maestri • **Rédactrice:** Caroline Charron • **Cheffe du service secrétariat de rédaction et qualité éditoriale:** Saliha Hamzic • **Secrétaire de rédaction:** Lydie Théophin • **Correctrice:** Pauline Coullet • **Documentaliste:** Hélène Ferron • **Chef du service S/T/U/D/I/O et direction artistique:** Bruno Delobelle • **Maquette:** Cyril Lauret • **Mise en pages et illustration:** Isabelle Sénéchal • **Iconographe:** Brigitte Gilles de la Londe • **Photographe:** Alain Potignon • **Photo de couverture, copyright:** © da-kuk/E+/Getty Images • **Responsable fabrication:** Laurence Parlouer • **Photogravure:** Key Graphic (Paris) • **Imprimeur:** Dupliprint Mayenne, sur papier certifié PEFC • **Promotion, commercialisation et diffusion:** VPC – 12, mail Barthélemy-Thimonnier, CS 10450 Lognes, 77437 Marne-la-Vallée Cedex 2 • **Vente en ligne:** librairie.onisep.fr • **Relations clients:** service-clients@onisep.fr • **Code de diffusion Onisep:** 901728 • **ISSN:** 1772-2063 • **ISBN papier:** 978-2-273-01728-2 • **ISBN numérique:** 978-2-273-01727-5 • **Le kiosque:** Sciences, Technologies • **Dépôt légal:** décembre 2025 • Reproduction, même partielle, interdite sans accord préalable de l'Onisep.

10-31-1316

L'EMPLOI EN 10 POINTS

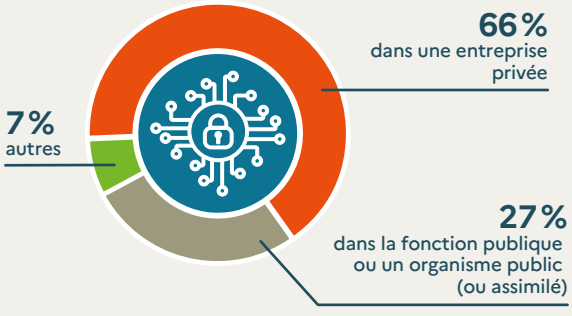
Y a-t-il des débouchés pour les jeunes ? À quels postes et avec quel niveau ? Peut-on faire carrière ? Comment évoluer ? Quels seront les métiers demain ? Des questions que vous vous posez sûrement sur le secteur de la cybersécurité. Voici les réponses en 10 points.

DE QUOI PARLE-T-ON ?

1 UN SECTEUR TRANSVERSAL

Le recours de plus en plus fréquent aux outils numériques dans l'univers professionnel, tous métiers et tous secteurs confondus, entraîne un accroissement des risques de cyberattaque, obligeant les entreprises, les administrations, l'armée, etc., à se préparer au mieux à y faire face. Cela implique le recrutement de personnes qualifiées dans le domaine de la SSI (sécurité des systèmes d'information). Ces professionnels travaillent majoritairement au sein d'entreprises privées, mais aussi dans les services publics, les sociétés de consultants ou des services spécialisés.

Répartition des professionnels par types d'entreprise

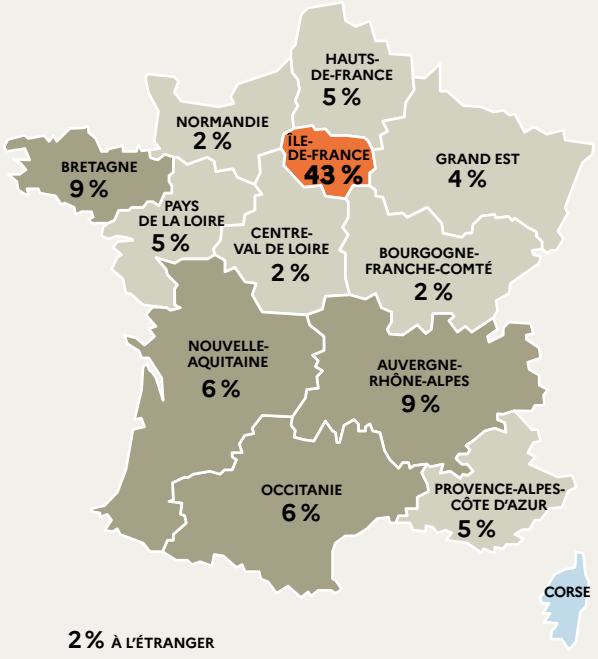


Source : Observatoire des métiers de la cybersécurité, 2025.

2 UNE RÉGION PHARE : L'ÎLE-DE-FRANCE

L'Île-de-France regroupe près de la moitié des professionnels de la cybersécurité. Néanmoins, les régions Nouvelle-Aquitaine, Auvergne-Rhône-Alpes, Bretagne et Occitanie accueillent à elles quatre près d'un tiers des salariés du secteur.

Répartition des salariés en France



Source : Observatoire des métiers de la cybersécurité, 2025.

QUELS DÉBOUCHÉS POUR LES JEUNES ?

3 DES POSTES À POURVOIR

L'utilisation accrue des outils numériques, la multiplication des cyberattaques et le renforcement des obligations des entreprises, notamment dans le domaine de la protection des données, augmentent de manière constante les besoins de professionnels qualifiés.

23 183 offres d'emploi en cybersécurité en 2024 (+ 49 % en 5 ans).

Source : Observatoire des métiers de la cybersécurité, 2025.

4 DES OPPORTUNITÉS POUR TOUS LES PROFILS

Selon le rapport 2025 de l'Observatoire des métiers de la cybersécurité, les entreprises ont autant besoin de profils à bac + 5 que de personnes moins diplômées (bac + 2 ou bac + 3) ou d'autodidactes ayant obtenu des certifications, et qui peuvent débuter rapidement avec une formation interne. Si les compétences techniques sont indispensables, les savoir-faire sont aussi importants que les savoir-être (empathie, esprit d'équipe, discrétion, sang-froid…).

34 % des offres d'emploi ne précisent pas le niveau d'études requis.

Source : Observatoire des métiers de la cybersécurité, 2025.

5 DES EMPLOIS STABLES

La plupart des emplois proposés dans la cybersécurité sont des CDI (contrats à durée indéterminée).
Les recrutements à la suite d'un stage ou d'une formation en alternance sont en importante hausse, tout comme le « marché caché » (recommandations, approches directes, candidatures spontanées, réseaux sociaux), qui représente 43 % des recrutements.

Répartition des offres d'emploi par types de contrat

* Contrat à durée indéterminée.
** Contrat à durée déterminée.

Source : Observatoire des métiers de la cybersécurité, 2025.

6 DES SALAIRES ATTRACTIFS

Les entreprises (surtout privées) offrent parfois des salaires particulièrement attractifs dans la cybersécurité.
Ils augmentent également avec l'expérience, mais il faut d'abord faire ses preuves. Le domaine d'activité, le type de structure (privée ou publique), la taille de l'entreprise, le niveau de responsabilité, la géographie ou encore le profil des candidats font aussi varier la rémunération.

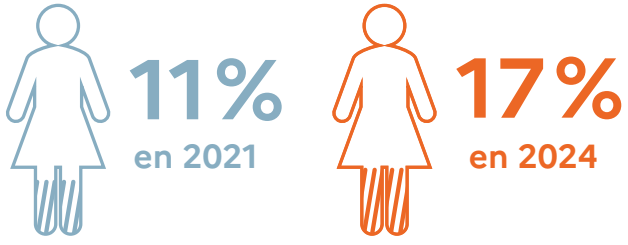
40 000 € brut par an, soit 3 300 € brut par mois, c'est le salaire moyen dans la cybersécurité.

Source : Campus Cyber Évolution, 2025.

7 DE PLUS EN PLUS DE FILLES

La féminisation du secteur est en marche. Même si elles restent largement sous-représentées, les femmes sont accueillies à bras ouverts dans la cybersécurité, sur tous les profils de poste.

Part de femmes dans le secteur



Source : Cyberscope, 2024.

COMMENT FAIRE CARRIÈRE ?

8 ÉVOLUER, C'EST POSSIBLE

« Réussir un diplôme d'université grâce à l'autoformation m'a donné confiance pour continuer à me former. »

p. 21

FADIMATOU, 44 ANS
Auditrice en cybersécurité

« Après un bac général et un DUT* en physique à Dakar, au Sénégal, je suis venue en France pour obtenir un diplôme d'ingénieur en systèmes d'information et télécommunications, à l'UTT**. »

* Diplôme universitaire de technologie, de niveau bac+2, devenu une certification intermédiaire du BUT (bachelor universitaire de technologie), de niveau bac+3.
** Université de technologie de Troyes.

« J'ai commencé à travailler dans une entreprise de services en tant que consultante qualification et normalisation. Puis j'ai intégré le groupe Covéa* pour piloter des tests de sécurité applicative. »

* Regroupant Maaf, MMA et GMF.

« Après quelques années, j'ai décidé de me former dans le domaine de la cybersécurité. J'ai suivi un MOOC* qui m'a permis de passer un DU** de data analyst. »

* *Massive Open Online Course,* ou cours en ligne.
** Diplôme d'université.

« Cette étape m'a donné envie d'aller plus loin. J'ai utilisé mon congé formation pour commencer un MS* expert en cybersécurité en cours du soir. »

* Mastère spécialisé.

« Après mon diplôme, l'entreprise a été réorganisée, et on m'a proposé un poste d'auditrice à la direction cybersécurité. »

ET LES MÉTIERS DEMAIN ?

9 L'IA FAIT BOUGER LES LIGNES

L'IA (intelligence artificielle) est de plus en plus utilisée pour détecter les menaces de sécurité en analysant des données. Elle optimise et automatise certaines actions et libère les professionnels, toujours pressés par le temps, de tâches parfois répétitives et chronophages. Mais l'IA fait aussi peser de nouvelles menaces sur les entreprises et institutions.
Les spécialistes du domaine sont donc recherchés pour sécuriser les outils qui l'intègrent et pour vérifier qu'elle ne crée pas de nouvelles failles de sécurité.

21,9 % par an, c'est la croissance estimée de l'IA dans la cybersécurité en France entre 2024 et 2030.

Source : Portail de l'IE (intelligence économique), 2025.

10 LA CRYPTOGRAPHIE POUR SÉCURISER DES DONNÉES

Les architectures classiques doivent être revisitées pour garantir la sécurité des données où qu'elles soient, notamment dans le *cloud*. Parmi les pistes explorées : le chiffrement homomorphique, qui permet de traiter des données en les laissant cryptées.

4 386 événements de sécurité ont été traités en 2024 (+15 % par rapport à 2023), dont

1 361 incidents* (+18 % par rapport à 2023).

* Événements de sécurité identifiés comme provenant d'un acteur malveillant ayant conduit des actions avec succès sur le SI (système d'information) de la victime.

Source : Panorama de la cybermenace 2024, Anssi (Agence nationale de la sécurité des systèmes d'information), 2025.

PORTRAITS DE **PROS**

GESTION DE LA SÉCURITÉ ET PILOTAGE DES PROJETS DE SÉCURITÉ

CONCEPTION ET MAINTIEN D'UN SYSTÈME D'INFORMATION SÉCURISÉ

GESTION DES INCIDENTS ET DES CRISES DE SÉCURITÉ

CONSEIL, SERVICE ET RECHERCHE

MÉTIERS CONNEXES

MON PARCOURS

Après un bac général, j'ai commencé à travailler, tout en suivant, en formation continue, un BTS, une licence et un master. Consultante dans les ressources humaines pendant quelques années, j'ai préparé, toujours grâce à la formation continue, un double diplôme en systèmes d'information et j'ai passé des certifications professionnelles. Puis j'ai participé à la création de la cellule cybersécurité de la filiale informatique du groupe des Eaux de Marseille, avant d'en prendre la direction. J'ai enfin rejoint une entreprise de transport maritime comme BISO (business information security officer). Aujourd'hui, je suis indépendante.

Aude Folcher, 38 ans
RSSI (RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION), INDÉPENDANTE, À MARSEILLE (13)

Mission après mission, Aude accompagne les entreprises ou les administrations dans leur stratégie de cybersécurité. Parallèlement, elle œuvre pour une meilleure représentation des femmes dans le secteur.

En tant qu'indépendante, je ne connais pas la routine. Chacune de mes missions de RSSI, ou « CISO » (chief information security officer), représente un nouveau défi. J'interviens pour évaluer les risques, concevoir une stratégie de cybersécurité, la mettre en œuvre, et former les équipes internes. Selon le cas, mon travail peut aller du déploiement de solutions de sécurité (chiffrement, pare-feu…) à la gestion des incidents, en passant par l'ajout de clauses de sécurité dans les contrats de sous-traitance, ou la mise en conformité avec les réglementations (NIS, LPM…). Dans tous les cas, je démarre chaque intervention par un diagnostic précis des besoins. Ensuite, je définis les priorités : sécurisation des systèmes, accompagnement au changement, rédaction de procédures d'urgence en cas de cyberattaque, sensibilisation des collaborateurs, etc. À chaque fois, je découvre des environnements techniques variés et des équipes différentes, ce qui me stimule énormément. Parallèlement à ces missions, je suis très impliquée dans la promotion de la cybersécurité au féminin. J'ai fondé le collectif les BrHackeuses, qui encourage les femmes à développer leurs compétences dans ce domaine. Je suis aussi référente du Cefcys (Cercle des femmes de la cybersécurité) pour la région Sud.

