



GUIDE DE DÉMARRAGE DE CARRIÈRE

EN CYBERSÉCURITÉ

<https://cyberini.com>
Édition 2025



UNE PÉNURIE DE COMPÉTENCES À COMBLER



42% des entreprises demandent à leurs employés de suivre au moins une formation cybersécurité par an. [1]



Le taux d'embauche est 2,4x plus élevé dans les métiers du numérique que dans les autres secteurs. [2]



45 % des entreprises ont des difficultés à pourvoir les postes ouverts dans la cybersécurité. [3]



De 2017 à 2021 il y a eu 2 fois plus d'offres d'emploi en cybersécurité et ils vont encore doubler en 2025+. [4]



La pénurie est causée par un écart entre profils de candidats et attentes de recruteurs.

Les RSSI recommandent ainsi d'accroître l'engagement dans la **formation** et la **certification**, ainsi que d'augmenter les rémunérations. [5]

[1] <https://www.getapp.fr/blog/7574/rapport-sur-menaces-cybersecurite-france-2025>

[2] <https://www.pole-emploi.org/accueil/actualites/infographies/les-metiers-du-numerique...>

[3] <https://www.pwc.fr/fr/decryptages/securite/la-cybersecurite-fait-face-a-une-penurie-de-talents...>

[4] <https://www.lesechos.fr/travailler-mieux/metiers-reconversion-professionnelle/salaires...>

[5] <https://www.silicon.fr/cybersecurite-penurie-competences-persiste-414958.html>



UN DOMAINE VASTE ET D'AVENIR

L'une des raisons de la pénurie de compétences évoquée vient du fait que la cybersécurité **est un domaine très vaste et évolutif**. Et cela constitue une véritable **opportunité**. La stratégie nationale « France 2030 » vise à ouvrir **37 000 offres d'emploi en cybersécurité** à partir de 2025. Elle veut faire émerger des champions de la cybersécurité et met les moyens : **1 milliard d'euros d'investissements**.

1. Les multiples spécialisations permettent à chacun de **trouver sa propre voie**. Aujourd'hui, la cybersécurité est requise dans beaucoup de domaines : industrie, finance, commerce, juridique... etc. Les compétences recherchées sont ainsi **très variées, et chacun peut y trouver sa place**.
2. Ces évolutions constantes **créent de nouveaux métiers chaque an**. Plusieurs études montrent que la **moitié des métiers de demain n'existent pas encore (surtout dans le numérique)**. Cela donne **une chance de se reconversion (ou de commencer à partir de zéro)** à tout âge.

« Les profils techniques, type hackers et pentesters sont très recherchés, mais les entreprises ont aussi besoin de sensibilisation et de pédagogie. Il faut des personnes qui aillent au contact des équipes, capables de leur expliquer les règles de base de sécurité »

- Thierry Grandpierre, responsable de la filière Cybersécurité de l'Esiee Paris.



France Compétences établit chaque année une liste des **métiers émergents**. En tête de celle-ci pour l'année 2021 et 2022 se trouvent les métiers de « *Gestionnaire de la sécurité des données, des réseaux et des systèmes* » et de « *Développeur sécurité* ».



60 000€

C'est le salaire brut annuel moyen d'un ingénieur en cybersécurité après 2 à 5 ans d'expérience. Les métiers de la cybersécurité sont les mieux payés du secteur numérique et peuvent dépasser **100 000€** par an après 10 années d'expérience.
Source : Regionjobs



Un boom de métiers cybersécurité est imminent ! Les domaines de l'intelligence artificielle, de la bio-informatique ou encore du métavers vont bouleverser nos vies dans les prochaines années. Il y aura des millions de postes à pourvoir dans le monde. Votre futur métier n'existe peut-être pas encore !



LES PROFILS DE LA CYBERSÉCURITÉ



L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) réalise régulièrement des enquêtes sur les usages, les outils et les acteurs de la cybersécurité. Voici les résultats de sa dernière enquête sur [les profils de la cybersécurité](#).

1

45% des professionnels de la cybersécurité ont moins de 5 ans d'ancienneté

Le secteur est très dynamique et l'âge moyen se situe entre 30 et 49 ans. **20% ont 2 ans d'expérience ou moins dans la cybersécurité.**

2

46,6% n'ont pas de diplômes spécialisés en cybersécurité

Les reconversions sont possibles. Par ailleurs **25% des profils ont une certification en cybersécurité uniquement.**

3

89% sont des hommes, que la structure soit spécialisée ou non en cybersécurité

Seuls **12,2%** des professionnels exerçant dans une structure spécialisée en cybersécurité **sont des femmes.**

4

15,7% des profils sont des consultants en cybersécurité

C'est le métier le plus représenté. Suivi par les **RSSI** (12,4%), **Architectes cybersécurité** (6%) et **Auditeurs cybersécurité** (5,7%).

