30/01/2026

Rapport Enquête métier & sur-soi

Ecole d’ingénieurs CESI

Maxime STOFFEL
TOTALENERGIES GLOBAL INFORMATION TECHNOLOGY SERVICES

Table des matières

1. INTRODUCTION

Dans un contexte mondial de plus en plus marqué par des cyberattaques et la numérisation croissante des infrastructures critiques, la cybersécurité industrielle s'impose comme un enjeu stratégique majeur. Les récentes attaques contre des infrastructures énergétiques, de transport ou de santé ont mis en lumière la vulnérabilité de nos systèmes de production face aux menaces cyber.

C'est dans ce contexte que le métier d'Industrial Cybersecurity Officer (Responsable cybersécurité industrielle) émerge comme un métier essentiel au sein des organisations. Positionnés à l'intersection entre les technologies opérationnelles (OT) et les systèmes d'information (IT), ces professionnels assurent la protection des actifs de production contre les cybermenaces, tout en garantissant la continuité opérationnelle des installations.

Cette enquête métier vise à mieux comprendre la réalité du métier en analysant les missions quotidiennes et l'environnement de travail. Elle permet aussi d'identifier les formations et les compétences nécessaires pour y accéder. Elle s'intéresse également aux perspectives d'évolution et aux tendances du marché de l'emploi, tout en mettant en évidence la contribution de ce métier aux enjeux du développement durable.

L'objectif de cette enquête est aussi de comprendre le rôle de l'ingénieur au sein de l'entreprise et de la société : sa posture, ses responsabilités, sa place dans la hiérarchie, et sa capacité à influencer des décisions qui dépassent la technique. En cybersécurité industrielle, l'ingénieur n'est pas uniquement un expert des normes ou des systèmes OT/IT ; il devient un acteur de confiance, garant de la résilience des infrastructures critiques, et un médiateur entre contraintes opérationnelles, exigences de sécurité, conformité réglementaire et enjeux sociétaux.

2. PORTRAIT DU MÉTIER

2.1 Définition et périmètre

L'Industrial Cybersecurity Officer est un professionnel chargé de protéger les systèmes industriels et les infrastructures critiques contre les cybermenaces. Contrairement à la cybersécurité informatique traditionnelle (IT), ce métier se concentre sur les technologies opérationnelles (OT) : automates, systèmes SCADA, réseaux industriels et équipements de production.

Le cœur de la mission consiste à garantir la sécurité, la disponibilité et l'intégrité des actifs de production tout au long de leur cycle de vie, depuis la phase de conception et construction jusqu'à l'exploitation quotidienne.

Dans la plupart des organisations industrielles, l'ingénieur s'insère dans une chaîne de décision où interagissent direction de projet, exploitation, maintenance, équipes IT, équipes OT, achats/fournisseurs. Sa capacité n'est pas qu'à identifier une vulnérabilité, mais dans sa capacité à faire adopter des mesures réalistes, compatibles avec les contraintes de production et les objectifs business.

2.2 Témoignages professionnels

Profil interrogé : Industrial Cybersecurity Officer Europe
Entreprise : TotalEnergies (Division Énergies Renouvelables)
Secteur : Production d'énergies renouvelables (éolien, solaire, hydraulique, biomasse)
Date de l'entretien : Janvier 2026

Profil interrogé : Consultant cybersécurité industrielle / OT (ESN spécialisée cybersécurité)
Entreprise : Entreprise de Services du Numérique (interventions multi-clients industriels)
Secteur : énergie, transport, industrie manufacturière
Date de l'entretien : Janvier 2026

2.2.1 Missions et activités quotidiennes

Au sein de TotalEnergies, le professionnel interrogé assure la cybersécurité des actifs de production d'énergies renouvelables sur l'ensemble du territoire européen. Son périmètre couvre toutes les phases du projet, de la construction des installations à leur exploitation opérationnelle. Les activités quotidiennes s'articulent autour de trois axes principaux :

Le suivi de projets : Il constitue une partie importante de l'activité. Il s'agit d'accompagner les équipes projet pour intégrer les exigences de cybersécurité dans les cahiers des charges, les architectures techniques et les processus opérationnels.

La participation aux appels d'offres : Le professionnel évalue les propositions des fournisseurs sous l'angle cybersécurité, analyse les risques associés aux solutions proposées et formule des recommandations pour sécuriser les équipements et systèmes avant leur déploiement.

Le suivi des réalisations fournisseurs : Assurer que les exigences de sécurité définies en amont sont effectivement respectées lors de l'installation et de la mise en service des équipements.

La part d'initiative dans ce métier est estimée à 70%, témoignant d'une forte autonomie.

2.2.2 Outils et méthodes de travail

Contrairement à ce que l'on pourrait imaginer pour un métier technique, les outils quotidiens restent relativement simples. Excel et une plateforme de Gestion Électronique des Documents (GED) constituent l'essentiel de son quotidien. Cela s'explique par la nature du métier, davantage orienté vers la gestion de projet, l'analyse de risques et la coordination que vers la technique pure.

