[FICHE MÉTIER]

Expert Cybersécurité

Emplois salariés dans la filière en 2022*

200

Le poste d'ingénieur cybersécurité est souvent externalisé.

18 % de femmes

16 % de salariés + 55 ans

Evolution quantitative à horizon 2030

-- - = + ++

340 emplois
estimation 2030

Transformation qualitative du métier

\+ ++ +++

* Filière des gaz, de la chaleur et des solutions énergétiques.

FINALITÉS DU MÉTIER

Évaluer les vulnérabilités des systèmes informatiques.

Mettre en place une veille sur la sécurité informatique et initier des stratégies de prévention.

Mener des actions curatives et gérer les incidents après intrusions ou dysfonctionnements.

LES 4 ENJEUX D'ÉVOLUTION À HORIZON 2030

1 LA CYBERSÉCURITÉ AU CŒUR DU SYSTÈME ÉNERGÉTIQUE

Les ingénieur cybersécurité sont les garants de la stabilité du réseau énergétique comme de la protection des données clients / utilisateurs en aval de la filière.

Le nombre de cyber attaques est en augmentation constante et cette tendance devrait perdurer, avec une sophistication de la menace.

L'énergie est un service essentiel, placé critique par les directives européennes sur la sécurité informatique (ex : NIS 2 en 2023). La conformité règlementaire restera centrale à l'avenir.

Ce profil (internalisé ou externalisé) va ainsi connaitre une forte demande couplée à une technicité accrue.

2 LES ENJEUX DE SÉCURITÉ D'UN RÉSEAU DÉCENTRALISÉ

Le système énergétique Gaz est transnational. De plus, l'intégration des énergies vertes le font évoluer vers un réseau plus décentralisé.

Les risques de sécurité informatique augmentent en ce sens. Il s'agira d'assurer la sécurité et la stabilité d'un réseau qui demande une coordination transnationale, et avec des acteurs de plus en plus interdépendants sur les activités production, transport, stockage...

Les métiers de la cybersécurité devront redoubler de vigilance afin que chaque opérateur (particulier ou entreprise) soit au niveau de sécurité requise.

3 LES RISQUES LIÉS À LA TRANSFORMATION NUMÉRIQUE

L'arrivée massive de l'IA générative mais aussi le recours à l'Internet des objets, à la Blockchain ou au Metavers, génèrent de nouveaux défis pour la filière Gaz. L'enjeu majeur est de faire face à une cybercriminalité maitrisant aussi ces nouvelles technologies.

Tous ces facteurs prônent une gestion rigoureuse et revisitée des risques.

Le niveau d'accessibilité / confidentialité des données, les tests de pénétration, les risques liés à la chaine logistique informatique... seront donc réévalués vers une nouvelle architecture de sécurité.

4 L'IMPORTANCE DE LA VEILLE ET DE LA PÉDAGOGIE

On peut faire un parallèle entre la mise à niveau informatique d'un système et la nécessité de veille technologique et juridique de ces métiers en cybersécurité. Pour ces profils les connaissances évoluent en permanence. La curiosité, le questionnement, l'adaptabilité seront toujours plus sollicités.

Les aptitudes pédagogiques, notamment à transmettre aux utilisateurs les bonnes pratiques et les mesures de sécurité, deviennent incontournables.

Le conseil aux équipes opérationnelles va aussi s'intensifier afin de conférer à celles-ci plus de capacités à prévenir ou à réagir.

MISSIONS ET ACTIVITÉS CLÉS

Concevoir, déployer et gérer des solutions de sécurité (pare-feu, antivirus, détection d'intrusion, etc.)

Surveiller les activités dans les systèmes, les réseaux, les applications informatiques et identifier les failles de sécurité (test de pénétration, etc.)