5

90% des répondants sont en CDI, ou sont fonctionnaires

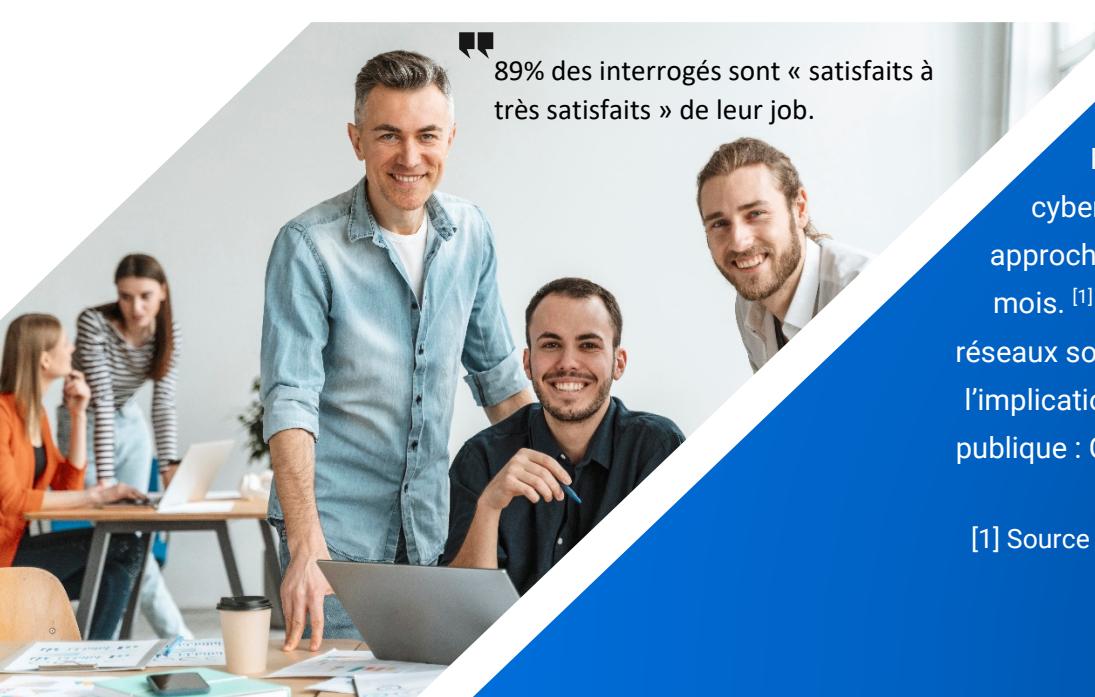
L'Île-de-France concentre **plus de la moitié** des professionnels. + de 50% des profils travaillent dans une société de **+1000 salariés.**

6

56% ont été recrutés via le « marché caché » (hors offre d'emploi)

Le marché caché représente les recrutements à la suite de **recommandations, candidatures spontanées ou approches directes.**

89% des interrogés sont « satisfaits à très satisfaits » de leur job.



Près de 8 professionnels de la cybersécurité sur 10 déclarent être approchés par des recruteurs tous les mois. ^[1] Cela montre l'importance des réseaux sociaux (comme LinkedIn) et de l'implication dans des projets à visibilité publique : Github, Blog, Site/Forum, etc...

[1] Source – Zdnet « *la crise du recrutement ne s'arrange pas* »

LES METIERS DE LA CYBERSÉCURITÉ



Conscient de l'utilité de la cybersécurité, le gouvernement français à l'intention de mettre les moyens pour développer les formations et les aides envers la cybersécurité

Le [panorama des métiers de la cybersécurité](#) établit par l'ANSSI vise à offrir un référentiel des métiers de la cybersécurité. Ces derniers sont classés par thèmes et offrent une vision pour les recruteurs ainsi que pour les candidats désirant faire carrière dans le domaine. Voici le résumé de ces thèmes.

Gestion de la sécurité et pilotage des projets de sécurité

Principaux métiers : Directeur cybersécurité, responsable de projet, Responsable de la Sécurité des Systèmes d'Information (RSSI).

Gestion des incidents et des crises de sécurité

Principaux métiers : Opérateur et Analyste SOC, Responsable CSIRT, Analyste réponse à incident, gestion de crise, analyste de la menace.