2.2.3 Environnement et conditions de travail

Le professionnel est basé à Montpellier, avec un bon équilibre entre présence au bureau et télétravail. Il préfère notamment privilégier le présentiel pour favoriser les échanges et maintenir le lien social, sans pour autant exclure la flexibilité du travail à distance particulièrement le vendredi.

Les journées sont denses, avec une moyenne de 9 heures de travail quotidien. L'aspect « Europe » du poste implique des décalages horaires et une forte disponibilité: il n'est pas rare de répondre à des emails tard le soir pour communiquer avec des équipes situées dans d'autres fuseaux horaires.

Les déplacements sont fréquents. Un aller-retour mensuel à Paris pour se coordonner avec l'équipe centrale (composée de 2 personnes basées au siège), et environ deux audits annuels à l'étranger d'une semaine chacun.

Le statut de cadre au forfait jour offre une flexibilité horaire appréciée, permettant d'adapter son planning aux contraintes projet tout en préservant un équilibre vie professionnelle-vie personnelle satisfaisant.

2.2.4 Une dimension fortement collaborative

Le travail s'effectue en interaction constante avec de nombreux interlocuteurs : équipes techniques, chefs de projet, fournisseurs, partenaires internationaux. La communication avec l'équipe parisienne est quotidienne, ce qui garantit une coordination fluide et une cohérence des pratiques à l'échelle européenne.

2.2.5 Les atouts du métier

L'environnement multiculturel : Travailler avec des équipes de différentes nationalités, naviguer entre les contextes réglementaires européens et collaborer avec des partenaires internationaux enrichit considérablement l'expérience professionnelle.

La diversité des sujets traités : Le métier touche à de nombreuses dimensions : technique (réseaux, systèmes embarqués), réglementaire (conformité RGPD, SOX), organisationnelle (processus, gouvernance) et stratégique (analyse de risques, gestion de crise).

Enfin, la conscience géopolitique : Observer les évolutions des cybermenaces, comprendre les tensions internationales et leurs implications sur la sécurité des infrastructures critiques.

2.2.6 Les contraintes et défis

Comme tout métier à responsabilités, celui-ci comporte ses propres contraintes. La principale difficulté évoquée se trouve dans la dimension politique du poste. Faire comprendre les enjeux de cybersécurité à des interlocuteurs non techniques, comprendre et mettre en place les exigences de sécurité et contraintes opérationnelles.

Le métier est également décrit comme stressant, notamment en raison du timing serré des projets et de la pression liée à la gestion des failles de sécurité.

Cependant, les responsabilités ne sont pas jugées excessives et le métier permet de maintenir un équilibre de vie satisfaisant, ce qui constitue un point d'équilibre important pour la durabilité professionnelle.

3. PARCOURS ET ACCÈS AU MÉTIER

3.1 Profil du métier

Le métier d'Industrial Cybersecurity Officer est accessible principalement avec un diplôme de niveau Bac+5, idéalement issu d'une école d'ingénieurs ou d'un master universitaire spécialisé.

Le professionnel interrogé a suivi un parcours en réseaux et télécommunications avec une option cybersécurité, illustrant l'importance d'une base technique solide en systèmes et réseaux.

Ce qui est particulièrement intéressant, c'est la diversité des parcours possibles. Il n'est pas obligatoire d'avoir suivi une spécialisation en cybersécurité dès la formation initiale. Beaucoup de professionnels proviennent du domaine juridique, notamment de la gouvernance, de la gestion des risques et de la conformité (GRC).

3.2 Certifications professionnelles

Plusieurs certifications sont particulièrement valorisées :

Les certifications ISO :

- ISO 27001 : norme internationale sur le management de la sécurité de l'information. Elle définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (SMSI).
- ISO 27005 : dédiée à la gestion des risques en sécurité de l'information, elle fournit des lignes directrices pour l'analyse et le traitement des risques.

Les certifications spécifiques à la cybersécurité industrielle :

- IEC 62443 : norme internationale de référence pour la sécurité des systèmes d'automatisation et de contrôle industriels (IACS).
- EBIOS RM (Expression des Besoins et Identification des Objectifs de Sécurité - Risk Manager) : méthode d'analyse de risques développée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Les certifications généralistes en cybersécurité :

- CISSP (Certified Information Systems Security Professional) : certification reconnue mondialement, qui couvre l'ensemble des domaines de la sécurité de l'information.
- Secuarch : certification axée sur l'architecture de sécurité.

3.3 Compétences développées sur le terrain

Au-delà des diplômes et certifications, c'est sur le terrain qu'on apprend réellement. Le professionnel interrogé témoigne avoir développé des compétences qu'il ne possédait pas nécessairement au départ de sa carrière.

Parmi celles-ci, la maîtrise du RGPD (Règlement Général sur la Protection des Données) est devenu indispensable. En effet, il structure de nombreuses décisions en matière de sécurité des données personnelles et impacte directement les architectures systèmes.