FICHE MÉTIER

RSSI (RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION)

Formation : master en cybersécurité, en informatique, en ingénierie des systèmes complexes ou en management des systèmes d'information (parcours en sécurité des systèmes informatiques), ou encore diplôme d'ingénieur avec une spécialisation en sécurité informatique, complété par 5 à 10 années d'expérience professionnelle ; MS spécialiste en cybersécurité.
Qualités : créativité, pédagogie, rigueur.

Retrouvez les déroulés des sigles des diplômes p. 29.

Xavier Leschaeve, 52 ans
DIRECTEUR DE LA CYBERSÉCURITÉ, LOUIS VUITTON, À PARIS (75)

À la tête d'une équipe dont certains membres se trouvent à l'étranger, Xavier met en place la politique de cybersécurité de Louis Vuitton. Il s'assure que les précautions sont bien respectées dans tous les services de l'entreprise. Un travail de chef d'orchestre.

Louis Vuitton maîtrise sa chaîne de production, en s'appuyant sur l'équipe technique LV_NEO que j'encadre. À chaque étape, du développement à la vente des produits, je veille à la sécurisation des serveurs et à la prise en compte de la cybersécurité dans les applications, les sites d'e-commerce, les e-mails pouvant faire l'objet d'hameçonnage, etc. À tous les stades, je peux faire intervenir des personnes de mon équipe, qui en compte 20, et que je choisis en fonction du besoin et des compétences nécessaires. Celles-ci évaluent et conseillent également les fournisseurs pour que nous ne soyons pas attaqués ou contaminés par leurs intermédiaires. Je mets aussi en place des audits, des contrôles et des tests d'intrusion pour vérifier que tout fonctionne correctement. Je sensibilise enfin nos salariés aux bonnes pratiques, via des *escape games*, des tests d'hameçonnage, etc. C'est à la fois un métier technique (pour identifier la nature des attaques), de communication (pour les expliquer à la direction) et de management (pour animer une équipe). Le but : faire comprendre les enjeux de la cybersécurité afin que les mesures soient acceptées et appliquées. Je me déplace parfois sur nos sites à l'étranger, au sein desquels j'ai des relais pour adapter les mesures aux réglementations de chaque pays.

MON PARCOURS

Mon bac général en poche, je me suis dirigé vers une école d'ingénieurs, l'IMT* Nord Europe. Une fois mon diplôme obtenu, j'ai d'abord été consultant chez Axa avant d'évoluer vers la cybersécurité. J'ai ensuite intégré le groupe Rémy Cointreau au poste de RSSI**, puis j'ai été embauché chez Louis Vuitton.

* Institut Mines Télécom.
** Responsable de la sécurité des systèmes d'information.

FICHE MÉTIER

DIRECTEUR/DIRECTRICE DE LA CYBERSÉCURITÉ

Formation : master en cybersécurité, en informatique, en ingénierie des systèmes complexes, en mathématiques et applications ou en réseaux et télécommunications (parcours sécurité des systèmes informatiques ou des systèmes d'information), ou encore diplôme d'ingénieur avec une spécialisation en sécurité informatique, complété par 10 à 15 années d'expérience professionnelle et éventuellement un MS expert en cybersécurité ou un MS spécialiste en cybersécurité. **Qualités :** pédagogie, rigueur, sens des responsabilités.

Retrouvez les déroulés des sigles des diplômes p. 29.

MON PARCOURS

J'ai obtenu un bac STI2D*, un DUT** GEII***, puis une licence et un master en systèmes de télécommunications et informatique. D'abord ingénieur sécurité dans l'aéronautique, j'ai rapidement rejoint une entreprise d'intégration de solutions en cybersécurité. J'ai ensuite travaillé pour la filiale d'un grand groupe aéronautique en tant qu'ingénieur cybersécurité produits, avant d'intégrer Collins Aerospace comme ingénieur cybersécurité, puis de diriger l'équipe cybersécurité produits.

* Sciences et technologies de l'industrie et du développement durable.
** Devenu une certification intermédiaire du BUT.
*** Génie électrique et informatique industrielle.

Mickaël Sabelle, 46 ans

RESPONSABLE DE L'ÉQUIPE CYBERSÉCURITÉ PRODUITS, COLLINS AEROSPACE, À BLAGNAC (31)

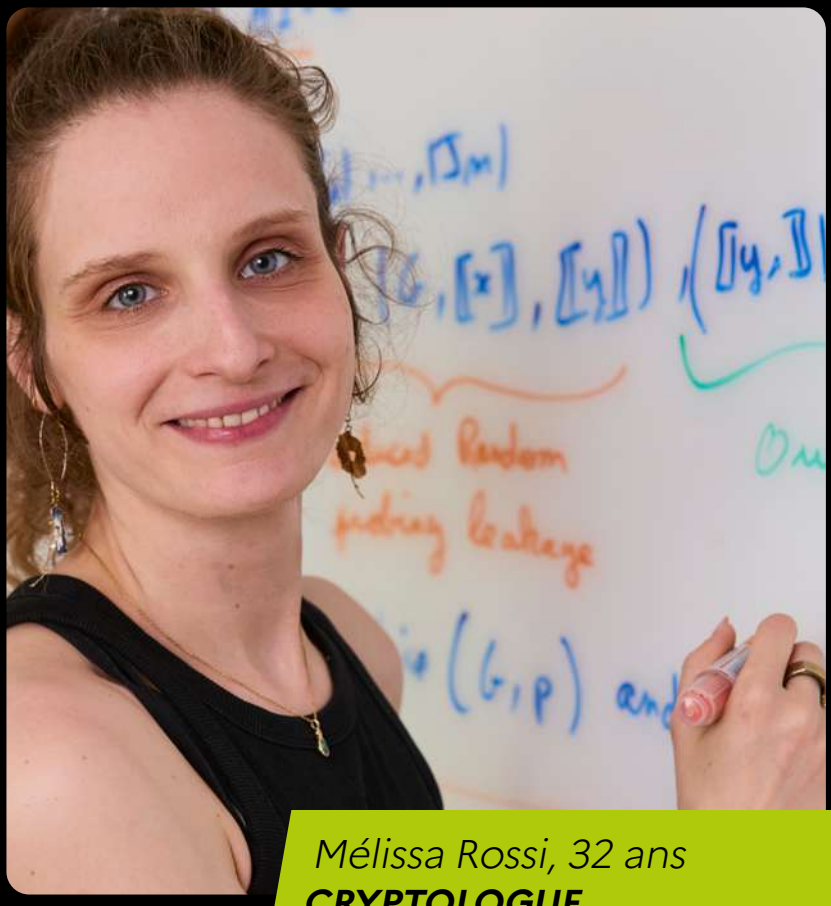
Avec son équipe, Mickaël s'assure de la sécurité des équipements d'aide à la navigation aérienne développés dans l'entreprise. Projets de recherche et veille permanente complètent ses tâches pour anticiper des cyberattaques visant les avions.

Je dirige une équipe d'ingénieurs spécialisés en systèmes, logiciels et conception d'architectures de sécurité. Nous sécurisons tout ce qui contribue à l'exploitation des avions afin qu'ils puissent voler d'un point A à un point B. Notre travail consiste à évaluer les risques de cybermenace sur les équipements embarqués (système de communication par satellite, outils d'échange de données bord/sol, GPS de l'avion, système de téléphonie…) afin d'assurer la sécurité des passagers. Nous suivons le cycle de développement de ces éléments électroniques, de leur conception à leur intégration. Nous réalisons des vérifications sur les nouveaux produits, mais aussi dès que l'un d'eux est modifié, grâce à des bancs de tests durant lesquels nous simulons toutes sortes d'attaques. Nos clients (constructeurs aériens ou compagnies aériennes) nous contactent aussi en cas de défaillance de l'un de nos systèmes. Dans ce cas, il faut investiguer pour découvrir si le problème est lié à une panne non intentionnelle ou à une cyberattaque. J'accompagne les ingénieurs dans leurs prises de décision, la résolution des difficultés techniques et les relations avec nos clients. Enfin, nous menons de nombreux projets de recherche sur les solutions techniques qui contreront les menaces de sécurité de demain.

FICHE MÉTIER

INGÉNIEUR/INGÉNIEURE EN CYBERSÉCURITÉ AÉRONAUTIQUE
Formation : master en informatique ou en ingénierie des systèmes complexes (parcours en cybersécurité des systèmes embarqués), diplôme d'ingénieur généraliste ou spécialisé en informatique (cybersécurité des systèmes embarqués) ou en aéronautique (sécurité des systèmes d'information) ; MS spécialiste en cybersécurité. **Qualités :** anticipation, créativité, rigueur.

Retrouvez les déroulés des sigles des diplômes p. 29.



Mélissa Rossi, 32 ans
CRYPTOLOGUE, CRYPTOEXPERTS, À PARIS (75)

MON PARCOURS

Après un bac général, je me suis orientée vers une classe prépa scientifique pour intégrer l'école d'ingénieurs Télécom Paris. J'ai obtenu un double diplôme en sciences de l'ingénieur et en recherche en informatique, puis j'ai préparé un doctorat à l'ENS* de Paris-Ulm en cryptographie et cryptanalyse post-quantique. J'ai ensuite été embauchée à l'Anssi** en tant qu'experte en cryptologie avant de rejoindre CryptoExperts.

* École normale supérieure.
** Agence nationale de la sécurité des systèmes d'information.

Spécialiste de la cryptologie, Mélissa collabore avec des chercheurs du monde entier pour mettre au point des systèmes de codage afin de protéger nos usages numériques. Un secteur dans lequel la France est à la pointe de la technologie.

Le petit cadenas que l'on voit en haut d'une page Internet, c'est de la cryptologie, c'est-à-dire du codage et du décodage de données secrètes. À l'aide de formules mathématiques, je sécurise ces dernières sur les téléphones, les cartes bancaires, les documents d'identité, les ordinateurs, les objets connectés ou les cryptomonnaies. Ces codes sont essentiels pour protéger nos données personnelles et je dois sans cesse les perfectionner, parce que les cyberattaques évoluent ! Ma spécialité est la cryptographie post-quantique. Avec l'arrivée potentielle d'ordinateurs quantiques sur le marché (qui permettent de résoudre des problèmes complexes), n'importe qui pourrait déverrouiller le codage qui protège la confidentialité. Avec des équipes du monde entier, nous inventons ou analysons des algorithmes pour vérifier que les codes sont déchiffrables uniquement par la personne qui en a la clé. Par exemple, certains pirates mettent les cartes bancaires dans un four à micro-ondes pour tenter de découvrir leurs données cryptées ! Nous devons être prudents afin de les protéger dans toutes les situations. Je participe à des conférences pour partager mes travaux ou établir de nouvelles collaborations. Je fais de la recherche la majorité du temps, mais me charge aussi de missions d'expertise pour des clients cherchant à se protéger des cyberattaques.

FICHE MÉTIER

CRYPTOLOGUE
Formation : master en informatique, en ingénierie des systèmes complexes ou en mathématiques et applications (parcours en cryptologie, en cryptographie et sécurité informatique…), ou encore diplôme d'ingénieur avec spécialisation en cryptographie et sécurité des systèmes informatiques, éventuellement complétés par un MS cybersécurité des infrastructures et des données ou un doctorat en cryptologie.
Qualités : anticipation, créativité, esprit logique.

Retrouvez les déroulés des sigles des diplômes p. 29.

Jean-Baptiste Gard, 42 ans
ARCHITECTE EN CYBERSÉCURITÉ, HÔPITAL DE SAINT-QUENTIN (02)

Entouré de machines, Jean-Baptiste veille à ce que le système informatique de l'hôpital dans lequel il travaille soit le plus sûr possible. Cela va de la mise en place de logiciels de sécurité, qu'il configure avec son équipe, à l'analyse d'incidents.

MON PARCOURS

J'ai obtenu un bac général et un BTS en informatique. J'ai suivi une LP en informatique et réseaux, avant d'intégrer, en 4e année, la filière systèmes, réseaux et télécommunications d'une école d'ingénieurs, pour un cursus en alternance au centre hospitalier de Saint-Quentin. J'ai ensuite été embauché par ce dernier au poste de responsable infrastructure réseaux et téléphonie, avant d'évoluer à mon poste actuel.

Le groupe hospitalier pour lequel je travaille compte 11 établissements qui traitent les données de santé des patients. Mon métier consiste à intégrer des protections dans le système informatique du groupe (antivirus, pare-feu, systèmes anti-intrusion, authentification à double facteur, etc.) pour sécuriser ces données. Cela nécessite de communiquer avec toutes les personnes qui se connectent à notre système d'information (salariés, prestataires) afin que mes actions soient comprises et appliquées. Nous achetons des solutions de protection, mais je m'occupe de configurer la partie logicielle. Si tout le monde au sein du service informatique participe à la cybersécurité, je suis chargé de définir la stratégie globale, d'analyser la menace et les risques, d'élaborer les règles de sécurité (politique d'accès, mots de passe…) et de coordonner les équipes lors de simulations d'attaques. Nous commandons également des audits réguliers pour vérifier l'absence de failles de sécurité. La cybersécurité évolue plus vite que l'informatique générale, la menace également, notamment avec l'intelligence artificielle. Je peux intervenir en cas d'attaque, et je dialogue avec mes homologues d'autres centres ou groupes hospitaliers pour partager nos expériences, nos façons de faire, etc.