Métiers annexes

La catégorie des métiers annexes est très large. Il s'agit notamment des **métiers juridiques** (Data Protection Officer), de **gestion des risques, cyberpolice, développement**, et toutes les activités en tant qu'**indépendant(e)**.

Conception et maintien d'un SI sécurisé

Principaux métiers : Architecte sécurité, Développeur sécurité, cryptologue, auditeur sécurité (ou pentester), administrateur de solutions en sécurité.

Conseil, services et recherche dans la cybersécurité

Principaux métiers : Consultant cybersécurité, formateur cybersécurité, développeur/intégrateur de solutions cybersécurité, chercheur en sécurité.

Pour plus d'informations sur les métiers de la cybersécurité, visionnez la vidéo complète sur YouTube :
<https://youtu.be/W8GNMNQn2Fo>



100 OFFRES D'EMPLOI ANALYSÉES



Les postes analysés concernaient tous les domaines de la **cybersécurité** mais aussi toutes régions, profils et diplômes confondus. [Retrouvez la vidéo complète sur YouTube](#). Voici les compétences les plus recherchées par les employeurs, triées selon le pourcentage d'offres d'emploi les mentionnant.



LES COMPÉTENCES TECHNIQUES LES PLUS RECHERCHÉES (hard skills)

1 61% : Les Réseaux informatiques

Les compétences réseaux les plus demandées sont TCP/IP, réseau Wi-Fi, Pare-feu et Dénis de service.

2 37% : Pentest et hacking éthique

Compétences en audit, assistance et prévention contre les menaces et malwares. Et exploitation de vulnérabilités.

3 35% : Analyse et gestion des risques

La méthode EBIOS est souvent citée, et des connaissances en Politique de sécurité et RGPD.

4 32% : Systèmes d'exploitation

Linux/Windows principalement, et mentions pour « active directory » ainsi que la « virtualisation ».

5 25% : Compétences dans les SOC et CERT

Opération, amélioration et mise en place ainsi que gestion d'incident et de crise.

Notamment les normes ISO 2700X ainsi que PCI-DSS ou encore les référentiels ANSSI.

7 22% : Programmation

Les langages de programmation les plus cités sont Python, le langage C, Powershell, bash et les langages web.

8 15% : Conseil et consulting

Principalement des conseils et recommandations internes, mais aussi pour des clients externes.

9 13% : RGPD / DPO

Mise en conformité, assistance et audits. Le côté juridique gagne du terrain au fil des années.

100 OFFRES D'EMPLOI ANALYSÉES (suite)



LES COMPÉTENCES NON TECHNIQUES LES PLUS RECHERCHÉES (soft skills)

1 52% : L'anglais

Un niveau d'anglais dit « technique » et/ou un « bon niveau » et le plus souhaité.

2 38% : L'autonomie

Autonomie « relationnelle » qui sous-entend que le candidat ne sera « pas seul devant son écran ».

3 35% : La rigueur

Une rigueur avec « réactivité et méthodologie » pour être efficace si la situation l'exige.

4 26% : La curiosité

Tout en étant « force de proposition » et « à l'écoute » des besoins.

5 22% : La veille

Une veille à la fois stratégique, réglementaire et technique comme l'exige le domaine.

6 21% : Le travail en équipe

Savoir travailler en équipe et pouvoir également « partager les connaissances ».

7 20% : Esprit d'analyse et de synthèse

Notamment pour « accompagner » les collaborateurs et clients.