De même, la loi SOX (Sarbanes-Oxley Act), réglementation financière américaine imposant des contrôles stricts sur les systèmes d'information, a dû être intégrée dans ses compétences.

3.4 Perspectives d'évolution

Le métier d'Industrial Cybersecurity Officer offre plusieurs possibilités d'évolution. La voie managériale est une possibilité, avec des possibilités de progression vers des postes de chef de service cybersécurité puis de directeur de la sécurité des systèmes d'information (DSSI ou CISO - Chief Information Security Officer).

3.5 Compétences clés pour réussir

- Systèmes et réseaux : comprendre les architectures réseaux, les protocoles (TCP/IP, Modbus, OPC-UA), l'administration système et les infrastructures cloud/on-premise.

- Développement : comprendre le développement logiciel aide à comprendre les vulnérabilités applicatives, à analyser du code et à dialoguer efficacement avec les équipes de développement.

- Analyse de risques : savoir identifier, évaluer et hiérarchiser les risques cyber est au cœur du métier.

- Gestion des vulnérabilités et audit : capacité à réaliser des audits de sécurité, à interpréter les résultats de tests d'intrusion.

Les compétences relationnelles sont tout aussi essentielles :

- Communication et compréhension : savoir vulgariser des concepts techniques pour des interlocuteurs non-spécialistes, rédiger des rapports clairs, présenter des analyses.

- Gestion des indicateurs : produire des tableaux de bord pertinents, suivre des indicateurs de performance de sécurité.

- Gestion de la pression : garder son sang-froid face à un incident de sécurité, prioriser efficacement, prendre des décisions rapides dans l'urgence.

3.6 Vision prospective

Interrogé sur l'évolution des compétences requises dans cinq ans, le professionnel estime que ça ne devrait pas beaucoup varier. Les bases techniques (réseaux, systèmes, sécurité) et les soft skills évoquées conserveront leur importance.

En revanche, la capacité à effectuer une veille technologique continue est une compétence de plus en plus essentielle. Dans un domaine où les menaces évoluent quotidiennement, où de nouvelles vulnérabilités sont découvertes quotidiennement et où les technologies se transforment rapidement (IA, IoT industriel, edge computing), rester informé devient primordiale.

3.7 Insertion professionnelle

Les offres d'emploi sont nombreuses et les entreprises peinent parfois à recruter des profils qualifiés.

Néanmoins, l'insertion n'est pas immédiate. Comme le souligne notre professionnel, "le plus compliqué est de faire les premières expériences et arriver à capitaliser dessus". Les employeurs recherchent des profils ayant déjà une première expérience terrain, créant un paradoxe classique pour les jeunes diplômés : comment acquérir de l'expérience si toutes les offres en exigent déjà ? Plusieurs stratégies permettent de contourner cet obstacle :

- Privilégier les stages de fin d'études significatifs dans des SOC (Security Operations Center) ou des équipes cybersécurité.
- Viser les ESN (Entreprises de Services du Numérique) spécialisées en cybersécurité qui recrutent des profils juniors pour les former.

Une fois la première expérience acquise et capitalisée, les portes s'ouvrent plus facilement et les opportunités d'évolution se multiplient.

4. ANALYSE DU MARCHE DE L'EMPLOI

4.1 Un secteur en forte croissance

Le marché de la cybersécurité connaît une forte croissance grâce transformation numérique des entreprises et l'augmentation des cyberattaques. Le rapprochement entre IT-OT pousse les industriels à recruter des experts capables de sécuriser leurs systèmes de production. Le renforcement réglementaire (NIS2, DORA, Cyber Resilience Act) et le contexte géopolitique tendu amplifient cette demande.

4.2 Analyse des offres d'emploi

L'analyse de deux offres représentatives illustre la diversité des opportunités, du débutant au confirmé.

OFFRE 1 : Consultant Cybersécurité Risques (Squad - Niveau confirmé)

- Profil : 2+ ans d'expérience GRC, Master/École d'ingénieur
- Missions : conseil multi-clients (banque, industrie, défense), gestion des risques, conformité réglementaire (DORA, NIST, LPM, PASSI), plans d'intervention incidents
- Compétences : normes de sécurité, communication/présentation, travail en équipe
- Environnement : ESN certifiée PASSI/LPM, déplacements fréquents missions client

OFFRE 2 : Cyber Security Intern (Willhire - Niveau débutant)

- Profil : Étudiant/diplômé récent en informatique, aucune expérience requise
- Missions : identification vulnérabilités, monitoring sécurité, support audits, documentation incidents
- Compétences : fondamentaux réseaux, Linux/Windows, scripting Python (bonus), frameworks ISO 27001/NIST
- Avantages : certificat, possibilité d'embauche (PPO)
- Rémunération : 18$/heure (~2 700€/mois temps plein)

Compétences systématiquement recherchées :

- Techniques : analyse de risques, normes (ISO 27001, NIST, IEC 62443), architectures réseau, outils SIEM
- Soft skills : communication/vulgarisation, travail en équipe, veille continue, gestion de la pression
- Exigences réglementaires récentes (DORA, NIS2, LPM)

4.3 Perspectives 5-10 ans

La demande devrait se développer avec l'augmentation des cyberattaques, l'IoT industriel et la transformation numérique. Les évolutions anticipées incluent une spécialisation (cloud, OT, IA security), l'automatisation et l'hybridation des profils (technique + business + juridique).