FICHE MÉTIER

ARCHITECTE EN CYBERSÉCURITÉ
Formation : master en informatique, en ingénierie des systèmes complexes ou en réseaux et télécommunication (parcours en sécurité des systèmes informatiques ou des systèmes d'information, en évaluation du risque ou en cryptologie et sécurité informatique), ou encore diplôme d'ingénieur avec une spécialisation en architecture du SI (système d'information); MS expert en gouvernance de la sécurité des réseaux et des systèmes.
Qualités : esprit logique, rigueur, sens de l'analyse.

Retrouvez les déroulés des sigles des diplômes p. 29.

Stéphanie Ledoux, 41 ans
GESTIONNAIRE DE CRISE CYBER, ALCYCONIE, À SAINT-MALO (35)

Soutenue par son équipe, Stéphanie intervient auprès d'organisations touchées par une cyberattaque ou souhaitant s'y préparer. Elle les accompagne dans leurs prises de décision. Un métier de conviction, fait de tensions et porteur de sens.

J'interviens dans des secteurs dits « sensibles » (défense, télécoms, finance, transports, etc.). Dans une crise cyber, chaque minute compte. Dès les premiers signaux, je crée une cellule de crise en mobilisant une équipe d'experts (analystes géopolitiques, juristes en droit du numérique, ingénieurs en cyberdéfense…). Je coordonne le travail de ces différents intervenants, j'alerte les autorités et je veille à la sécurisation de la communication interne et externe. Les dirigeants que nous accompagnons sont souvent sous le choc et les décisions peuvent parfois être difficiles à prendre lorsque s'impose, par exemple, la coupure de l'accès à un système ou la déclaration d'une fuite de données. Il faut les aider à choisir les bons mots pour rassurer leurs salariés, leurs clients clés, leurs fournisseurs, etc. Mais notre force se construit avant la tempête, en préparant des plans de gestion de crise. Cela passe par la structuration de cellules de crise, la définition de processus décisionnels, la rédaction de premiers messages, et la réalisation de simulations grandeur nature. Un véritable travail d'équipe, dans lequel je me sens utile.

MON PARCOURS

Après un bac général et un double bachelor franco-allemand en marketing et finance, j'ai suivi un MSc* en communication, en alternance. J'ai travaillé pour le secteur du transport ferroviaire et aéronautique avant de diriger la communication du groupe Roullier (spécialiste de la nutrition végétale et animale). J'y ai découvert les enjeux de la gestion de crise. J'ai alors passé, en formation continue, un MBA** en cybersécurité, dans le but de créer ma propre entreprise, Alcyconie, qui est née en 2018.

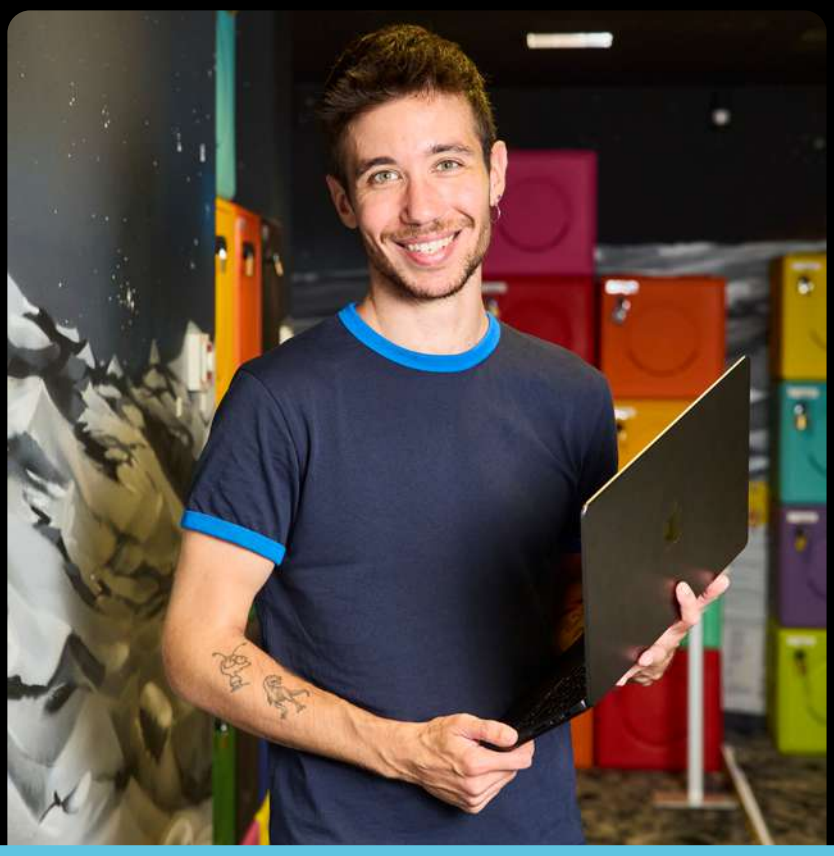
* Master of Science.
** Master of Business Administration.

FICHE MÉTIER

GESTIONNAIRE DE CRISE CYBER

Formation : master en informatique, en ingénierie des systèmes complexes ou en mathématiques et applications (parcours en sécurité des systèmes informatiques, en cryptologie…), ou encore diplôme d'ingénieur ou diplôme d'école d'informatique intégrant une spécialisation en sécurité informatique. **Qualités :** empathie, réactivité, sens des responsabilités.

Retrouvez les déroulés des sigles des diplômes p. 29.



Archibald Thirion, 32 ans

ANALYSTE SOC (SECURITY OPERATION CENTER), *CHEZ SCALEWAY, À PARIS (75)*

Garant de la sécurité informatique d'un fournisseur de *cloud*, Archibald anticipe les cybermenaces. Il traque les tentatives d'attaques, les failles et les vulnérabilités, mais sensibilise également ses collègues sur les risques cyber.

MON PARCOURS

Après un bac général, j'ai suivi un double cursus ingénieur civil et architecte sans le terminer, car j'ai préféré me réorienter vers une licence en design de mode. Après avoir fait plusieurs créations, candidaté à divers concours de mode et travaillé quelque temps dans le cinéma, j'ai choisi de changer de voie une seconde fois. Durant la crise sanitaire de 2019, je me suis beaucoup intéressé à l'informatique, et j'ai alors décidé de m'inscrire à l'école 42, puis j'ai rapidement été embauché par Scaleway.

Je travaille pour un fournisseur de *cloud* européen comptant plus de 600 employés en France. Les attaques peuvent donc se produire n'importe quand et, surtout, venir de n'importe où. Mon métier consiste, entre autres, à chercher des traces qui auraient été laissées par des cybercriminels. Pour ce faire, j'analyse les comportements anormaux au sein du réseau informatique de l'entreprise, et je fais en sorte de bloquer les intrusions avant qu'elles ne se produisent. Nous avons à notre disposition des outils avancés qui scannent notre infrastructure en temps réel, et lorsque je reçois une alerte via ces dispositifs, je dois rapidement déterminer s'il s'agit d'une menace effective ou d'un « faux positif » (fausse alerte). Je réfléchis également aux vulnérabilités qui peuvent exister et mets en place des procédures préventives pour faire face à d'éventuels cybercriminels, qui perfectionnent sans cesse leurs techniques. Cela exige de réaliser une veille constante sur les méthodes d'attaque les plus récentes et de se former continuellement pour savoir s'adapter en permanence. Mon travail passe aussi par la communication, afin de sensibiliser mes collègues aux bonnes pratiques, par exemple face au *phishing* (ou « hameçonnage ») ou à la gestion des mots de passe.

FICHE MÉTIER

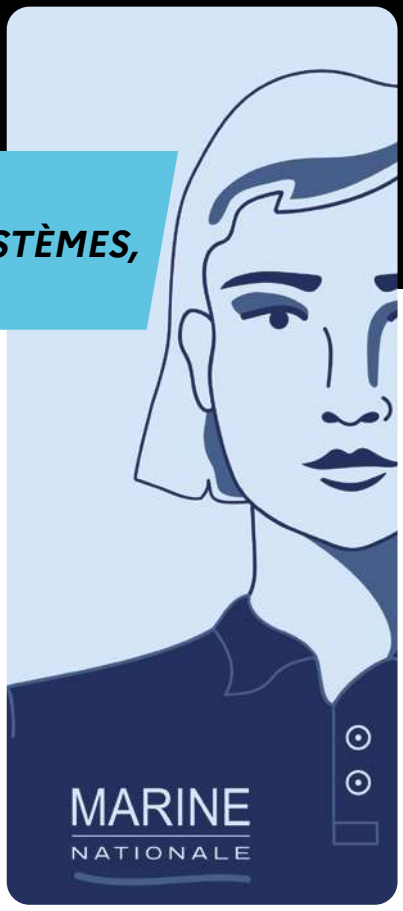
ANALYSTE SOC *(SECURITY OPERATION CENTER)*
Formation : BTS CIEL (cybersécurité, informatique et réseaux, électronique) ou BTS SIO (services informatiques aux organisations), complété par un BUT informatique ou un BUT R&T (réseaux et télécommunications) avec un parcours en cybersécurité, une LP métiers de l'informatique : administration et sécurité des systèmes et des réseaux, une LP métiers des réseaux informatiques et télécommunications, etc. **Qualités :** pédagogie, sang-froid, sens de l'analyse.

Retrouvez les déroulés des sigles des diplômes p. 29.

MON PARCOURS

Diplômée d'un bac général, j'ai obtenu un DUT* réseaux et télécommunications, puis une LP en administration des systèmes et réseaux informatiques. J'ai travaillé 3 ans à la station biologique de Roscoff en tant qu'administratrice systèmes, avant de m'engager dans la Marine nationale pour devenir officier marinier (équivalent de sous-officier). Après avoir passé une certification interne à l'armée, j'ai débuté en tant qu'opératrice radio sur un porte-hélicoptères amphibie, puis je me suis spécialisée dans la cyberdéfense et j'ai été affectée à mon poste actuel.

* Devenu une certification intermédiaire du BUT.



Chloé Maque, 30 ans
PREMIER-MAÎTRE, ANALYSTE FORENSIQUE SYSTÈMES, COMCYBER*, À RENNES (35)

Au sein d'un quartier militaire, Chloé a pour mission principale d'intervenir à la suite d'une cyberattaque sur les systèmes informatiques du ministère des Armées. Son travail peut être comparé à celui d'une détective numérique.

Il y a 2 ans, j'ai été affectée au Comcyber*, le centre d'analyse en lutte informatique défensive. Même loin de la mer, je commence ma journée en enfilant mon uniforme bleu de marin. J'évolue dans un environnement interarmées, aux côtés de militaires et de civils. Lors d'un incident cyber, je me déplace en équipe et je collecte des preuves numériques (*logs*, disques durs, mémoire). On appelle cela « faire de l'analyse forensique ». J'identifie les techniques utilisées par les attaquants, et je peux aussi réaliser un rétroplanning de leurs actions. Enfin, je contribue à l'assainissement du système compromis et formule des recommandations pour éviter que cela ne se reproduise. Ce que j'aime dans le statut de militaire, c'est de ne pas passer tout mon temps derrière un ordinateur. Chaque semaine, il peut m'arriver de participer à un footing d'équipe ou de pratiquer le tir sur mes heures de travail. Certes, je suis spécialisée en cyber, mais je reste avant tout militaire et je dois être opérationnelle. À tout moment, je peux être envoyée sur un exercice cyber à l'étranger ou intervenir sur un théâtre d'opérations, en lien avec mes compétences, pour défendre les intérêts de la France.

* Commandement de la cyberdéfense.

FICHE MÉTIER

ANALYSTE FORENSIQUE SYSTÈMES

Formation : BTS CIEL (cybersécurité, informatique et réseaux, électronique) ou BTS SIO (services informatiques aux organisations), complété par un BUT R&T (réseaux et télécommunications) ou une LP métiers de l'informatique : administration et sécurité des systèmes et des réseaux, puis éventuellement par un master informatique ou un diplôme d'ingénieur spécialisé en cybersécurité ; CS cybersécurité ou CS SNO (services numériques aux organisations). **Qualités :** esprit d'équipe, rigueur, sens de l'analyse.

Retrouvez les déroulés des sigles des diplômes p. 29.

MON PARCOURS

Intéressé par l'informatique et les jeux vidéo, j'aime comprendre comment tout cela fonctionne. J'ai raté le bac deux fois, mais une école m'a accepté en BTS systèmes numériques* et j'ai effectué la 2de année en alternance. J'ai alors suivi la 3e année de bachelor cybersécurité de l'ESGI**, toujours en alternance, que j'ai prolongée avec un master cybersécurité. Et je l'ai obtenu tout en participant à des concours de hacking. J'ai ensuite travaillé dans différentes entreprises en tant qu'analyste de la menace cybersécurité, avant d'intégrer Team Cymru.

* Devenu le BTS cybersécurité, informatique et réseaux, électronique.
** École supérieure de génie informatique.