8 16% : Expression orale et écrite

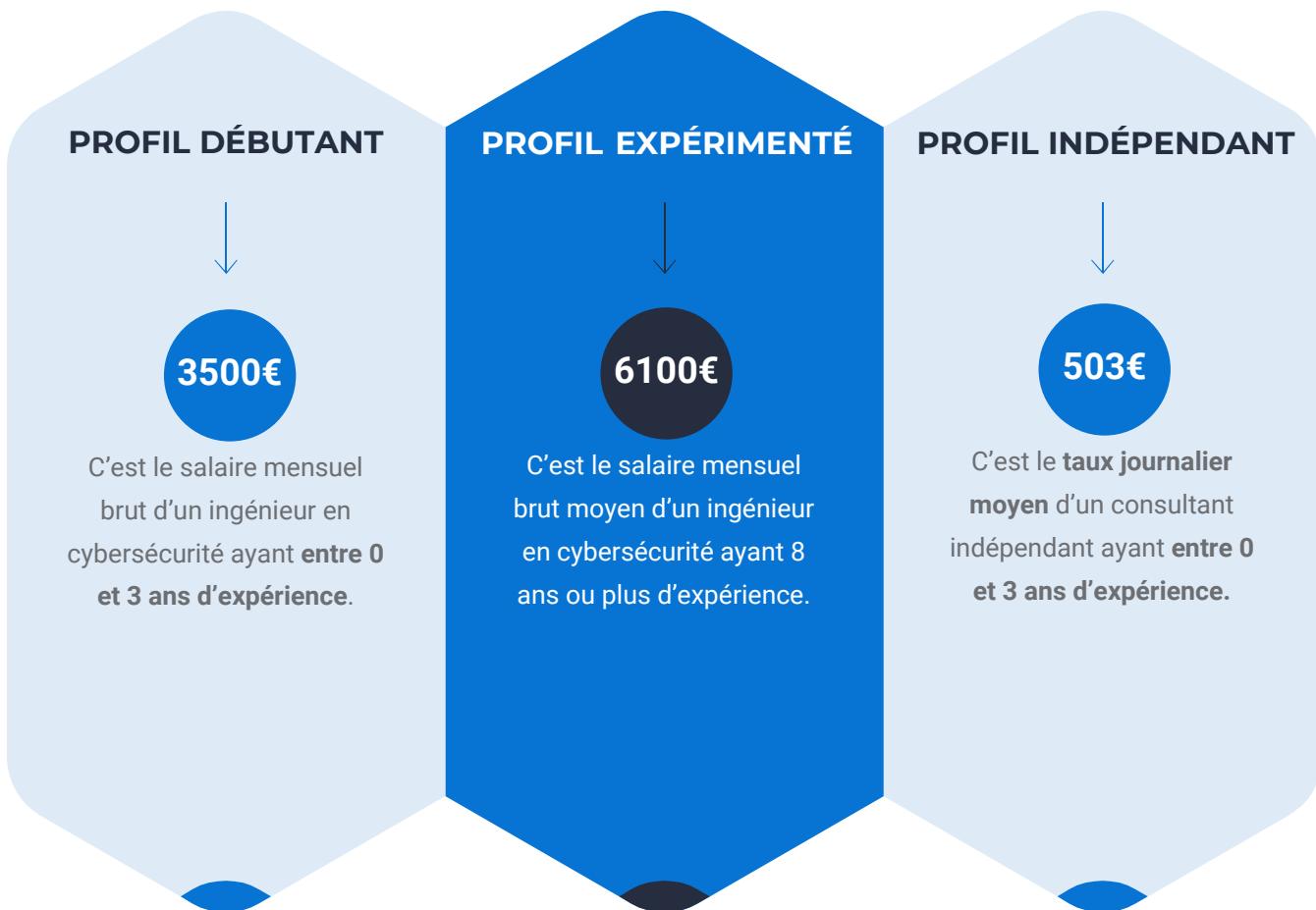
Le terme « Aisance relationnelle » est particulièrement utilisé.

TABLEAU DES MOTS-CLÉS LES PLUS COURANTS DANS LES OFFRES D'EMPLOI

Sécurité, 251	Développement, 54	Données, 37	Analyse, 29	Vulnérabilités, 19
Cyber, 90	Experience, 53	Technologies, 35	Veille, 27	Conformité, 18
Reseaux, 81	Risques, 52	Projets, 32	Incidents, 25	ISO, 17
Connaissance, 84	Informatique, 50	Outils, 32	SOC, 22	Menaces, 16
Compétence, 74	Equipe, 47	Architecture, 32	SIEM, 22	Curieux, 15
Cybersécurité, 64	Gestion, 46	Autonome, 30	Windows, 21	Cloud, 14
Systèmes, 62	Anglais, 45	Missions, 30	Linux, 20	Audit, 14
Technique, 61	Formation, 43	Clients, 29	Relationnel, 19	Python, 11

DES SALAIRES ATTRACTIFS

Les domaines de l'IT sont parmi les mieux payés. Ces salaires sont basés sur [l'étude des rémunérations nationales](#) 2022 par le cabinet de recrutement **Hays**.



Les fonctions IT dédiées à la sécurisation des données sont fortement recherchées.

LE CHIFFRE MARQUANT DE L'ANSSI

Dans son panorama de la menace informatique, l'ANSSI dévoile une augmentation de 37 % des intrusions avérées dans les systèmes d'information entre 2020 et 2021. Chiffre qui ne cesse d'augmenter.