Réagir calmement aux incidents de sécurité, investiguer les violations et mettre en place des mesures correctives

Sensibiliser les utilisateurs en matière de sécurité informatique

Être le garant de la conformité règlementaire en matière de cybersécurité

Assurer un bon niveau de Compréhension et de communication des renseignements sur les menaces en termes de cybersécurité dans l'ensemble de l'organisation.

L'ÉVOLUTION DES COMPÉTENCES À HORIZON 2030

COMPÉTENCES TECHNIQUES*

- Maitrise des logiciels et solutions de sécurité web, d'amélioration de performance des systèmes, de correction des vulnérabilités, etc.
- Connaissance en codage (Python, C.perl, Lisp, etc.)
- Connaissance des solutions de protection des données personnelles clients ou utilisateurs et des techniques de Rançonlogiciel, attaques DDoS, Hammeçonnage, Piratage, etc.
- Connaissance des SI de types industriels (activités de production, stockage, distribution énergétique)
- Maitrise des règlementations en vigueur (NIS1, NIS2, RGPD, etc.)

- Compréhension des architectures « cloud » et des risques associés (chaine logistique informatique)
- Maitrise des modèles d'intelligence artificielle et de « machine learning » pour automatiser les tâches et augmenter la protection
- Capacité à sécuriser les réseaux IoT et les protocoles de communication
- Connaissance des SI Smart Grids et des solutions pour augmenter la sécurité à chaque acteur du réseau
- Capacité d'indentification et de prévention des failles de sécurité dans les systèmes blockchain

*A noter : Cette liste de compétences techniques donne une vision globale des besoins en compétences. Suivant les besoins des organisations et les projets associés, certaines de ces compétences seront mises en avant.

COMPÉTENCES COMPORTEMENTALES

- Maîtrise de l'anglais obligatoire
- Sens du diagnostic, d'analyse et de synthèse
- Curiosité et adaptabilité, goût pour la veille
- Capacité de résolution de problème et d'inventivité
- Sens du travail en équipe, notamment avec des équipes pluridisciplinaires
- Sens de la pédagogie et de la sensibilisation
- Rédaction des spécifications techniques des solutions de sécurité
- Capacité d'adaptation et maintien du calme dans les situations de forte pression
- Capacité à communiquer auprès de non experts du domaine

- Ingénierie de solutions cybersécurité complexes, vision globale des risques et des solutions
- Sens de la communication
- Conseil et vulgarisation des connaissances et des actualités cybersécurité auprès de différents utilisateurs (prestataires, direction, etc.)
- Aptitudes à la négociation avec des prestaires et sous-traitants en sécurité informatique (ESN)

Légende :
Compétences nouvelles — Compétences à renforcer

QUELLES COMPÉTENCES DANS LES OFFRES D'EMPLOIS ? ZOOM SUR LE MARCHÉ DU TRAVAIL SUR LES 4 DERNIÈRES ANNÉES

- **L'agilité digitale** est au cœur de ce métier. Sa récurrence – présente dans +55 % des offres d'emploi depuis 4 ans – démontre la technicité ainsi que l'appétence à la veille technologique intrinsèques à ces profils.
- Autres compétences incontournables, **l'analyse et la résolution de problèmes** recherchées dans 50 % des offres d'emplois. Ces aptitudes de recherche curative ou préventive de failles et de conception des solutions de sécurité s'exercent dans des environnements et systèmes qui se complexifient. La capacité à être autonome (36 %) ainsi que **force de proposition** (24 %) vient compléter ces profils analytiques.
- Les compétences relationnelles font aussi partie des compétences les plus demandées sur ce poste : **travail en équipe** et **communication** (autour de 35 % des offres d'emplois)
- Des compétences en **relation commerciale** (54 %), **orientation client** (24 %), **orientation qualité** (33 %) sont aussi très présentes, notamment en lien avec les postes d'ingénieur cybersécurité en ESN.