5. CONTRIBUTION DU MÉTIER AUX OBJECTIFS DE DÉVELOPPEMENT DURABLE (ODD)

5.1 Cybersécurité industrielle et durabilité des infrastructures

Le métier d'Industrial Cybersecurity Officer contribue directement à la robustesse des infrastructures industrielles, en garantissant leur disponibilité, leur intégrité et leur sûreté face aux cybermenaces. Dans un contexte où les installations industrielles sont de plus en plus numérisées et interconnectées, une cyberattaque peut entraîner des arrêts de production, des dommages matériels, voire des impacts environnementaux majeurs (pollution, gaspillage énergétique, accidents industriels).

En sécurisant les systèmes de contrôle industriels (SCADA, automates, réseaux OT), l'ingénieur en cybersécurité industrielle agit comme un responsable de la continuité des activités, ce qui s'inscrit pleinement dans une logique de développement durable. La prévention des incidents contribue à limiter les pertes de ressources, à éviter des reconstructions coûteuses et à prolonger la durée de vie des équipements industriels.

5.2 Contribution aux Objectifs de Développement Durable de l'ONU

La cybersécurité industrielle s'inscrit naturellement dans une logique de développement durable parce qu'elle vise à maintenir dans le temps des systèmes essentiels au fonctionnement de la société. Dans un environnement OT, une cyberattaque peut provoquer un arrêt de production, une dégradation matérielle, un incident de sûreté ou un impact environnemental. La contribution aux ODD se lit donc dans la prévention de ces ruptures, et dans la capacité à rendre la transformation numérique compatible avec la sécurité et la continuité.

Plusieurs Objectifs de Développement Durable (ODD) sont directement ou indirectement concernés par ce métier :

- ODD 7 – Énergie propre et d'un coût abordable

  Dans le cas étudié, l'Industrial Cybersecurity Officer intervient dans le secteur des énergies renouvelables. En protégeant les infrastructures de production d'énergie éolienne, solaire ou hydraulique, il contribue à garantir un approvisionnement énergétique fiable et sécurisé, condition indispensable à la transition énergétique.

- ODD 9 – Industrie, innovation et infrastructure

  La cybersécurité accompagne l'innovation technologique tout en assurant la robustesse des infrastructures critiques. Le rôle de l'ingénieur est ici de concilier transformation numérique et sécurité, afin de permettre une industrialisation durable et maîtrisée.

- ODD 13 – Lutte contre le changement climatique

  Une cyberattaque sur une infrastructure énergétique peut entraîner un recours temporaire à des moyens de production plus polluants ou des pertes d'efficacité énergétique. En sécurisant ces installations, le métier participe indirectement à la réduction de l'empreinte carbone et au maintien d'une production d'énergie durable.

- ODD 16 – Paix, justice et institutions efficaces

  Dans un contexte géopolitique tendu, les cyberattaques ciblant les infrastructures critiques sont devenues stratégique. L'Industrial Cybersecurity Officer participe à la protection des États et des entreprises contre ces menaces, renforçant ainsi la stabilité des institutions et la sécurité des citoyens.

5.3 Le rôle sociétal de l'ingénieur cybersécurité à l'horizon 2030

À l'horizon 2030, la cybersécurité industrielle met l'ingénieur face à une responsabilité, ses décisions ne protègent pas uniquement des données, mais des infrastructures essentielles au fonctionnement de la société. La posture de l'ingénieur devient donc éthique : il doit arbitrer entre sécurité, continuité d'activité, contraintes budgétaires, exigences réglementaires et impact environnemental.

L'ingénieur doit être capable d'identifier ce qui réduit réellement le risque, de prioriser les mesures selon les conséquences possibles, et d'anticiper les effets indirects.

Enfin, l'ingénieur cybersécurité industriel a une responsabilité de pédagogie. Il doit sensibiliser les équipes métiers et opérationnelles, construire une culture de sécurité, et faire accepter des exigences parfois perçues comme contraignantes. Cette capacité à influencer, convaincre et coopérer devient aussi importante que l'expertise technique.

6. MISE EN PERSPECTIVE AU-DELA DU CAS TOTALENERGIES

L'entretien mené avec un Industrial Cybersecurity Officer au sein de TotalEnergies offre une vision concrète et approfondie du métier dans le contexte d'un grand groupe industriel opérant dans le secteur des énergies renouvelables. Ce premier témoignage met en évidence un positionnement fortement orienté vers la gouvernance de la cybersécurité, l'accompagnement des projets industriels et la coordination à l'échelle internationale.