3 étapes pour TROUVER le Métier qui VOUS correspond

1

METTEZ DE CÔTÉ LES PRÉJUGÉS

Peu importe votre profil, diplôme ou âge actuel, il est possible de vous former, de vous reconvertis ou d'ajouter des compétences fondamentales à votre parcours professionnel. Les métiers de demain n'existent pas encore et **les formations universitaires n'enseignent pas** (ou très peu) la cybersécurité. **Vous n'êtes donc pas en retard.** La passion pour le domaine et votre implication dans celui-ci sera plus déterminante qu'un parcours scolaire passé. **Tous les voyants sont au vert en cybersécurité**, et pendant encore de nombreuses années. La pénurie mondiale le prouve à elle seule. Il faut donc penser à l'avenir et prendre la situation comme une vraie **opportunité**.

2

TROUVEZ VOTRE VOIE

Identifiez d'abord le ou les domaine(s) de la cybersécurité **qui vous paraissent pertinents** : le réseau, le développement, le pentesting, le côté juridique ou autre. **Cela définira votre objectif global.** À partir de ce moment, vous pouvez le séparer en plusieurs **sous-objectifs**. Par exemple, pour évoluer dans la sécurité des réseaux, vous pouvez commencer par apprendre **le modèle OSI ou TCP/IP**. Vous pouvez prendre des cours sur **les adresses IP et les protocoles populaires**. Ce n'est qu'après que vous apprendrez à attaquer et à défendre les systèmes. Un hacker est avant tout un grand connaisseur des détails techniques.

3

CHERCHEZ ET APPRENEZ !

Une fois vos objectifs listés, même si vous ne les pensez pas parfaits : **cherchez un maximum de ressources pour acquérir des compétences et formez-vous sans attendre.** Même si vous changez d'objectifs par la suite, vos compétences acquises ne seront jamais inutiles. Dans les pages suivantes vous découvrirez d'autres conseils à suivre ainsi qu'une **carte mentale à télécharger** pour vous aider à définir vos objectifs selon les grands domaines de la cybersécurité.



5 CONSEILS POUR AMÉLIORER VOTRE EMPLOYABILITÉ

1. SURFEZ SUR LA TENDANCE

Les métiers du numérique sont en évolution constante : Délégué à la protection des données, IOT developer, ingénieur en IA, sécurité Cloud... sont des métiers qui n'existaient pas il y a 5 ou 10 ans. [Une étude affirme que 85% des emplois de 2030 n'existent pas encore aujourd'hui](#). S'intéresser dès maintenant à la sécurité **des technologies d'avenir** : blockchain, métavers, bio-informatique ou encore intelligence artificielle, c'est s'assurer un métier futur.

2. FORMEZ-VOUS À VIE

La cybersécurité est l'un des domaines les plus **évolutifs et dynamiques**. La transversalité du domaine à toute l'informatique, et l'application systématique aux nouvelles technologies **permet à chacun de trouver sa place**. La cybersécurité requiert une mise à jour constante des compétences. La formation se fait ainsi sur le long terme, et l'idéal est donc de commencer **aujourd'hui**. Vous trouverez sur la page suivante des conseils pour commencer.

3. LISEZ (BIEN) LES OFFRES D'EMPLOI

Vous pourrez y trouver des postes inconnus auparavant, mais surtout vous y trouverez ce que les recruteurs attendent du côté technique ou non. Ne soyez pas découragé si un diplôme d'ingénieur semble requis, vous pouvez parfois postuler **avec un profil alternatif**. [Face à la pénurie de talents, les recruteurs s'ouvrent à de nouveaux profils](#). Rappelez-vous que **56% des profils sont recrutés par le « marché caché » (hors offre d'emploi)** en cybersécurité.

4. METTEZ EN PLACE DES PROJETS PROFESSIONNELS

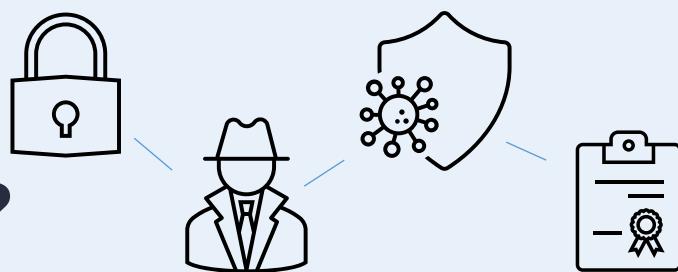
Cela vous aide à apprendre par la pratique, et fortifiera votre profil pour candidater. Votre ou vos projet(s) doivent si possible s'aligner avec vos buts. [Vous trouverez beaucoup d'idée de projets cybersécurité sur Internet](#).