LES FORMATIONS*

Formations initiales

Bac+5

- Master Informatique avec spécialisation en sécurité informatique
- Master Recherche en Cybersécurité
- Diplôme d'Ingénieur en Cybersécurité
- Diplôme d'Ingénieur en Sécurité des SI

Écoles

Télécom Paris , M2i, ENSIIE, Institut Mines-Télécom, ESIEA, Université de Technologie Troyes, EC-Council Certified Ethical Hacker, CyberUniversity, etc.

Formations continues

Bac + 5

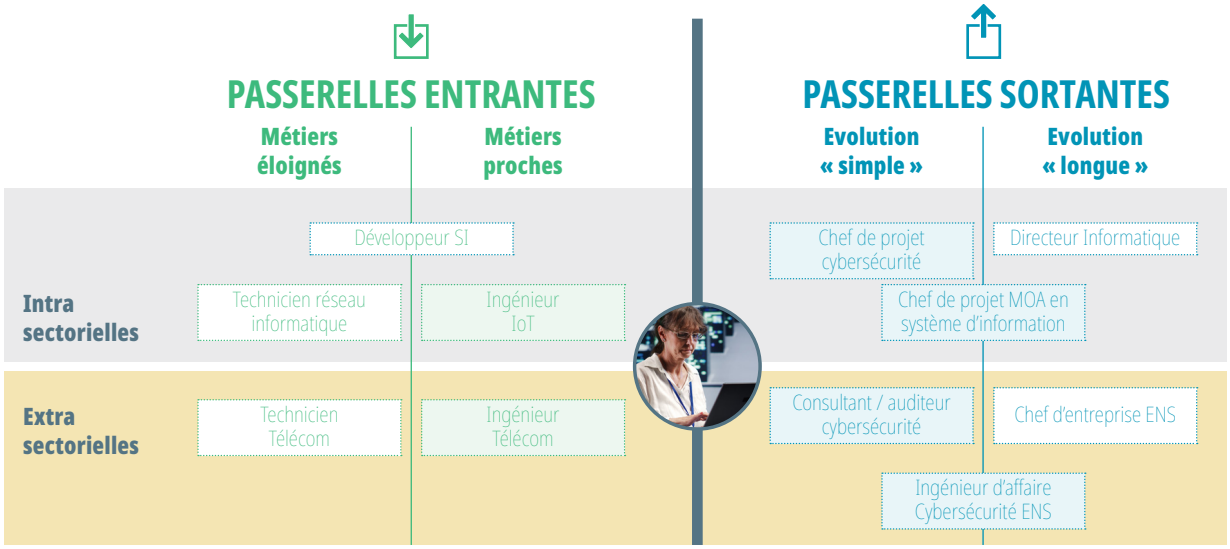
Master Pro Sécurité des Systèmes d'Information

Certifications

- (CISSP) : Certification internationale en cybersécurité.
- (CEH) : Certification pour les professionnels de la sécurité éthique.
- (CISM) : Certification pour la gestion de la sécurité des systèmes d'information.

* Nous présentons ici des exemples de formation les plus courantes.

LES PASSERELLES MÉTIER EXPERT CYBERSÉCURITÉ



FACTEURS DE TENSION

En 2022, ce poste est déjà très recherché avec plus de 15 000 offres d'emplois par an, dont une soixantaine d'offres dédiées à la filière et cette tendance va s'accentuer. Il est souvent externalisé dans des Entreprises du Services Numériques (ESN) généralistes ou spécialisées en cybersécurité.

Même si en volume ce n'est pas un métier prépondérant, l'ingénieur cybersécurité a un rôle stratégique au sein de chacun des maillons de cette filière. Ce qui rend son recrutement d'autant plus sensible. Le marché du travail étant concurrentiel et les compétences très pointues ainsi que régulièrement revisitées

L'évolution technologique et les nouvelles cybermenaces renforceront les besoins en profils cybersécurité au sein du secteur énergétique, l'ensemble de la filière devra, pour être attractive, mettre en avant à la fois la variété des enjeux et des métiers en cybersécurité ainsi que les parcours proposés.