Thibault Seret, 29 ans
ANALYSTE DE LA MENACE EN CYBERSÉCURITÉ, TEAM CYMRU, À AMSTERDAM (PAYS-BAS)

Derrière ses ordinateurs, Thibault traque les pirates internationaux, analyse des virus complexes, rédige des rapports et des communications publiques. Il aime la collaboration entre pairs et la grande autonomie dont il bénéficie.

Depuis chez moi, je travaille avec trois ordinateurs : un pour mes recherches, un autre connecté à mon entreprise pour accéder aux e-mails, aux outils internes…, et un dernier pour réaliser des tests, stocker et analyser des virus… Ce dernier est très sécurisé : rien ne peut en sortir. Nous sommes trois investigateurs cybercriminels dans l'équipe. Je suis spécialisé dans les groupes malveillants reliés à des gouvernements étrangers (Iran, Corée du Nord…), une collègue aux États-Unis travaille sur les botnets* et un autre nous aide de manière transversale sur ces deux domaines. Nous nous parlons quotidiennement, car nous utilisons les mêmes outils et données ; nous échangeons des astuces et relisons les textes des conférences que nous donnons sur nos recherches respectives pour des entités privées et publiques. La collaboration est essentielle, y compris avec des homologues qui se trouvent chez des concurrents. Comme mon entreprise vend des données, mon rôle est de démontrer à quel point elles sont sécurisées et fiables. Il nous arrive également de coopérer avec la police, comme en 2024 lors de l'opération EndGame, au cours de laquelle nous avons contribué à identifier des botnets et trois gros virus. Je ne compte pas mes heures, et mes journées sont différentes en fonction des sujets dont je m'occupe.

* Réseau d'ordinateurs infectés par des logiciels malveillants.

FICHE MÉTIER

ANALYSTE DE LA MENACE CYBERSÉCURITÉ
Formation : master en cybersécurité, diplôme d'ingénieur spécialisé en informatique ou diplôme d'école spécialisée en informatique ou en cybersécurité, éventuellement complété par un MS spécialiste en cybersécurité ou un MS sécurité de l'information et des systèmes.
Qualités : aisance relationnelle, autonomie, persévérance.

Retrouvez les déroulés des sigles des diplômes p. 29.

MON PARCOURS

Adolescente, j'ai commencé à m'intéresser à la cybersécurité lorsque mon site a été attaqué. J'ai alors choisi de suivre un bac général, une classe prépa et un diplôme d'ingénieur en informatique. J'ai été embauchée à la Société générale, où j'avais fait mon stage de fin d'études. J'ai ensuite évolué au poste de RSSI* adjointe à Bourse Direct, avant d'entrer chez AG2R La Mondiale pour y créer un Cert**. Aujourd'hui, je m'occupe de l'équipe de réponse aux incidents d'Advens.

* Responsable de la sécurité des systèmes d'information.
** *Computer Emergency Response Team,* ou équipe de réponse aux incidents de cybersécurité, joignable 24 heures sur 24 et 7 jours sur 7.

Marine Martin, 32 ans
RESPONSABLE DE L'ÉQUIPE RÉPONSE AUX INCIDENTS, ADVENS, À PARIS (75)

Marine intervient à la demande d'entreprises ou d'administrations ayant subi une cyberattaque ou dont le système informatique a été endommagé. Telle une détective, elle mène l'enquête pour déterminer la cause et l'origine du problème.

Je suis responsable d'une équipe de huit personnes et, tels des cyber-pompiers, toujours à plusieurs, nous répondons, dans l'urgence, à un incident en cours après une cyberattaque. Nous sommes sollicités à n'importe quelle heure du jour et de la nuit pour intervenir dans tous types de structures (petites et moyennes entreprises, administrations, grands groupes) appartenant à tous les secteurs d'activité. Nous agissons à distance ou en nous déplaçant partout en France lorsque les moyens de communication ne sont plus sûrs. Selon la taille de l'entreprise, nous traitons avec le directeur, le RSSI* ou encore le responsable de communication. Nous apportons une expertise technique, mais nous devons également rassurer les clients paniqués. J'organise le travail et les astreintes de mon équipe, je fixe les priorités, les éléments à investiguer, etc. Je peux être amenée à transmettre nos résultats d'analyse à la police. Notre métier exige une grande rigueur, notamment lorsque nous manipulons des preuves, qui peuvent éventuellement être exploitées lors d'un procès. Entre les missions, nous prenons du temps pour récupérer physiquement et psychologiquement et développons nos outils en faisant de la R&D** et de la veille.

* Responsable de la sécurité des systèmes d'information.
** Recherche et développement.

FICHE MÉTIER

RESPONSABLE DE CENTRE DE RÉPONSE AUX INCIDENTS

Formation : master en informatique, en ingénierie des systèmes complexes ou en réseaux et télécommunication, ou encore diplôme d'ingénieur spécialisé en cybersécurité avec une forte composante en systèmes et réseaux, complétés par quelques années d'expérience professionnelle et, éventuellement, un MS cybersécurité des infrastructures et des données.
Qualités : empathie, réactivité, sang-froid.

Retrouvez les déroulés des sigles des diplômes p. 29.

Tristan Manzano, 33 ans

ANALYSTE RÉPONSE AUX INCIDENTS DE SÉCURITÉ, THEIA SECURITY DATA NETWORK, À SAINT-AVERTIN (37)

Seul ou en équipe, Tristan intervient dans des entreprises de tous secteurs pour repérer les failles de sécurité informatique. Il analyse tout signal suspect sur les systèmes d'information et peut se déplacer en urgence lors d'une cyberattaque.

MON PARCOURS

Après un bac pro CIEL*, j'ai fait un BTS R&T**, puis je me suis inscrit à Cesi, une école d'ingénieurs où j'ai suivi ma formation en alternance jusqu'en 4e année, mais je ne l'ai pas terminée. J'ai alors créé mon entreprise en cybersécurité. Après 5 ans d'activité, un partenaire m'a proposé une fusion. Je suis devenu directeur technique, responsable de la partie cybersécurité et défense de cette nouvelle entité.

* Cybersécurité, informatique et réseaux, électronique.
** Réseaux et télécommunications.

Mon métier consiste à analyser la cybermenace qui pèse sur les entreprises avec lesquelles nous collaborons. Je travaille seul ou en équipe de quatre ou cinq personnes, selon le périmètre de la mission. Nous utilisons les mêmes outils que les hackeurs pour chercher les failles dans tout ce qui est connecté (voitures, caméras de surveillance, ordinateurs, robots…). Depuis une dizaine d'années, il y a une hausse des intrusions physiques dans les bâtiments des entreprises afin de prendre la main sur leur système informatique. Mon équipe et moi pouvons donc faire des tests de manipulation de personnes, en appelant un employé et en se faisant passer pour un faux conseiller, par exemple, pour voir s'il se fait piéger en donnant des mots de passe ou des informations sensibles. Je travaille aussi en cyberdéfense, en centralisant les incidents qui surviennent sur le serveur de mon entreprise cliente. Chaque mission se termine par un rapport détaillé. Nous avons mis en place des astreintes, car, en cas d'alerte, nous souhaitons comprendre, dans les 15 minutes qui suivent, s'il s'agit d'une attaque, d'une simple panne informatique ou d'une erreur d'origine humaine. Nous sommes également référencés par le Csirt* régional, qui répartit les missions comme un centre d'urgence santé.

* *Computer Security Incident Response Team*, ou équipe de réponse aux incidents de cybersécurité, joignable 24 heures sur 24 et 7 jours sur 7.

FICHE MÉTIER

ANALYSTE RÉPONSE AUX INCIDENTS DE SÉCURITÉ

Formation : master en informatique, en ingénierie des systèmes complexes ou en réseaux et télécommunication (parcours en sécurité des systèmes d'information et des réseaux), ou encore diplôme d'ingénieur avec une spécialisation en sécurité informatique, éventuellement complété par un MS spécialiste en cybersécurité. **Qualités :** aisance relationnelle, autonomie, curiosité.

Retrouvez les déroulés des sigles des diplômes p. 29.

MON PARCOURS

Après un bac général, je me suis orientée vers une licence en droit. Puis je suis entrée à l'emlyon Business School, où j'ai obtenu un diplôme de niveau bac+5 en management. J'ai toujours été intéressée par la cybersécurité et, en remarquant que le secteur du conseil recrutait, j'ai postulé chez Capgemini Invent. Avant le début de mon contrat dans cette entreprise, j'ai suivi quelques mois de formation à l'école 42, une école spécialisée en informatique.

Camille Ghadban, 29 ans

CONSULTANTE SENIOR EN PROTECTION DE DONNÉES PERSONNELLES, CAPGEMINI INVENT, À ISSY-LES-MOULINEAUX (92)

Camille intervient dans des entreprises de différents secteurs et s'adapte à leurs spécificités. Elle veille notamment à ce que les données personnelles de leurs clients soient correctement gérées et ne fuitent pas. Un métier de service gratifiant.

J'interviens lorsqu'une entreprise qui possède des données de clients rencontre un problème, comme une *data breach**, ou qu'elle souhaite opérer une transformation digitale. Je travaille également en amont sur la prévention et la mise en conformité pour la gestion des risques. Je suis experte des sujets de cybersécurité des données personnelles : coordonnées de clients, numéros de cartes bancaires ou de sécurité sociale… Elles circulent et je m'assure qu'elles sont correctement protégées. Je commence par analyser les bases de données de l'entreprise, étudier la plateforme qui les héberge et, pour cela, je collabore aussi bien avec des acteurs techniques, comme les développeurs, qu'avec des acteurs métiers, comme les responsables achats, marketing ou financiers. Je propose une suppression définitive des données qui ne sont plus utilisées et j'instaure de nouvelles stratégies, par exemple un tri tous les 6 mois. Je peux aussi vérifier que la mise en place d'une IA** est conforme à la réglementation. Ce travail nécessite une grande flexibilité, puisqu'il se déroule parfois le week-end afin de ne pas perturber le fonctionnement de l'entreprise cliente.

* Littéralement une « brèche dans la donnée », qui permet à des hackeurs de s'introduire dans un système et de voler des données.
** Intelligence artificielle.

FICHE MÉTIER

CONSULTANT/CONSULTANTE EN PROTECTION DE DONNÉES PERSONNELLES

Formation : master en droit des affaires ou en droit international et droit européen (parcours en données personnelles ou en droit de la concurrence et des contrats), voire en droit des nouvelles technologies ou en droit du numérique, ou diplôme d'ingénieur spécialisé en informatique ou encore diplôme d'école d'informatique, éventuellement complété par un MS cybersécurité des infrastructures et des données, un MS expert en gouvernance de la sécurité des réseaux et des systèmes ou un MS spécialiste en cybersécurité. **Qualités :** adaptabilité, aisance relationnelle, écoute.

Retrouvez les déroulés des sigles des diplômes p. 29.

MON PARCOURS

Diplômé d'un bac général, j'ai préparé un DUT* informatique, une L3 en informatique et un master en sécurité des systèmes d'information. Mon stage de fin d'études s'est déroulé à l'Anssi, où j'étais auditeur en cybersécurité. Puis je suis entré dans une société de conseil, dans laquelle je suis resté près de 4 ans. J'ai ensuite créé mon entreprise, MA Cyber, en 2020 dans le domaine de l'audit et du *pentest*, qui compte aujourd'hui sept employés.

* Devenu une certification intermédiaire du BUT.

Antoine Martin, 32 ans
PENTESTEUR, MA CYBER, À PARIS (75)

Antoine mène des missions de *pentests* (« tests d'intrusion » en français) pour identifier les vulnérabilités d'entreprises variées. Une partie de son temps est également consacrée à la mise à jour de ses connaissances dans un domaine en évolution permanente.

Je suis sollicité pour des missions de *pentests* par des entreprises (tous secteurs confondus) lorsque celles-ci souhaitent identifier les risques auxquels elles sont exposées et s'en protéger. Je me mets dans la peau d'un hackeur en utilisant les mêmes techniques et outils que lui, afin d'identifier les vulnérabilités de leur système d'information. Je commence par recueillir les besoins de l'entreprise qui a fait appel à moi. Je peux réaliser un audit de sécurité pour vérifier que la configuration du système respecte les bonnes pratiques et les normes en vigueur, ou des tests externes sur ce qui est accessible via Internet (site vitrine, application, etc.) pour repérer d'éventuelles failles. Je me rends ensuite dans l'entreprise et j'utilise un compte fourni par celle-ci, afin de tenter de récupérer des données sensibles : feuilles de paie, brevets, données bancaires. Dans 90 % des cas, je parviens à accéder à ces informations, alors que je ne devrais pas. Mon travail consiste alors à compliquer au maximum la tâche des pirates potentiels en proposant des corrections. Et dans un monde qui évolue très rapidement, 25 % de mon temps est consacré à la veille et à la recherche pour être encore plus performant.

FICHE MÉTIER

PENTESTEUR/PENTESTEUSE

Formation : BUT informatique ou LP métiers de l'informatique : administration et sécurité des systèmes et des réseaux, de préférence complété par un master en informatique ou en réseaux et télécommunication, diplôme d'ingénieur avec une spécialisation en sécurité informatique et réseaux, ou encore diplôme d'école spécialisée en informatique ou en cybersécurité. **Qualités :** aisance relationnelle, patience, rigueur.