5. AYEZ L'ÉTAT D'ESPRIT « HACKER » !

Les métiers de la cybersécurité sont prisés et passionnantes, mais ils ne sont pas forcément faits pour tout le monde. **Un hacker a soif de connaissances et de défis**. Cela implique de ne pas abandonner face aux problèmes et d'oser passer des heures à la recherche d'une solution. Le recruteur cherchera à s'assurer que le candidat dispose d'un tel état d'esprit. Il n'y a aucun mal à être débutant(e). Tout le monde l'est un jour, y compris les milliers de personnes qui se reconvertisse chaque année. Évidemment, **la meilleure façon de commencer est de suivre un plan et de faire certifier ensuite les compétences acquises**.

[C'est précisément le but des formations cybersécurité certifiantes sur Cyberini](#)

PAR OÙ COMMENCER ?



PAR OÙ COMMENCER EN HACKING ÉTHIQUE

- Voici la [carte mentale qui regroupe tous les domaines et sous-domaines qui composent le hacking éthique.](#)
- Vous pouvez également suivre du contenu gratuit d'introduction au domaine sur Cyberini : [créer un compte Cyberini gratuitement.](#)
- Vous pouvez visionner la vidéo dédiée : [Par où commencer en HACKING.](#)
- Vous pouvez obtenir une [certification cybersécurité reconnue par l'État sur Cyberini](#) (100% finançable) pour faire valider vos compétences.

3 CONSEILS pour RÉUSSIR VOTRE RECONVERSION

- ✓ Vos expériences professionnelles actuelles **comptent** même si elles ne sont pas techniques : vous n'avez pas « perdu du temps » ! Il s'agit notamment des compétences en travail d'équipe, gestion du temps, etc.
- ✓ Vous pouvez déjà monter en compétences en lien avec la cybersécurité dans **votre travail actuel (si cela est possible)**.
- ✓ Des projets (professionnels ou personnels) et **une formation certifiante** sont **vos meilleurs alliés**.

 À l'avenir, nous changerons 6 à 7 fois de métier au cours de notre vie professionnelle.

- Carine SEILER, haut-commissaire aux compétences



LES CONSEILS EN VIDÉO

Pour en savoir plus, suivez la vidéo « Réussir sa reconversion en cybersécurité » à travers le lien suivant :

https://www.youtube.com/watch?v=G8u1i_2bA3g







TIRER PARTI DU MARCHÉ CACHÉ

Le marché caché représente **56% des recrutements en cybersécurité** selon le sondage de l'ANSSI cité au début de ce document. Les recruteurs partent souvent à la recherche de profils qu'ils jugent pertinents avant même de publier des offres d'emploi. Voici donc comment **placer votre profil devant leurs yeux**.

1. Vous devez vous constituer une **présence sur les réseaux sociaux**. Notamment les réseaux sociaux professionnels et ceux permettent de créer du contenu : **LinkedIn, YouTube, TikTok**.
2. Vous devez **mettre en avant vos projets/portfolios**. Par exemple un compte **Github**, un **site personnel**, un badge **CTF** (Capture The Flag). [Cyberini vous propose une plateforme CTF guidée pour vous entraîner](#). Libre à vous de montrer tout ce qui est pertinent sur votre CV et qui démontre une expérience **en pratique**. Vous pouvez créer votre portfolio grâce à divers sites. [Voici la vidéo YouTube complète pour créer votre portfolio](#) et voici [les 3 étapes pour faire carrière en vidéo](#).
3. Vous devez **participer à la communauté**. Rejoignez des groupes de **discussions** (**les candidats Cyberini disposent d'un serveur Discord privé**), **suivez des entreprises**, répondez à leurs sondages, etc. Vous connecter avec d'autres personnes dans le domaine va automatiquement mettre en avant **votre profil** (et vous rendre plus humain qu'un « simple » CV).

Récupérez des cartes de visite

Les cartes de visite permettent d'entrer en contact direct avec un recruteur.

Au-delà de la connexion **physique** établie avec votre interlocuteur, vous obtenez un moyen rapide de le contacter ensuite. Des salons de recrutement ou autres événements nationaux et internationaux sont ainsi des opportunités : FIC, NDH, HIP...



Au-delà de la cybersécurité, on estime qu'environ 70% des offres d'emploi sont diffusées dans le marché caché.
Astuce : il ne faut pas hésiter à miser sur les candidatures spontanées et à varier les postes recherchés : la cybersécurité est souvent transversale !