Afin d'adopter une approche plus holistique, conforme aux attentes de l'enquête métier, ce premier retour a été complété par un second échange avec un professionnel de la cybersécurité industrielle exerçant en Entreprise de Services du Numérique (ESN), intervenant pour le compte de clients industriels de secteurs variés (énergie, transport, industrie manufacturière). Ce second entretien permet d'apporter un regard complémentaire, davantage centré sur les missions opérationnelles, le conseil multi-clients et l'adaptabilité aux contextes industriels.

Ces deux témoignages ont été mis en perspective avec des analyses issues de sources institutionnelles, notamment l'APEC et des études sur l'emploi en ingénierie, qui soulignent la diversité des contextes d'exercice du métier d'ingénieur ou de responsable en cybersécurité industrielle.

6.1 Variations du métier selon le type d'organisation

Dans les grands groupes industriels (énergie, transport, chimie, agroalimentaire), l'Industrial Cybersecurity Officer intervient généralement sur un périmètre large et structuré. Il agit comme un référent sécurité transverse, impliqué dans la définition des politiques de cybersécurité, l'accompagnement des projets industriels et la coordination avec des équipes centrales. Les missions sont souvent orientées vers la gouvernance, la gestion des risques, la conformité réglementaire et le pilotage de prestataires externes.

Selon le second professionnel interrogé, exerçant en ESN spécialisée en cybersécurité, le métier prend une dimension plus opérationnelle et fortement orientée client. L'ingénieur ou consultant en cybersécurité industrielle intervient sur des missions ponctuelles et variées : audits de sécurité des environnements OT, analyses de risques, accompagnement à la mise en conformité réglementaire (IEC 62443, NIS2) ou assistance en phase de réponse à incident. Le rythme de travail y est souvent plus soutenu, avec des déplacements fréquents et une forte exigence d'adaptabilité.

Dans les PME industrielles, le rôle est généralement plus polyvalent. L'ingénieur cybersécurité peut cumuler plusieurs fonctions : sécurité des systèmes industriels, support IT, gestion des infrastructures réseau et parfois même participation à la production. Les ressources étant plus limitées, la cybersécurité repose davantage sur la capacité de l'ingénieur à prioriser les risques et à mettre en œuvre des solutions.

6.2 Vision RH du métier d'ingénieur en cybersécurité industrielle

Dans le cadre de cette enquête métier, un entretien a été mené avec un professionnel des Ressources Humaines impliqué dans le recrutement et le suivi de profils techniques évoluant dans des environnements industriels à forts enjeux. Cet échange visait à recueillir une vision spécifiquement RH du métier d'ingénieur en cybersécurité industrielle, complémentaire du témoignage métier précédemment analysé.

Profil interrogé : Responsable Recrutement / HR Business Partner (périmètre : métiers IT / cybersécurité)

Du point de vue des Ressources Humaines, le métier d'ingénieur en cybersécurité industrielle est aujourd'hui considéré comme un profil stratégique et critique pour les organisations industrielles. Il est directement lié à la continuité des activités, à la protection des infrastructures critiques et à la maîtrise des risques opérationnels. Les recruteurs soulignent l'existence de tensions fortes sur le marché, liées à un déséquilibre croissant entre la demande des entreprises et la disponibilité de profils capables de maîtriser simultanément les dimensions techniques, organisationnelles et réglementaires propres aux environnements industriels.

L'entretien met en évidence que le recrutement de cet ingénieur ne repose pas uniquement sur une expertise « cyber » au sens strict. Les Ressources Humaines insistent sur le fait que la compréhension des contraintes de production, de sûreté et de disponibilité des systèmes est déterminante. La sécurité doit être intégrée dans des contextes industriels où l'arrêt d'un système peut avoir des conséquences économiques, humaines ou environnementales majeures.

Cette spécificité explique en partie la rareté des profils, notamment à un niveau junior. Les recruteurs rencontrent des difficultés à identifier des candidats capables de dialoguer efficacement avec des interlocuteurs très variés, tout en portant des exigences de sécurité parfois perçues comme contraignantes. Les Ressources Humaines privilégient ainsi des ingénieurs disposant de bases solides en systèmes et réseaux, d'une capacité d'apprentissage rapide, et la montée en compétences progressive pour correspondre aux besoins.

Les compétences comportementales occupent une grande place dans cette vision RH. L'ingénieur est amené à intervenir dans des situations à forts enjeux, parfois en contexte de crise ou de tension projet. Les capacités de communication claire, de pédagogie, de priorisation sous contrainte et de gestion du stress sont identifiées comme des critères de

sélection déterminants. La capacité à convaincre des équipes d'exploitation, à adapter son discours à des interlocuteurs non techniques et à conserver une posture professionnelle dans l'urgence constitue un facteur clé de réussite dans le métier.

Enfin, la dimension du développement durable est de plus en plus intégrée dans les attentes RH, non pas sous la forme d'un discours théorique sur les Objectifs de Développement Durable, mais à travers l'évaluation de la capacité de l'ingénieur à intégrer des contraintes d'impact dans ses décisions. À ce titre, les Ressources Humaines identifient l'ingénieur en cybersécurité industrielle comme un acteur clé de l'ingénierie responsable à l'horizon 2030.