Retrouvez les déroulés des sigles des diplômes p. 29.

Lena David, 29 ans

HACKEUSE ÉTHIQUE, SYNACKTIV, À RENNES (35)

Lena organise les interventions de son équipe de hackeurs éthiques dans des entreprises clientes. Après des tests d'intrusion permettant d'identifier les failles informatiques, elle leur remet un rapport facilitant la prise de décision de leur direction.

Nos clients sont des entreprises de tous secteurs et de toutes tailles, qui font appel à nous pour évaluer le niveau de sécurité de leur site Internet, de leur application et/ou de leur réseau interne. J'organise une réunion avec chacune d'entre elles pour comprendre ses besoins, puis je choisis dans mon équipe le binôme qui m'accompagnera dans la mission. En accord avec le commanditaire, son budget et ses enjeux, je définis les tests à effectuer, les fonctionnalités sur lesquelles se focaliser, etc. Mon rôle est de me placer dans la posture d'un pirate informatique et d'anticiper les cyberattaques pour éviter qu'elles ne deviennent une réalité. Je me sers d'outils qui détectent les problèmes classiques, comme une mauvaise configuration de sécurité, mais je note également les failles découvertes durant mes recherches, comme l'accès à des données confidentielles ou la possibilité d'utiliser certaines fonctionnalités à des fins malveillantes. Pour clôturer chaque mission, je rédige un rapport contenant le détail de mon étude, des recommandations pour renforcer la sécurité, ainsi qu'un résumé managérial, à destination d'un public non spécialiste.

MON PARCOURS

Après un bac général, j'ai suivi une classe prépa scientifique afin d'intégrer l'INP-Enseeiht*, dans le département informatique et mathématiques appliquées. J'y ai obtenu un double diplôme : un titre d'ingénieur et un master en sécurité des systèmes et des réseaux. À la suite de mon stage de fin d'études, j'ai été embauchée chez Synacktiv en tant qu'experte sécurité. Je suis aujourd'hui responsable d'une équipe de près de 20 personnes.

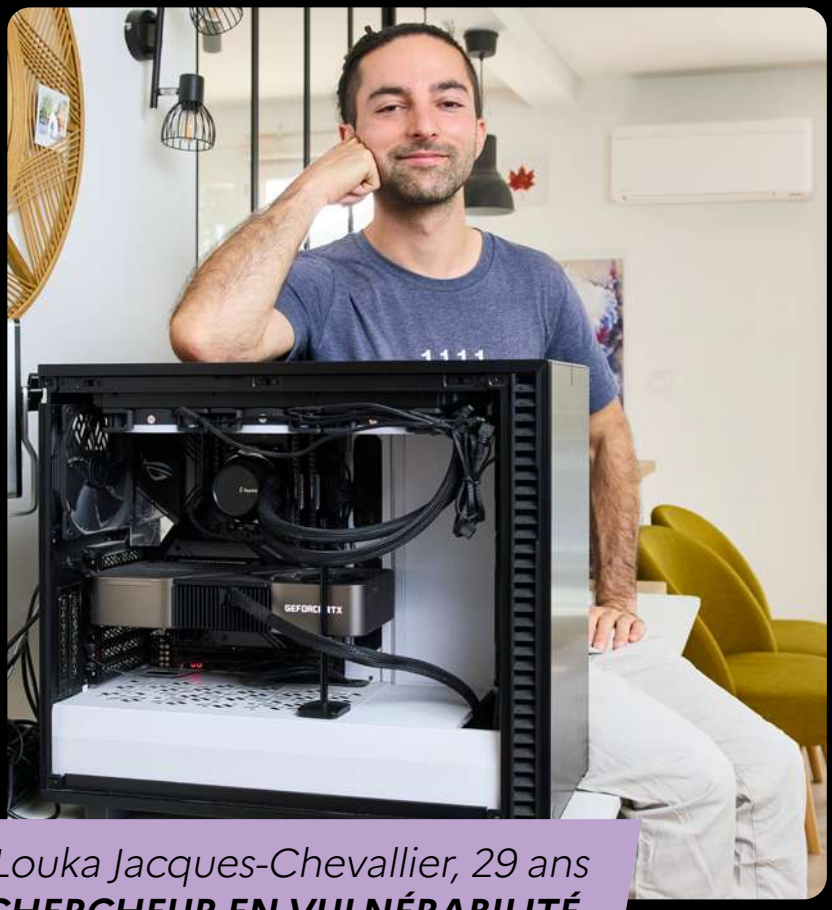
* Institut national polytechnique de Toulouse.

FICHE MÉTIER

HACKEUR/HACKEUSE ÉTHIQUE

Formation : BUT informatique, BUT réseaux et télécommunications, bachelor d'école d'ingénieurs ou d'école spécialisée, ou encore LP métiers de l'informatique : administration et sécurité des systèmes et des réseaux, complété par un master, un diplôme d'ingénieur ou un diplôme d'école spécialisée dans les domaines de l'informatique et de la cybersécurité.
Qualités : adaptabilité, aisance relationnelle, curiosité.

Retrouvez les déroulés des sigles des diplômes p. 29.



Louka Jacques-Chevallier, 29 ans
CHERCHEUR EN VULNÉRABILITÉ, OFFENSKILL, À LYON (69)

Depuis qu'il a lancé sa société, Louka se consacre au développement d'outils pour plus d'efficacité dans la recherche de failles de sécurité. Il écrit aussi des articles sur ce sujet, crée du contenu éducatif et aide les entreprises à se sécuriser.

MON PARCOURS

Mon bac général en poche, je me suis orienté vers une école d'ingénieurs avec prépa intégrée : l'Esisar*. J'ai effectué mon stage de fin d'études aux États-Unis dans une entreprise d'observabilité *cloud*, avant d'intégrer une boîte de consultants pour faire du *pentest*, en France. Puis j'ai rejoint une société d'e-commerce en ligne pour sécuriser leur infrastructure et leur site, tout en commençant à monter ma propre entreprise, OffenSkill.

* École nationale supérieure en systèmes avancés et réseaux de l'Institut polytechnique de Grenoble.

En tant que chercheur en sécurité informatique à mon compte, j'effectue un travail qui s'apparente à celui du pentesteur. Les entreprises me contactent et je les rencontre pour comprendre leurs métiers, leurs spécificités, le type de données en jeu (bancaires, de santé…), etc. J'explique également ma méthodologie. À partir du code source fourni par l'entreprise ou des sites et des adresses IP (numéros d'identification des appareils connectés) à auditer, j'observe comment fonctionnent ces systèmes et les technologies qui les composent. Je recherche ensuite les vulnérabilités, puis j'analyse si des données ou des accès administrateur peuvent être volés. À mi-parcours, je fais le point avec l'entreprise, je commence à rédiger le rapport d'audit, qui explique la manière d'exploiter chaque faille trouvée, son impact, sa criticité, et les mesures correctives à envisager. Une fois ces dernières appliquées, je fais une vérification finale. Je peux aussi former, sur demande, l'équipe chargée du système informatique dans l'entreprise. La cybersécurité est un domaine où il n'existe pas de limite aux apprentissages et dans lequel on peut toujours s'améliorer. Entre les missions, je travaille à la rédaction d'articles, à la création de contenus éducatifs et au développement de nouveau outils.

FICHE MÉTIER

CHERCHEUR/CHERCHEUSE EN VULNÉRABILITÉ

Formation : master en informatique, en mathématiques et applications ou en réseaux et télécommunication (parcours en cybersécurité), ou encore diplôme d'ingénieur avec une spécialisation en informatique et réseaux, en systèmes numériques ou en cybersécurité. **Qualités :** organisation, persévérance, polyvalence.

Retrouvez les déroulés des sigles des diplômes p. 29.

Fadimatou Abdoulaye, 44 ans
AUDITRICE EN CYBERSÉCURITÉ, COVÉA, À PARIS (75)

Fadimatou veille à ce que les prestataires informatiques du groupe Covéa respectent les exigences de sécurité définies dans leur contrat. Un métier exigeant qui requiert rigueur, organisation et un sens aigu de la communication.

Nous sommes deux dans mon équipe à évaluer les prestataires informatiques (sociétés de services, éditeurs de logiciels, etc.) avec lesquels le groupe Covéa (Maaf, MMA, GMF) a signé un accord de sécurité. J'analyse l'ensemble des documents attestant la conformité des services et outils fournis : politique de sécurité, gestion des accès, cryptographie, sécurité physique,respect des réglementations, etc. L'objectif est de réduire le risque de tout incident de sécurité, notamment les fuites de données. Avant de lancer un audit, je mobilise les parties prenantes internes (personnes de différents services : achats, clients, assistance, protection juridique…) ainsi que le prestataire fournisseur concerné et le cabinet d'audit externe. Ce dernier nous accompagne dans l'analyse des documents, en s'appuyant sur les exigences contractuelles. Je pilote l'ensemble du processus : planification, suivi de l'avancement, vérification de la conformité. Un audit dure entre 3 et 9 mois et j'en gère plusieurs simultanément, à différents stades d'avancement. Nous en réalisons entre 10 et 20 par an. À l'issue de chacun, le cabinet rédige une synthèse assortie d'une note de conformité, et je m'assure que les éventuelles non-conformités sont corrigées par le fournisseur.

MON PARCOURS

Après un bac général et un DUT* mesures physiques à Dakar, j'ai suivi des études d'ingénieur en informatique et systèmes d'information à l'UTT**. Une fois diplômée, j'ai commencé ma carrière comme consultante en tests logiciels et automatisation, avant d'occuper plusieurs postes à GMF Assurances (groupe Covéa). Parallèlement, j'ai passé un DU*** de data analyst et une certification de manager de projet intelligence artificielle. J'ai ensuite profité d'un congé formation de 1 an pour suivre un MS en cybersécurité, à l'UTT également. À mon retour, j'ai intégré la direction cybersécurité du groupe Covéa.

* Devenu une certification intermédiaire du BUT.
** Université de technologie de Troyes.
*** Diplôme d'université.

FICHE MÉTIER

ÉVALUATEUR/ÉVALUATRICE DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

Formation : master en informatique ou diplôme d'ingénieur spécialisé en sécurité des systèmes d'information ou en réseaux et télécommunication, éventuellement complété par un MS expert en gouvernance de la sécurité des réseaux et des systèmes ou un MS spécialiste en cybersécurité.
Qualités : aisance relationnelle, organisation, sens de l'analyse.

Retrouvez les déroulés des sigles des diplômes p. 29.

Thierry Berthier, 59 ans

ENSEIGNANT-CHERCHEUR ET CONSULTANT EN CYBERSÉCURITÉ, IUT* DE LIMOGES (87)

À l'université, Thierry forme les futurs développeurs de logiciels et spécialistes en cybersécurité. Au centre de recherche de l'académie militaire de Saint-Cyr Coëtquidan, il travaille aussi à la sécurisation des systèmes connectés : un enjeu crucial !

MON PARCOURS

Après un bac général, une licence et une maîtrise* de mathématiques, j'ai obtenu un DEA** en théories des nombres et un doctorat en algèbre et cryptographie. En plus de mon métier d'enseignant à l'université de Limoges, je dirige le groupe sécurité intelligence artificielle robotique du Hub France IA***. En tant que chercheur associé au CReC, le centre de recherche de Coëtquidan, je participe aussi à des groupes de réflexion et de conseils scientifiques. Je suis également consultant en cybersécurité et cyberdéfense.

* Aujourd'hui master 1.
** Diplôme d'études approfondies, aujourd'hui master 2.
*** Intelligence artificielle.

Spécialiste de la cybersécurité des systèmes physiques embarqués et de tout objet connecté pouvant être la cible d'une attaque pour en prendre le contrôle, je consacre 50 % de mon temps à l'enseignement et 50 % à la recherche. À l'IUT* de Limoges, je suis enseignant en BUT informatique. Dès la 2e année, le programme académique initie les étudiants à la sécurité informatique et à l'IA (intelligence artificielle), ce qui passe notamment par l'algèbre, les probabilités et les statistiques. La formation comprend de la théorie, mais aussi des TP (travaux pratiques), et la cybersécurité est intégrée dans toutes les matières afin d'apprendre à développer des applications, des sites, des solutions sécurisées, etc., sans créer de failles de sécurité. Au centre de recherche de Saint-Cyr Coëtquidan, je travaille sur la cybersécurité dans l'espace de combat, sur l'IA militaire et la sécurisation des avions, des drones, des satellites, des bateaux… Les enjeux sont énormes et vont s'intensifier avec l'arrivée des robots humanoïdes, qui sont déjà très avancés en Chine. Je mène une veille technologique nécessaire, je participe à des colloques et je partage mes recherches en rédigeant des articles dans des revues spécialisées. La recherche est un travail de longue haleine.

FICHE MÉTIER

ENSEIGNANT-CHERCHEUR/ENSEIGNANTE-CHERCHEUSE EN CYBERSÉCURITÉ

Formation : doctorat en cybersécurité. **Qualités :** curiosité, persévérance, polyvalence.

Retrouvez les déroulés des sigles des diplômes p. 29.