Comme pour un CV, le fond compte autant que la forme ! Le fond de votre profil sont vos compétences acquises durant votre formation. La forme est quant à elle la mise en avant sur Internet de vos compétences. Cela compte beaucoup dans « l'expérience » que les entreprises recherchent dans leurs offres d'emploi.





Formations cybersécurité en ligne :

COMMENT FAIRE LES BONS CHOIX ?



Comment trouver un organisme de formation fiable ?

Un organisme de formation doit disposer d'un **numéro de déclaration d'activité** impliquant un formalisme strict et un bilan pédagogique et financier annuel. De plus, et notamment pour prétendre aux financements publics, un organisme de formation doit être **certifié Qualiopi®**. Pour cela il doit passer des audits réguliers certifiants la **qualité** de ses formations. Enfin, il convient de vérifier si l'organisme est bien **spécialisé et approuvé** dans le domaine.

→ Cyberini est un organisme de formation certifié Qualiopi® depuis avril 2021 et membre de l'Alliance pour la Confiance Numérique (ACN). La formation est labellisée « SecNumedu-FC » par l'ANSSI.

Comment savoir si je pourrais trouver un travail ensuite ?

Il est tout à fait possible de travailler dans la cybersécurité après une formation en ligne. Mais en réalité, trouver un travail dépend de plusieurs facteurs **externes** : votre profil, les tâches demandées, le recruteur concerné, la concurrence, etc... Aucun diplôme, y compris universitaire, ne peut donc garantir un emploi en tant que tel.

→ Cyberini vous garantit cependant, [avis et interviews](#) à l'appui, que votre employabilité sera grandement améliorée. La plupart de nos candidats obtiennent un travail dans le domaine à court ou moyen terme.



Comment savoir si une formation est adaptée à ma situation/mes buts ?

Vous pouvez demander un devis et le programme de formation à un organisme. Le programme peut être modifié selon vos besoins : durée, contenu, support... En passant, n'hésitez pas à demander les possibilités de financement vous concernant.

→ Cyberini vous permet d'apprendre à votre rythme à 100% en ligne et sans limite de temps. La formation est financable (CPF, Pôle emploi, employeur, région, etc).

À PROPOS DE Cyberin



2% TERMINÉ

Leçon Précédente Marquer comme Terminé ✓

Metasploit en pratique (exploitation d'une vulnérabilité dans Metasploitable) EN COURS

Leçon Ressources Additionnelles

The screenshot shows the Metasploit Framework's exploit selection screen. The user has selected the 'msf5' exploit for 'vsftpd'. The interface displays a list of matching modules, including 'exploit/unix/ftp/vsftpd_234_backdoor'. A progress bar at the bottom indicates the video is 02:10 minutes long.

Vous saurez comment prendre le contrôle de votre machine Metasploitable à l'aide d'un service vulnérable. Et vous apprendrez à protéger vos systèmes d'exploitation.

[Plus d'informations](https://metasploit.com)



Michel KARTNER

Fondateur de Cyberini

Je suis formateur en cybersécurité depuis 2013 avec + de 100 000 étudiants suivant mes cours. Le but étant d'aider chacun à progresser depuis son niveau actuel. Le tout dans une bonne ambiance ! Je serais ravi de vous compter également parmi nous pour vous aider à atteindre VOS buts ☺



- [Accéder à la formation cybersécurité](#)
- [Plus d'informations sur Cyberini](#)
- [Avis et interviews d'anciens étudiants](#)
- [Télécharger le programme de formation](#)

- [Accéder à la formation cybersécurité](#)
 - [Plus d'informations sur Cyberini](#)
 - [Avis et interviews d'anciens étudiants](#)
 - [Télécharger le programme de formation](#)



Ils se sont **formés**, ils se sont **reconvertis**
Et ils **témoignent**

Et vous, quelle sera VOTRE
success story ?



Thomas TREDEZ
Administrateur sécurité

J'ai décroché un poste d'administrateur sécurité au sein d'une ESN basé à Nantes et je suis en poste à Niort dans la cybersécurité.



Maziar Zenderhoudi
Chargé gouvernance EBIOS

J'ai postulé spontanément chez une société Montpelliéraise spécialisée en SI et Cyber sécurité, qui m'a répondu pour un poste de chargé de mise en place gouvernance - EBIOS.