7. CONCLUSION ENQUETE METIER

Cette enquête métier a permis de souligner l'importance de l'Industrial Cybersecurity Officer dans un contexte marqué par la numérisation des systèmes industriels et l'intensification des cybermenaces. À travers l'analyse d'un témoignage professionnel, l'étude du marché de l'emploi et la consultation de référentiels reconnus, ce travail a apporté une compréhension globale des missions, des compétences et des responsabilités associées à ce métier.

Outre ses aspects techniques, le métier se caractérise par sa grande transversalité, son aspect humain et décisionnel, sans oublier son impact sur la société. L'ingénieur en cybersécurité industrielle joue un rôle crucial dans la protection des infrastructures critiques et s'aligne parfaitement avec les enjeux de développement durable et de transition énergétique, en cohérence avec la vision de l'ingénieur responsable à l'horizon 2030.

8. ENQUÊTE SUR SOI

8.1 Feedback de l'entourage

L'enquête sur soi s'inscrit dans une démarche introspective, visant à mieux comprendre mon fonctionnement, mes forces, mes limites et mes valeurs, afin de les confronter aux exigences actuelles et futures du métier d'ingénieur en cybersécurité industrielle. Cette démarche repose sur plusieurs outils complémentaires : le feedback de l'entourage, des tests de personnalité, l'analyse de situations de réussite et d'échec, ainsi qu'un travail d'identification des valeurs personnelles. L'objectif est d'identifier les écarts entre mon profil actuel et les attendus du métier, afin de construire un plan d'action réaliste et progressif.

Pour mieux me connaître et avoir un regard extérieur, j'ai demandé des avis à des personnes de mon entourage : des camarades, d'anciens collègues, ainsi que des proches. J'ai volontairement choisi des profils variés, tant sur le plan professionnel que personnel. Au total, 11 personnes ont répondu (6 de mon entourage personnel, 5 de mon entourage professionnel). Les adjectifs les plus récurrents sont : rigoureux, fiable, curieux, autonome et exigeant. Les points de vigilance les plus cités sont : perfectionnisme, tendance à avancer seul sur le technique et partage d'information insuffisant en équipe.

Pour structurer les réponses, j'ai utilisé un questionnaire commun comprenant notamment : 10 adjectifs me décrivant, mes qualités et défauts associés à des situations, ce que la personne apprécie le plus, les aspects les plus difficiles à gérer, et les valeurs/principes qu'elle me donne.

Plusieurs retours reviennent régulièrement. Sur le plan professionnel, on me décrit souvent comme sérieux, rigoureux et investi dans ce que j'entreprends. Plusieurs personnes ont souligné ma capacité à m'approprier rapidement des sujets techniques complexes et à travailler de façon autonome, surtout quand les objectifs sont clairs.

Cependant, certains retours pointent aussi un perfectionnisme qui peut parfois être excessif, ce qui peut alourdir ma charge de travail ou rendre la délégation difficile. En groupe, on m'a parfois fait remarquer que je prenais rapidement en main les aspects techniques sans toujours assez expliquer mes choix ou partager l'avancement, ce qui peut créer un décalage avec l'équipe. Ces remarques me permettent de progresser dans ma communication et renforcer le travail collaboratif, notamment avec des personnes moins techniques.

Sur le plan personnel, les qualités qui reviennent le plus sont la fiabilité, la curiosité et le sens des responsabilités. Cela confirme une posture tournée vers la recherche de solutions et la prise en compte des conséquences de mes décisions, ce qui me semble important dans les métiers liés à la cybersécurité.

Je suis en accord avec l'idée d'un profil structuré et fiable. Je suis également en accord avec le point de vigilance sur le perfectionnisme : je l'associe à une exigence de robustesse, mais je constate qu'il peut devenir un frein si je ne priorise pas mieux (risque de surinvestissement).

De plus, je reconnais le manque de communication de ma part, cela vient souvent d'une volonté d'efficacité, mais l'effet peut être contre-productif si l'équipe ne suit pas. Dans une logique ingénieur, ce point constitue un axe de progression prioritaire.

8.2 Tests de personnalité et analyse comportementale

Pour mieux comprendre ma façon de fonctionner, j'ai complété les retours de mon entourage par quelques tests de personnalité (MBTI) visant à mieux comprendre mes préférences de fonctionnement. Les résultats montrent un profil plutôt tourné vers l'analyse, la logique et l'anticipation, et qui se sent à l'aise dans des environnements organisés et structurés.

Concrètement, cela signifie que je comprends assez facilement les systèmes complexes, que j'aime prendre le temps de réfléchir et évaluer les risques. En revanche, quand une situation est trop floue ou mal définie, je peux être un peu mal à l'aise au début, j'ai tendance à vouloir rapidement poser un cadre pour avancer.

Les tests ont aussi souligné que je ne suis pas du genre à prendre la parole spontanément, surtout en groupe. Je préfère réfléchir avant d'intervenir, pour apporter des arguments solides. C'est à la fois une force et un point sur lequel je peux progresser, notamment dans les situations qui demandent plus de communication.