Maud Pellerin, 46 ans
JURISTE IT (INFORMATION TECHNOLOGY) *ET CYBERSÉCURITÉ, KLESIA, À PARIS (75)*

Véritable garde-fou juridique de l'entreprise, Maud veille à ce que les différents services respectent les lois et les obligations légales en matière de sécurité informatique, mais s'assure aussi de la conformité des contrats d'achats de prestations informatiques.

Je suis la référente juridique de la direction des risques SSI* et de la résilience. Je l'aide à comprendre les lois sur la sécurité informatique et à écrire des instructions à destination des salariés. J'assiste aussi la direction des achats, en rédigeant des contrats de prestation informatique. Je rédige des stipulations qui garantissent la sécurité des accès aux locaux et aux systèmes d'information de Klesia, et qui protègent l'entreprise en cas d'attaque ou d'incident informatique. Je négocie souvent les clauses de responsabilité, de sécurité et de garanties avec mon homologue côté prestataire. Le défi principal : déterminer les montants d'indemnisation dus par le prestataire en cas de manquement. Mes missions nécessitent de veiller en permanence à la prise en compte des réglementations françaises et européennes en matière de sécurité informatique, qui évoluent régulièrement. Je dois aussi me soucier des autres domaines du droit. Ainsi, si l'entreprise est victime d'un vol de données par un salarié malveillant, c'est le droit social qui s'applique pour le sanctionner. La signature du contrat étant la dernière étape d'un process parfois long, mais nécessaire, je dois rester rigoureuse pour garantir la sécurité juridique de l'entreprise.

* Sécurité des systèmes d'information.

MON PARCOURS

Titulaire d'un bac général, j'ai validé une 1re année de prépa littéraire avant de me réorienter en 1re année de licence en droit. J'ai ensuite obtenu une maîtrise* en droit privé et un DESS** en droit des affaires internationales. À la suite d'un stage, j'ai été recrutée à BNP Paribas en tant que juriste spécialisée sur les successions, avant d'évoluer vers la direction des achats. Puis j'ai travaillé chez un prestataire de services informatiques comme directrice juridique adjointe, avant de rejoindre le groupe Klesia à mon poste actuel.

* Devenu le master 1.
** Devenu le master 2.

FICHE MÉTIER

JURISTE EN CYBERSÉCURITÉ
Formation : master en droit du numérique, complété par des formations dans le domaine de la cybersécurité et des réglementations propres au secteur d'activité visé. **Qualités :** autonomie, curiosité, rigueur.

Retrouvez les déroulés des sigles des diplômes p. 29.

Quentin Nicaud, 35 ans
DIRECTEUR COMMERCIAL EN CYBERSÉCURITÉ, ELYSIUM SECURITY, À SAINT-CYR-AU-MONT-D'OR (69)

MON PARCOURS

J'ai suivi un bac général, un bachelor en commerce et marketing puis, en alternance, un MBA* marketing international, management et vente**. Je suis alors parti 5 ans au Japon, où j'ai exercé d'abord comme professeur d'anglais, puis comme commercial et chargé de projet dans l'événementiel. De retour en France, j'ai continué à travailler dans ce secteur, mais la crise sanitaire de 2019 a stoppé mon activité. Je me suis donc formé, en autodidacte, à la cybersécurité. 3 ans plus tard, je suis devenu directeur commercial d'Elysium Security.

* Master of Business Administration, diplôme international de niveau bac+5.
** Devenu le MBA chargé d'affaires entreprises.

Quentin propose des solutions de cybersécurité adaptées aux besoins de ses clients. Aidé de son équipe, il exerce un travail qui demande de la patience, des connaissances techniques et de la disponibilité.

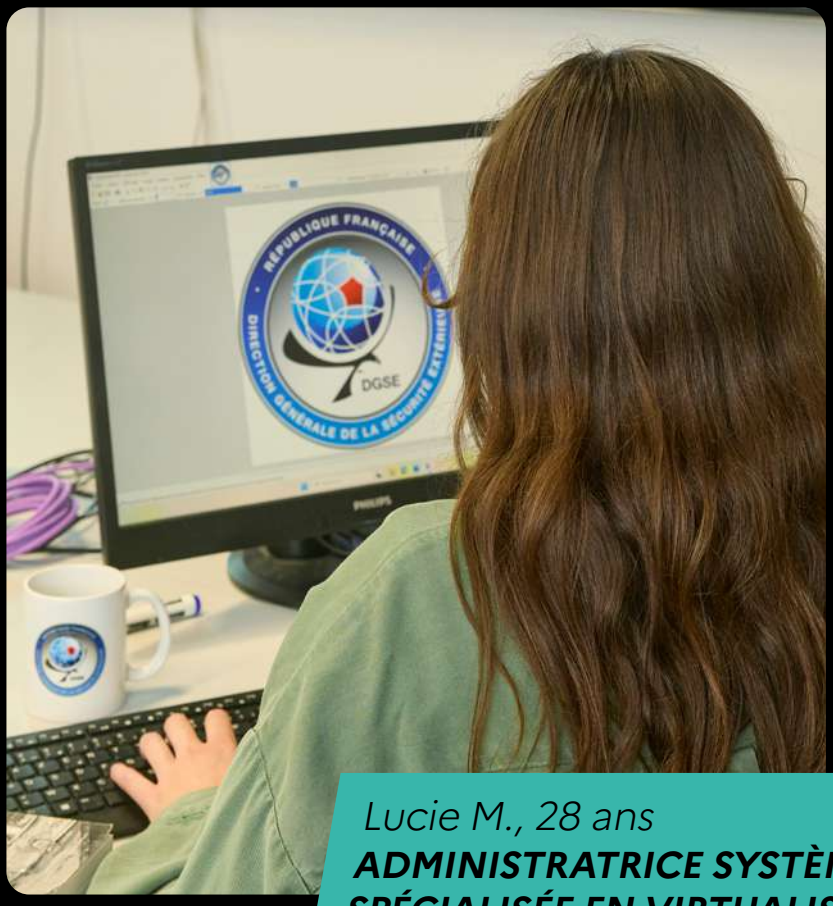
Avec l'aide de mon équipe, composée de quatre commerciaux, je travaille pour des entreprises et des administrations de toutes tailles. Notre rôle est de comprendre les besoins du client afin de hiérarchiser les actions en fonction du budget dont il dispose et de lui fournir une gamme complète de services en cybersécurité. Si je suis toujours le premier contact avec le RSSI* (ou équivalent) de l'entreprise cliente, en fonction du sujet, mon équipe et moi sommes parfois accompagnés de l'un de nos référents techniques. Notre force réside dans notre disponibilité, depuis la signature du contrat jusqu'à l'installation des solutions préconisées, en passant par l'audit, la formation, l'assistance, la gestion d'éventuels incidents, etc. L'activité est cyclique : en fin d'année, nous sommes plutôt sollicités pour réaliser des audits, le début d'année et l'été étant généralement plus calmes. Je me déplace en France et parfois à l'étranger pour rencontrer mes clients ou des prospects, notamment sur des salons professionnels. J'assure aussi une veille technique continue pour maintenir mes connaissances à jour. Une autre partie de mes tâches consiste à aider les commerciaux de mon équipe à monter en compétences, à suivre leur travail et leurs objectifs. Je suis également associé aux appels d'offres publics et participe aux comités de direction.

* Responsable sécurité des systèmes d'information.

FICHE MÉTIER

COMMERCIAL/COMMERCIALE EN CYBERSÉCURITÉ
Formation : bachelor et diplôme d'école de commerce ou master en informatique (parcours en cybersécurité), ou encore diplôme d'école spécialisée en cybersécurité. **Qualités :** curiosité, écoute, patience.

Retrouvez les déroulés des sigles des diplômes p. 29.



MON PARCOURS

Après un bac STI2D*, un BTS SIO** et une LP en réseaux informatiques et télécommunications, j'ai rencontré des représentants de la DGSE*** sur un salon, ce qui m'a donné envie de postuler, malgré un long processus de recrutement. Après un stage d'intégration et l'acquisition de certifications, j'ai débuté comme administratrice système d'exploitation avant d'évoluer vers la conception. Je prépare aujourd'hui un master en cybersécurité en formation continue.

* Sciences et technologies de l'industrie et du développement durable.
** Services informatiques aux organisations.
*** Direction générale de la sécurité extérieure.

Lucie M., 28 ans

ADMINISTRATRICE SYSTÈME SPÉCIALISÉE EN VIRTUALISATION, DGSE*, À PARIS (75)

Au sein de la direction technique et de l'innovation, Lucie gère les accès au système d'information fermé de la DGSE* et de ses antennes à l'étranger. Garante de la confidentialité des données, elle met en place des automatisations pour en réguler les accès.

Tous les agents de la DGSE* travaillent sur un réseau fermé, coupé de l'Internet pour éviter les intrusions. En équipe, nous avons construit l'architecture de ce système de A à Z, mais il faut gérer les mises à jour, les ajouts d'applications et la résolution d'incidents, ce qui justifie des astreintes au rythme d'une par mois. Avec mes collègues, nous gérons aussi la messagerie, le stockage de données, les pare-feu et les droits d'accès de milliers d'agents en France et dans les antennes à l'étranger, où je peux me rendre pour installer du matériel et des systèmes informatiques. Toutes les informations sont cloisonnées pour que personne n'ait accès à tout, même pas à l'identité réelle des agents que nous sommes chargés de protéger. Tout ce que je fais est tracé. La transparence fait partie intégrante de notre engagement. Je gère l'automatisation des accès, grâce au langage Python et PowerShell, et c'est une satisfaction de voir ce que j'ai développé se réaliser automatiquement. Nous nous servons d'outils à la pointe de la technologie et nous réalisons en interne des audits réguliers pour vérifier l'absence de faille de sécurité, car nous sommes garants de la confidentialité des opérations en France comme à l'étranger.

* Direction générale de la sécurité extérieure.

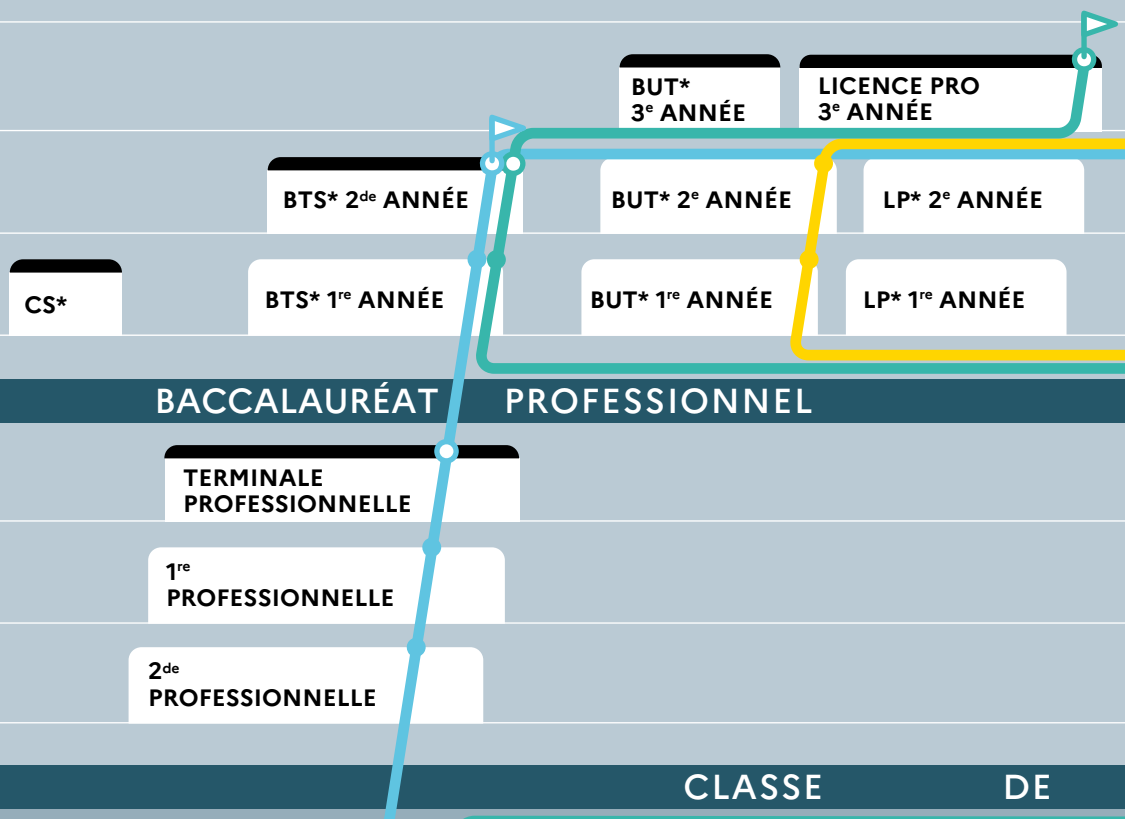
FICHE MÉTIER

ADMINISTRATEUR/ADMINISTRATRICE SYSTÈME
Formation : BTS CIEL (cybersécurité, informatique et réseaux, électronique), BTS SIO (services informatiques aux organisations), complété par un BUT informatique, un BUT R&T (réseaux et télécommunications) ou une LP métiers de l'informatique : administration et sécurité des systèmes et des réseaux ou encore une LP métiers des réseaux informatiques et télécommunications. **Qualités :** esprit d'équipe, persévérance, rigueur.