Augustin De Solère
Coordinateur Cybersécurité

J'ai trouvé une alternance en tant que Coordinateur Cybersécurité dans une grande banque ! Encore merci pour votre excellente formation



LE MESSAGE DU FORMATEUR

Les formations universitaires dans l'informatique sont très pauvres en cybersécurité. Ce que je trouve scandaleux ! Les compétences ne dépendent pas nécessairement d'un diplôme et un(e) autodidacte a toutes ses chances de réussite. Nos étudiants le prouvent...

— Michel KARTNER

RETROUVEZ-NOUS SUR CYBERINI !



ET BIEN D'AUTRES L'ONT FAIT 1

Les étudiants Cyberini apprennent pendant des mois (et aussi longtemps qu'ils le souhaitent).

Les objectifs à court ou moyen terme sont propres à chacun, mais la plupart font carrière en tant que salariés par la suite, ou en tant qu'indépendants.

Les scores finaux aux examens de certification sont parmi les plus élevés du marché, avec un taux de réussite de 100% tout simplement !

 **Victor Cavalcante**
IT, Digital, Data Privacy & Cybersecurity Legal Counsel
5 mois · Modifié

Un grand merci à **Michel Kartner** pour faire la pédagogie nécessaire autour de la cybersécurité, en la rendant accessible à des professionnels de tous bords.

Avec la formation « Hacking Ethique : le cours complet assurée par **Cyberini**, Michel nous met rapidement dans la peau des attaquants, en présentant les bons outils et réflexes à retenir pour contrer efficacement les menaces : systèmes d'information et empêcher les violations de données de nos clients et employeurs.

Cours à haute valeur ajoutée aux informaticiens bien entendu, mais également aux juristes et DPOs, car permettant développer des compétences techniques complémentaires à celles organisationnelles dont nous sommes habituées.



 **Jérôme Spaeter**
Développeur junior/étudiant Full Stack
1 mois

Certification Cybersécurité TOSA obtenue au niveau Expert (900/1000 pts)

Un grand merci à **Michel Kartner** et sa société **Cyberini** pour votre accompagnement et votre expertise, c'est une formation de grande qualité qui a largement été à la hauteur de mes espérances !

#cybersecurite #certification #hacking

 **Eddy Audrain**
Backend Technical Leader / DevSecOps chez EMOTIC
5 j

Je viens d'obtenir une nouvelle certification en Cybersécurité ! (avec un résultat de 90/100)

Merci à mon formateur **Michel Kartner** et son centre de formation **Cyberini**, grâce à qui j'ai pu décrocher cette certification !

CERTIFICATION
Tosa Cybersécurité

Nous soussignés, Marc Alpérovitch Président de la société Isograd, éditeur du Tosa et Clément Hammel, Responsable Pédagogique, certifions que :

Monsieur Jérôme Spaeter
a passé la Certification Tosa Cybersécurité, le 15 avril 2022 via le centre de passage Cyberini et a obtenu le score de 900/1000 points correspondant à un niveau Expert.

CLÉMENT HAMMEL
RESPONSABLE PÉDAGOGIQUE 

MARC ALPÉROVITCH
LE PRÉSIDENT 

 Certificat n° : 2304EDDAUD570
Date d'obtention : 25/04/2023
Eddy AUDRAIN a obtenu le certificat

Elaborer et mettre en oeuvre une démarche de cybersécurité

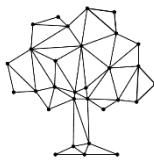
Certification enregistrée au Répertoire Spécifique des Certifications et Habilitations nr. 5322
Compétence(s) validé(s) :
Placer la gouvernance de la cybersécurité, gérer les systèmes d'information sécurisés, gérer les risques et protection des systèmes, évaluer le niveau de sécurité, gérer les incidents de cybersécurité.
Remis le 25/04/2023 par
Michèle ELBAZ représentante légale de ESIC.

12 · 2 commentaires

Retrouvez encore plus d'avis, de débouchés et d'interviews d'étudiants sur [la page suivante](#).



[Voir les formations](#)



SecNumedu
Formation continue

ANSSI

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

Cybe ini

ACTIVATEUR



FRANCE NUM

TOSA® Centre Agréé

ACN
Alliance pour la confiance numérique

CONTACT



Cyberini (Michel KARTNER)
128 rue la Boétie, 75008 Paris
SIRET : 79333268500023



+33 6 98 67 93 92



support@cyberini.com
<https://cyberini.com>

Cyberini est un organisme de formation enregistré sous le numéro 11756144875 auprès du préfet de région d'Ile-de-France. Cet enregistrement ne vaut pas agrément de l'Etat.