Je suis naturellement fait pour le métier d'ingénieur en cybersécurité : j'ai le sens de l'analyse, une approche méthodique et une bonne capacité d'anticipation. Pour évoluer, je ne cherche pas simplement à approfondir mes compétences techniques, mais surtout à développer mon influence et ma pédagogie. L'enjeu, pour moi, est de savoir expliquer et faire accepter les exigences de sécurité, que ce soit auprès des équipes IT/OT ou des décideurs.

8.3 Analyse des réussites et des échecs

Lors de mon BUT Informatique, j'ai travaillé sur un projet d'amélioration d'une infrastructure en équipe. J'ai assez vite pris le lead sur la partie technique et l'organisation du travail. Ça a bien marché surtout parce que j'ai pris le temps de bien cerner les besoins, d'anticiper les difficultés possibles et de proposer une architecture claire dès le début.

Mais sur ce même projet, j'ai aussi fait face à un vrai défi côté collaboration. Voulant à tout prix que la technique tienne la route, j'ai parfois avancé un peu en solo, sans assez expliquer ou formaliser mes décisions pour les autres. Résultat, certains collègues ont décroché ou n'ont pas vraiment pu s'approprier le projet. Cette expérience m'a permis de savoir mieux communiquer et partager, même quand une solution paraît évidente.

Heureusement, un stage m'a permis de progresser là-dessus. En intégrant une équipe informatique, j'ai dû documenter mon travail et faire des points réguliers avec mon tuteur. Cette habitude m'a aidé à mieux synthétiser des sujets techniques et à les rendre accessibles, même pour des personnes moins familières avec le domaine.

8.4 Identification des valeurs personnelles

L'analyse de mes valeurs personnelles, en lien avec le modèle de Shalom Schwartz, met en évidence des valeurs de sécurité, de responsabilité et de réalisation personnelle. La valeur de sécurité se traduit par un intérêt marqué pour la protection des systèmes, la prévention des incidents et la maîtrise des risques, c'est d'ailleurs ce qui m'a naturellement conduit vers la cybersécurité.

La responsabilité est de porter une attention particulière portée aux conséquences des décisions techniques, notamment lorsqu'elles peuvent impacter des utilisateurs, des infrastructures ou des organisations.

Enfin, la réalisation personnelle est étroitement liée à la recherche de sens dans les missions confiées. Elle se traduit par une motivation plus forte pour des projets ayant un impact concret et mesurable, plutôt que pour des tâches purement techniques sans finalité.

Cet ensemble de valeurs est cohérent avec un positionnement en cybersécurité orienté risques, gouvernance, audit et cybersécurité OT, où l'on doit concilier exigences de sécurité, contraintes opérationnelles et responsabilité.

9. LIEN ENTRE L'ENQUÊTE MÉTIER ET L'ENQUÊTE SUR SOI

Le croisement entre l'enquête métier menée et l'enquête sur soi constitue une étape clé du Projet de Formation Individuel. Ce travail m'a permis d'aller plus loin qu'une simple comparaison. Il m'a donné l'occasion d'analyser, avec un regard critique, la cohérence entre mon profil personnel, mes compétences actuelles et ce que le métier d'ingénieur en cybersécurité industrielle exigera d'ici 2030.

L'enquête métier met en évidence un métier exigeant, l'Industrial Cybersecurity Officer est attendu comme un acteur de confiance, capable d'analyser des environnements complexes, d'anticiper les risques, mais également d'influencer les décisions techniques et stratégiques au sein de l'entreprise. Ces attentes font fortement référence à certains traits identifiés dans mon enquête sur soi.

Mon goût pour l'analyse, ma rigueur méthodologique et mon besoin de structuration constituent des points de convergence forts avec les compétences attendues dans les domaines de l'audit de sécurité, de la gestion des risques et de la gouvernance de la cybersécurité. De plus, mon intérêt pour la prévention des incidents et la fiabilité des systèmes rejoint les responsabilités observées lors de l'enquête métier, notamment dans la protection des infrastructures critiques et la continuité des activités industrielles.

L'analyse de mes valeurs personnelles, à travers le modèle de Schwartz, renforce cette cohérence. Les valeurs de sécurité, de responsabilité et de fiabilité font partie de mes valeurs et sont en adéquation avec les enjeux éthiques, réglementaires et environnementaux portés par le métier.

Cependant, le croisement des deux enquêtes met également en évidence plusieurs écarts entre mon profil actuel et les exigences du métier d'ingénieur en cybersécurité industrielle. Le premier écart concerne la posture de communication. L'enquête métier souligne l'importance d'une communication proactive et pédagogique, notamment pour vulgariser des sujets techniques complexes auprès d'interlocuteurs non spécialistes (métiers, direction, partenaires). Or, l'enquête sur soi révèle une tendance à privilégier l'analyse technique au détriment de la communication et de la diffusion des messages ; un point sur lequel je dois travailler en priorité.