Retrouvez les déroulés des sigles des diplômes p. 29.

À CHACUN ET CHACUNE SON PARCOURS

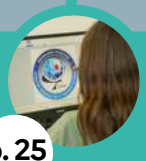
À bac+2, bac+3, bac+5, voire à bac+8, à l'université ou en école, les parcours de Tristan, Lucie, Mickaël, Thierry et Marine en témoignent : de nombreux diplômes, obtenus à différents niveaux d'études, permettent d'exercer un métier dans la cybersécurité.



p. 16

Tristan, 33 ans

Avec un bac pro CIEL* et un BTS* R&T*, Tristan entre en école d'ingénieurs. Il ne termine pas son cursus, mais crée son entreprise en cybersécurité.



p. 25

Lucie, 28 ans

Après un bac STI2D* et un BTS* SIO*, Lucie suit une LP* en réseaux informatiques et télécommunications. Elle rejoint la DGSE* après un long processus de recrutement.

p. 8

Mickaël, 46 ans

Titulaire d'un bac STI2D*, Mickaël s'inscrit en DUT* GEII*. Une licence et un master en systèmes de télécommunications et informatique lui permettent d'évoluer rapidement.

POUR ALLER PLUS LOIN
https://evolution.campuscyber.fr/files/TAL-CYB.pdf
www.onisep.fr

DOCTORAT 3 — BAC+8
DOCTORAT 2 — BAC+7
DOCTORAT 1 — MASTÈRE SPÉCIALISÉ — BAC+6
MASTER 2 — DIPLÔME D'INGÉNIEURS ou D'ÉCOLE SPÉCIALISÉE — BAC+5
MASTER 1 — DIPLÔME D'INGÉNIEURS ou D'ÉCOLE SPÉCIALISÉE — BAC+4
LICENCE 3 — DIPLÔME D'INGÉNIEURS ou D'ÉCOLE SPÉCIALISÉE — BAC+3
LICENCE 2 — ÉCOLE ou PRÉPA — BAC+2
LICENCE 1 — ÉCOLE ou PRÉPA — BAC+1

OU TECHNOLOGIQUE OU GÉNÉRAL

TERMINALE TECHNOLOGIQUE — TERMINALE GÉNÉRALE
1re TECHNOLOGIQUE — 1re GÉNÉRALE
2de GÉNÉRALE ET TECHNOLOGIQUE — 2de GÉNÉRALE ET TECHNOLOGIQUE

TROISIÈME

p. 22

Thierry, 59 ans

À la suite d'un bac général, Thierry s'oriente en licence, puis en master de mathématiques, qu'il complète avec un doctorat en algèbre et cryptographie. Il est aujourd'hui enseignant-chercheur.

p. 15

Marine, 32 ans

Marine passe un bac général et opte pour une prépa scientifique avant d'obtenir un diplôme d'ingénieur. Elle est embauchée dès la fin de son stage de fin d'études.

* LÉGENDE

BTS : brevet de technicien supérieur
BUT : bachelor universitaire de technologie
CIEL : cybersécurité, informatique et réseaux, électronique
CS : certificat de spécialisation
DGSE : Direction générale de la sécurité extérieure
DUT : diplôme universitaire de technologie, devenu une certification intermédiaire du BUT
GEII : génie électrique et informatique industrielle
LP : licence professionnelle
R&T : réseaux et télécommunications
SIO : services informatiques aux organisations
STI2D : sciences et technologies de l'industrie et du développement durable

ANNÉE D'EXAMEN

Dernier diplôme acquis ou en cours d'acquisition

LES DIPLÔMES DU SECTEUR

CS*, BTS*, BUT*, LP*, master, diplôme d'ingénieur, doctorat… les principaux diplômes pour travailler dans la cybersécurité sont présentés ici. La plupart d'entre eux comportent des stages ou peuvent être préparés en alternance. La formation continue constitue également un réel atout dans ce secteur.

CS

Après un bac | En 1 an

En lycée professionnel ou en CFA*

Le CS (certificat de spécialisation) est une qualification de niveau bac, centrée sur la maîtrise de savoirs, de savoir-faire et de gestes professionnels spécialisés.
→ **Apprentissage possible.**

- **CS cybersécurité**
- **CS SNO (services numériques aux organisations)**

BTS

Après un bac | En 2 ans

En lycée, en école ou en CFA*

Le BTS (brevet de technicien supérieur) débouche directement sur l'emploi ou sur une poursuite d'études.
→ **Apprentissage possible.**

- **BTS CIEL (cybersécurité, informatique et réseaux, électronique)**
- **BTS SIO (services informatiques aux organisations)**

BUT

Après un bac | En 3 ans

En IUT*

Le BUT (bachelor universitaire de technologie), dont le DUT (diplôme universitaire de technologie) est une certification intermédiaire à bac+2, débouche directement sur l'emploi ou sur une poursuite d'études.
→ **Apprentissage possible.**

- **BUT informatique**
- **BUT R&T (réseaux et télécommunications)**

LP

Après un bac, un bac+1 ou un bac+2 | En 1, 2 ou 3 ans

À l'université, en école, en lycée ou en CFA*

De durée variable selon le niveau d'entrée en formation, la LP (licence professionnelle) permet de se spécialiser ou d'acquérir une double compétence. Elle débouche directement sur l'emploi ou sur une poursuite d'études.
→ **Apprentissage possible.**

- **LP métiers de l'informatique : administration et sécurité des systèmes et des réseaux**
- **LP métiers des réseaux informatiques et télécommunications**

MASTER

Après un bac+3 | En 2 ans

À l'université

Plusieurs masters permettent de travailler dans le secteur de la cybersécurité après une licence adaptée ou de poursuivre des études en doctorat (bac+8) pour faire de la recherche.
→ **Apprentissage possible.**

- **Master cybersécurité**
- **Master droit des affaires**
- **Master droit des nouvelles technologies**
- **Master droit du numérique**
- **Master droit international et droit européen**
- **Master informatique**
- **Master ingénierie des systèmes complexes**
- **Master management des systèmes d'information**
- **Master mathématiques et applications**
- **Master réseaux et télécommunication**

DIPLÔME D'INGÉNIEUR

Après un bac | En 3 ou 5 ans

Après un bac+2 | En 3 ans

En école d'ingénieurs

Publiques ou privées, et aux frais de scolarité variables, les écoles d'ingénieurs délivrent des titres d'ingénieur (bac+5) reconnus par la CTI (Commission des titres d'ingénieur) et parfois des bachelors (bac+3). Elles recrutent majoritairement sur concours post-bac ou post-bac+2, mais aussi par le biais des admissions parallèles, après un bac+3 ou un bac+4. Elles proposent des spécialisations en systèmes avancés et réseaux, en cybersécurité et systèmes embarqués, en informatique et réseaux, en cybersécurité, en sécurité des systèmes d'information et cybersécurité…
→ **Apprentissage possible.**

Familles de métiers

- GESTION DE LA SÉCURITÉ ET PILOTAGE DES PROJETS DE SÉCURITÉ
- CONCEPTION ET MAINTIEN D'UN SYSTÈME D'INFORMATION SÉCURISÉ
- GESTION DES INCIDENTS ET DES CRISES DE SÉCURITÉ
- CONSEIL, SERVICE ET RECHERCHE
- MÉTIERS CONNEXES

DIPLÔME D'ÉCOLE SPÉCIALISÉE

Après un bac | En 3 ou 5 ans

Après un bac+2 | En 3 ans

En école

Les écoles spécialisées en cybersécurité dispensent des diplômes spécifiques, à bac+3 (bachelor), puis à bac+5. Dans certaines, il possible de passer un BTS* en informatique avant d'opter pour une spécialisation en bachelor.

➜ **Apprentissage possible.**

Les écoles d'informatique proposent des bachelors en 3 ans et des cursus en 5 ans permettant, en plus de l'acquisition des bases en informatique, de se spécialiser en sécurité informatique pour travailler dans la cybersécurité.

➜ **Apprentissage possible.**

Les écoles de commerce délivrent des bachelors en 3 ans et des diplômes à bac+5, qui attestent d'une formation généraliste couvrant l'ensemble des fonctions commerciales d'une entreprise.

➜ **Apprentissage possible.**

MS

Après un bac+5 | En 1 an

En école

Le MS (mastère spécialisé) est une formation conçue pour répondre à des besoins dans un domaine précis et vise l'acquisition de compétences spécialisées. Il est également accessible avec un bac+4 et 3 ans d'expérience professionnelle.

➜ **Apprentissage possible.**

MS cybersécurité des infrastructures et des données

MS expert en cybersécurité

MS expert en gouvernance de la sécurité des réseaux et des systèmes

MS spécialiste en cybersécurité

MS sécurité de l'information et des systèmes

EN FORMATION CONTINUE

Il existe de nombreuses formations pour continuer à se former une fois en poste, ce qui représente un enjeu crucial dans le domaine de la cybersécurité alors que l'activité économique ne cesse de se numériser. Si la plupart des diplômes (BTS*, BUT*, licence, master…) peuvent être suivis en formation continue, ou obtenus par la VAE (validation des acquis de l'expérience), il existe diverses manières de tester et d'actualiser ses connaissances.

LES MOOC

Ludiques et accessibles, les MOOC *(Massive Open Online Courses)* sont des cours en ligne qui permettent d'accompagner le développement de compétences. De nombreux organismes (l'Anssi*, la Cnil*, l'Inria*, etc.) et diverses plateformes (notamment My MOOC ou FUN MOOC) proposent de s'autoformer aux défis et aux enjeux de la cybersécurité. Certains MOOC donnent lieu à la délivrance d'un certificat, d'autres non (bien se renseigner).

LES CTF

Qu'ils s'appellent « France Cybersecurity Challenge », « European Cybersecurity Challenge », « Hackropole », « Passe ton hack d'abord » ou encore « Root-Me », les CTF (*Capture the Flag*, littéralement « Capturez le drapeau ») sont des jeux apparus dans les années 1990. Il s'agit de compétitions ludiques, en ligne ou en présentiel, afin de relever, individuellement ou en équipe, des défis liés à la cybersécurité. Ils peuvent être défensifs (pour apprendre à sécuriser un système ou un réseau) ou offensifs (pour exploiter les vulnérabilités d'un système).
À noter : le nombre de CTF accomplis ou bien les scores obtenus sont des critères pris en compte par les recruteurs.

LES FORMATIONS LABELLISÉES

De très nombreuses formations possèdent le label « SecNumedu FC » (formation continue). Délivré par le CFSSI (centre de formation de l'Anssi*), il garantit la spécialisation de la formation en cybersécurité selon une charte de critères précis, notamment une part de 70 % des enseignements consacrés à la cybersécurité. Les formations, labellisées pour 3 ans, sont dispensées au sein d'écoles privées, d'écoles d'ingénieurs, d'organismes de formation en ligne, de CCI (chambres de commerce et d'industrie), etc.
Retrouvez-les sur https://cyber.gouv.fr/secnumedu.
À noter : le CFSSI labellise également de très nombreuses formations initiales comme des BUT*, des licences, des masters, des diplômes d'ingénieurs, des MS*… (label « SecNumedu »).
D'autres labels existent, comme le label « CyberEdu », mis en place pour les formations, initiales et continues, non spécialisées en sécurité informatique, mais qui délivrent le bagage minimum nécessaire en matière de cybersécurité.
Plus d'informations sur https://www.cyberedu.fr.

**** Déroulé des sigles***

Anssi : Agence nationale de la sécurité des systèmes d'information
BTS : brevet de technicien supérieur
BUT : bachelor universitaire de technologie
CFA : centre de formation d'apprentis
Cnil : Commission nationale de l'informatique et des libertés
CS : certificat de spécialisation
DUT : diplôme universitaire de technologie
Inria : Institut national de recherche en sciences et technologies du numérique
IUT : institut universitaire de technologie
LP : licence professionnelle
MS : mastère spécialisé

10 QUESTIONS/RÉPONSES

La cybersécurité offre de multiples parcours de formation, du bac+2 au doctorat. Comment choisir celui qui vous convient ? Des experts répondent aux questions que vous vous posez.

1 POURQUOI SE FORMER À LA CYBERSÉCURITÉ ?

Le secteur est en demande croissante, voire en pénurie de talents. Des dizaines de milliers de postes sont à pourvoir et le recrutement s'effectue à tous les niveaux de formation. Autre atout : *« Les rémunérations sont supérieures de 15 à 20 % par rapport à celles du secteur informatique*, constate Reza El Galai, directeur de l'ITFoRCy*, *et l'impact sociétal est réel, puisque les professionnels du secteur contribuent à la sécurité de la nation. »* Sébastien Langlais, enseignant en informatique et cybersécurité sur le campus de l'école d'ingénieurs Isen* Ouest, explique également que *« dès qu'il y a du numérique, il existe un enjeu de cybersécurité, car là où l'attaquant cherche une porte d'entrée dans un système, le défenseur doit surveiller toutes les portes. On peut se former pour devenir spécialiste ou pour apporter une vision globale sur les risques de cybersécurité »*. De quoi susciter des vocations !

2 QUEL BAC CHOISIR AU LYCÉE ?

Travailler dans la cybersécurité nécessite d'avoir des compétences informatiques. Un bac général assorti des spécialités mathématiques, SI (sciences de l'ingénieur) ou encore NSI (numérique et sciences informatiques) est approprié pour s'engager dans des études de cybersécurité. Maxime Fenêtre, responsable pédagogique du BTS* SIO* et du bachelor en cybersécurité à l'ensemble Saint-Luc Cambrai, précise qu'une partie des enseignements du BTS SIO est axée sur le droit, la gestion et l'anglais : *« 30 % de nos recrutements concernent donc également des lycéens issus d'un bac général ayant conservé les spécialités SES* ou LLCE* anglais, mais nous ne fermons pas non plus la porte aux diplômés d'un bac pro CIEL* ou d'un bac STMG* ou STI2D*. »*

3 BTS* SIO* OU CIEL* : COMMENT CHOISIR ?

Le BTS CIEL apporte des compétences clés en électronique embarquée, en capteurs intelligents ou en réseaux de communication et aborde la cybersécurité de manière générale. Il propose deux options en 2de année : IR* pour travailler au développement d'objets interconnectés ; ER* pour apprendre à installer un réseau informatique. De son côté, le BTS SIO intègre dans ses enseignements un bloc de compétences entièrement consacré à la cybersécurité. En 2de année, elle est appliquée à deux options : l'option SISR* orientée vers les réseaux ; l'option SLAM* davantage tournée vers le développement d'applications. *« Pour résumer,* souligne Maxime Fenêtre, *le BTS CIEL offre surtout des débouchés dans l'industrie et le BTS SIO dans le secteur tertiaire. »*

4 POURQUOI OPTER POUR UN DIPLÔME À BAC+3 ?

« Une LP permet de se spécialiser, par exemple, en sécurité des systèmes et réseaux ou en applications Web. Un bachelor en cybersécurité délivre des connaissances plus approfondies en méthodes de gestion des risques et en sécurité défensive de l'entreprise à travers les aspects juridiques, de sensibilisation à la protection des données, etc. »*, détaille Maxime Fenêtre. Le BUT* mixe les matières générales et techniques, et convient à des étudiants se préparant à une poursuite d'études, même s'ils peuvent aussi choisir d'entrer sur le marché de l'emploi. *« Attention toutefois,* prévient Maxime Fenêtre, *il reste compliqué de passer d'un BTS* à une 3e année de BUT, les étudiants étant le plus souvent contraints d'entrer en 2e année. »* Dans tous les cas, un bac+3 ouvre la voie à des responsabilités accrues.

5 CYBERDÉFENSE : QUELLES FORMATIONS POUR DÉBUTER ?

L'armée et les institutions qui lui sont rattachées (Comcyber*, DGSE*…) recherchent des diplômés de BTS* SIO*, de BTS* CIEL* ou de bachelor en cybersécurité pour œuvrer à la défense du territoire. L'armée prend en charge les frais de scolarité des étudiants, qui reçoivent aussi une solde mensuelle. En contrepartie, ils signent un contrat d'engagement de 3 à 8 ans selon l'armée choisie (terre, air et espace ou Marine nationale). Autre avantage : ils n'ont pas à chercher leurs stages, qui s'effectuent au sein du ministère des Armées. *« Les lycéens peuvent ainsi opter pour le BTS CIEL en parcours marine plutôt qu'en parcours civil. Ils alternent cours académiques au lycée Vauban de Brest et formation militaire au CIN (Centre d'instruction naval) de Brest et effectuent l'ensemble de leurs stages dans des unités de la Marine. Au terme de leurs 2 années d'études, ils deviennent officiers mariniers et sont embarqués sur nos navires sans formation complémentaire »,* développe le capitaine de frégate Bertrand, chargé des partenariats avec l'Éducation nationale au sein de la Marine nationale. Le chef de bataillon Paul-Hubert, coordonnateur du BTS CIEL du lycée militaire de Saint-Cyr, tient un discours similaire : *« La moitié de nos élèves rejoignent l'armée de terre comme techniciens en cybersécurité ; les autres s'engagent comme civils de la défense au profit des services du ministère des Armées (DGSE, DRSD*, DRM*, DIRISI*). En plus du programme classique, les étudiants bénéficient chaque semaine d'heures supplémentaires consacrées à la cyberdéfense, à la pratique sportive et à la préparation du TOEIC*. »* Le bachelor cybersécurité de l'Epita*, conçu en partenariat avec l'École polytechnique et l'armée, s'adresse, quant à lui, à *« de jeunes bacheliers manifestant un intérêt poussé pour l'informatique, la cybersécurité et l'armée »,* révèle Yann Le Doré, directeur du bachelor cybersécurité de l'Epita*.

6 QUELS SONT LES ATOUTS DE L'APPRENTISSAGE ?

L'apprentissage, accessible à tous les niveaux de formation, participe au développement rapide des compétences professionnelles, sans délaisser les connaissances théoriques. Les apprentis perçoivent un salaire et leur expérience en entreprise est un réel levier à l'embauche. *« Les 3 années d'un cycle ingénieur suivies en alternance dans la même entreprise augmentent l'employabilité »,* confirme Sébastien Langlais. *« Chercher une entreprise d'accueil est également formateur,* assure Yann Le Doré. *Les étudiants apprennent à se présenter et à déposer une candidature. »* Enfin, le double encadrement tuteur académique-maître d'apprentissage garantit un suivi sur mesure aux apprenants. Sébastien Langlais conclut : *« Choisir l'apprentissage, c'est accepter des périodes à l'école plus denses, la charge académique étant la même que pour les autres étudiants, mais sur un temps réduit, et emmagasiner de l'expérience professionnelle. »*

7 PARTICIPER À UN JEU CTF* : QUELS AVANTAGES ?

Des compétitions, intitulées CTF (*Capture the Flag,* ou « Capturez le drapeau »), s'adressent aux lycéens et aux étudiants, et proposent, en ligne ou en présentiel, de relever des défis, individuellement ou en équipe, tout en s'amusant. Qu'ils s'appellent « Passe ton hack d'abord », « 404 CTF », « Root-Me »…, de nombreux challenges portent sur la cybersécurité. Une excellente opportunité d'apprentissage, d'après Reza El Galai : *« C'est une manière d'évaluer ses compétences de façon ludique. On y développe le sens du travail en équipe et donc des savoir-faire autant que des savoir-être. Et l'idée d'un challenge "gamifié" pour apprendre en s'amusant remporte de plus en plus de succès auprès des jeunes. »* Sans oublier que le nombre de participations à ces challenges, les thématiques abordées, les scores obtenus… sont autant d'atouts pris en compte lors des recrutements.

* Déroulé des sigles

BTS : brevet de technicien supérieur
BUT : bachelor universitaire de technologie
CIEL : cybersécurité, informatique et réseaux, électronique
Comcyber : Commandement de la cybersdéfense
DGSE : Direction générale de la sécurité extérieure
DIRISI : Direction interarmées des réseaux d'infrastructure et des systèmes d'information
DRM : Direction du renseignement militaire
DRSD : Direction du renseignement et de la sécurité de la défense
Epita : École pour l'informatique et les techniques avancées
ER : électronique et réseaux
IR : informatique et réseaux
Isen : Institut supérieur de l'électronique et du numérique
ITFoRCy : Institut de technologie de formation et de recherche en cybersécurité
LLCE : langues, littératures et civilisations étrangères
LP : licence professionnelle
SES : sciences économiques et sociales
SIO : services informatiques aux organisations
SISR : solutions d'infrastructure, systèmes et réseaux
SLAM : solutions logicielles et applications métiers
STMG : sciences et technologies du management et de la gestion
STI2D : sciences et technologies de l'industrie et du développement durable
TOEIC : *Test of English for International Communication* (test d'anglais évaluant, au niveau international, la capacité à communiquer dans un contexte professionnel)

8 MASTER OU DIPLÔME D'INGÉNIEUR : QUELLES DIFFÉRENCES ?

Le master est un diplôme reconnu en France et en Europe grâce au système LMD* et ouvre logiquement la porte du doctorat pour faire de la recherche. Un diplôme d'ingénieur, titre également reconnu à bac+5, peut aussi permettre de continuer en doctorat, mais souvent à condition de passer par un master à l'université. Le choix se fera donc davantage en fonction des spécialisations proposées à l'université ou en école d'ingénieurs et des particularités pédagogiques. L'UTT*, où travaille Reza El Galai, propose, par exemple, un double diplôme pour lequel les étudiants obtiennent à la fois un master et un diplôme d'ingénieur, grâce au stage final de 6 mois qui est mutualisé. *« Notre école a choisi, quant à elle, d'offrir une formation orientée vers la cyberrésilience, s'appuyant sur plusieurs laboratoires de recherche (en mathématiques, en cybersécurité ou encore en cognition) autour desquels gravitent des chercheurs dans ces différents domaines. Nous avons besoin de tous ces pans pour délivrer une formation complète en gouvernance des risques cyber »*, dévoile Jean-Marc Bascans, directeur de l'Ensar*, une toute nouvelle école d'ingénieurs.

9 UN DOCTORAT : QUELLE PLUS-VALUE ?

Le doctorat à bac+8 est le plus haut diplôme de l'enseignement supérieur, et se conclut par la soutenance d'une thèse. *« L'expertise d'un doctorat est intéressante pour la cybersécurité,* déclare Reza El Galai, *car certaines spécialités sont très recherchées comme la cryptologie ou l'IA*. »* Ce diplôme permet d'enseigner et d'occuper des postes en R&D*. De plus, sa reconnaissance partout dans le monde rend possible une mobilité internationale.

10 PEUT-ON CONTINUER À SE FORMER UNE FOIS EN POSTE ?

« Le domaine de la cybersécurité évolue si rapidement que se former en travaillant est indispensable », estime Sébastien Langlais. Pour cela, il est facile d'assister à des conférences afin de rester en veille sur les nouveautés techniques ou les nouvelles méthodologies de travail. Certaines sont spécialisées sur un sujet (cybersécurité et santé, RGPD*, sécurité dans le *cloud*, etc.). Suivre un MOOC* ou une formation dispensée par l'Anssi* ou par d'autres organismes, participer à un CTF*, acquérir, via son entreprise, des certifications sont également des possibilités. *« Le forum international de la cybersécurité, qui se tient tous les ans à Lille, peut aussi être l'occasion de rencontrer des écoles, des recruteurs, des représentants de collectivités, d'organismes de recherche, d'associations françaises et internationales, et d'assister à des tables rondes »*, ajoute Reza El Galai.

*** Déroulé des sigles**

Anssi : Agence nationale de la sécurité des systèmes d'information
CTF : *Capture the Flag*, littéralement « Capturez le drapeau » (challenge)
Ensar : École nationale supérieure des sciences applicatives et du risque
IA : intelligence artificielle
LMD : licence-master-doctorat
MOOC : *Massive Open Online Courses* (cours en ligne)
R&D : recherche et développement
RGPD : règlement général sur la protection des données
UTT : université de technologie de Troyes

33 % des salariés du secteur ont suivi plus de 5 jours de formation au cours des 12 derniers mois.

Source : Observatoire des métiers de la cybersécurité, 2025.

evolution.campuscyber.fr

CAMPUS CYBER EVOLUTION

LA PLATEFORME ACCESSIBLE À TOUS

POUR TROUVER SA VOIE DANS LA CYBERSÉCURITÉ

- carte des **formations**
- offres d'**emplois**
- **CVthèque**
- base de **ressources**

Ce travail a bénéficié d'une aide de l'Etat gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence «ANR-23-CMAS-0020» et a été réalisé en partenariat avec l'OPCO Atlas et Inria.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ONISEP

ZOOM SUR LES MÉTIERS DE LA CYBERSÉCURITÉ

Cybersécurité offensive, défense active, intelligence artificielle… les entreprises du domaine de la protection des données et des services dans les espaces numériques doivent en permanence innover pour prévenir les attaques malveillantes, d'une part, et accroître l'efficacité des réponses aux incidents dans de nombreux secteurs d'activité (transport, santé, assurance, armée, luxe, sécurité extérieure…), d'autre part. Grâce à des technologies de pointe et à une veille constante, les spécialistes du secteur contribuent à protéger les données sensibles et à garantir la continuité de l'activité des entreprises et des institutions étatiques.

Quels sont les métiers de la cybersécurité ? Quel est le quotidien des personnes qui y travaillent ? Quelles sont les opportunités pour les jeunes ? Comment y évolue-t-on ? Quelles sont les formations pour s'insérer ?

Largement illustré, ce « Zoom » propose une information synthétique sur un secteur qui recrute de plus en plus. Il fait découvrir les métiers via le témoignage concret de celles et ceux qui les exercent. Au travers de leur parcours, parfois atypique, il livre les clés de stratégies d'orientation possibles.

Ce guide aidera les jeunes à se projeter dans leur vie professionnelle et à trouver leur voie. Pour les équipes éducatives, c'est une ressource utile à la découverte des métiers et au parcours Avenir des élèves, au collège et au lycée, ainsi qu'à l'orientation des étudiants et étudiantes.

DANS CE NUMÉRO

Code de diffusion 901728
ISSN 1772-2063
Décembre 2025

Cette publication a été réalisée en collaboration avec :

CAMPUS CYBER

librairie.onisep.fr

ISBN 978-2-273-01728-2

4,90 €