Le métier requiert une posture d'ingénieur capable de défendre des choix de sécurité parfois contraignants face à des impératifs de coûts, de délais ou de performance. Cette dimension politique et transverse, fortement présente dans les environnements industriels décrits lors de l'enquête métier, reste à renforcer dans mon développement personnel. Enfin, une tendance au perfectionnisme peut constituer un frein dans des contextes projet contraints, où la priorisation et l'arbitrage sont essentiels.

À court et moyen terme, mon projet professionnel vise à réduire ces écarts de manière progressive et structurée. Après l'obtention de mon diplôme d'ingénieur, je souhaite m'orienter vers un poste en cybersécurité, idéalement dans les domaines de l'audit ou de la gestion des risques. Cette première phase me permettra de consolider mes fondamentaux techniques en réseaux, systèmes et sécurité, tout en développant une vision globale des systèmes d'information et des environnements industriels. Elle sera complétée par l'acquisition de certifications reconnues et par un travail ciblé sur le développement des compétences transverses, notamment la communication, la gestion de projet et la prise de décision en contexte contraint.

À plus long terme, mon objectif est d'évoluer vers un poste à responsabilité, intégrant une dimension de pilotage ou de management de la cybersécurité. Cette projection implique une montée en maturité non seulement sur le plan technique, mais également sur le plan humain, éthique et stratégique. Elle s'inscrit pleinement dans la vision de l'ingénieur à l'horizon 2030, c'est-à-dire un ingénieur capable de concilier performance technologique, résilience des infrastructures industrielles et responsabilité sociétale et environnementale.

10. BIBLIOGRAPHIE / WEBOGRAPHIE

1. Sources institutionnelles et référentiels en cybersécurité

- **ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)**
  Guide de la cybersécurité des systèmes industriels
  Consulté en Janvier 2026.
- **ANSSI**
  Méthode EBIOS Risk Manager – Guide d'analyse de risques
  https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm/
  Consulté en Janvier 2026.
- **NIST (National Institute of Standards and Technology)**
  Special Publication 800-82 – Guide to Industrial Control Systems (ICS) Security
  https://csrc.nist.gov/pubs/sp/800/82/r2/final
  Consulté en Janvier 2026.
- **NIST**
  Cybersecurity Framework (CSF)
  https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
  Consulté en Janvier 2026.

2. Normes et standards internationaux

- **ISO/IEC 27001**
  Information Security Management Systems – Requirements
  https://www.iso.org/fr/standard/27001
  Consulté en Janvier 2026.
- **ISO/IEC 27005**
  Information Security Risk Management
  https://www.iso.org/fr/standard/80585.html
  Consulté en Janvier 2026.
- **IEC 62443**
  Industrial communication networks – Network and system security
  https://fr.wikipedia.org/wiki/CEI_62443
  Consulté en Janvier 2026.

3. Études métiers et observatoires de l'emploi

- **APEC (Association Pour l'Emploi des Cadres)**
  Fiche métier – Ingénieur / Responsable cybersécurité
  https://www.apec.fr/tous-nos-metiers/informatique/ingenieur-securite-informatique.html
  Consulté en Janvier 2026.

4. Réglementations et cadres légaux

- **Union Européenne**
  Directive NIS 2 – Sécurité des réseaux et des systèmes d'information
  https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
  Consulté en Janvier 2026.
- **Union Européenne**
  Digital Operational Resilience Act (DORA)
  https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
  Consulté en Janvier 2026.
- **Sarbanes-Oxley Act (SOX)**
  https://fr.wikipedia.org/wiki/Loi_Sarbanes-Oxley
- **Règlement Général sur la Protection des Données (RGPD)**
  Règlement (UE) 2016/679
  https://www.cnil.fr/fr/reglement-europeen-protection-donnees
  Consulté en Janvier 2026.

5. Offres d'emploi analysées

- **Squad**
  Offre d'emploi Linkedin : Consultant Cybersécurité Risques – Niveau confirmé
  France.
  Consulté en Janvier 2026.
- **Willhire**
  Offre d'emploi Linkedin : Cyber Security Intern
  International.
  Consulté en Janvier 2026.

6. Ressources pédagogiques et professionnelles complémentaires

- **Agenda 2030 – Nations Unies**
  https://www.agenda-2030.fr/17-objectifs-de-developpement-durable/?
  Consulté en Janvier 2026.
- **Hack The Box**
  Plateforme de formation pratique en cybersécurité.
  https://www.hackthebox.com/
  Consulté en Janvier 2026.
- **MOOC Cybersécurité (divers organismes)**
  Plateformes de formation en ligne (ANSSI, universités, organismes spécialisés).
  https://cyber.gouv.fr/offre-de-service/formations-entrainement-et-decouverte-des-metiers/formations/formations-delivrees-par-lanssi/mooc-secnumacademie/
  Consulté en Janvier 2026.

7. Enquête sur soi

- **Test de personnalité**
  https://www.16personalities.com/fr/test-de-personnalite
  Consulté en Janvier 2026.