CONSULTANT CYBERSÉCURITÉ

Domaine d'activité
Métiers du conseil

Famille de métiers
Conseil SI

Autres appellations du métier
Consultant en sécurité des systèmes d'information

Nomenclature PCS
388c - Chefs de projets informatiques, responsables informatiques

Nomenclature ROME
38834 - Expert / Experte en cybersécurité

Mission

Le Consultant en cybersécurité analyse les risques cyber d'une entreprise afin de proposer des solutions de protection adaptées à ses besoins et respectant la réglementation applicable en matière de protection des données (RGPD notamment). Il peut être sollicité pour des missions de prévention des risques mais peut également intervenir auprès d'entreprises ayant subi une cyberattaque ou fournir une expertise dans le cadre de missions de conseil ou d'audit.

Activités

Proposition commerciale et cadrage des besoins client

- Participe aux réponses aux appels d'offre pour des projets de diagnostic et prévention des risques en matière de cybersécurité (élaboration de la méthodologie, tarification, soutenance...) et peut intervenir sur le volet « cybersécurité » d'une proposition d'intervention de conseil ou d'audit SI
- Identifie les problématiques du client en matière de cybersécurité, analyse les données client à disposition et les processus de protection existants, formule les hypothèses de travail et limites d'analyse
- Adapte les objectifs et étapes de la mission à partir de sa compréhension des enjeux (stratégie d'entreprise, organisation du système d'information) selon le type de mission (mission de conseil ou audit SI…)

Définition et mise en œuvre d'une stratégie de cybersécurité

- Définit des scénarios d'intrusion selon les activités et besoins spécifiques du client (banque, secteur public, numérique, défense…) afin de tester la vulnérabilité des systèmes
- Produit une cartographie des risques cyber des systèmes d'information
- À partir de l'identification des menaces, définit et met en œuvre selon le besoin du client les pistes d'amélioration des systèmes : amélioration des solutions et process en place, installation d'un logiciel de cybersécurité, définition de plans de continuité des activités, diffusion de bonnes pratiques digitales au sein de l'organisation, mise en place de tests de routines…
- Peut intervenir pour le compte de son propre cabinet afin de couvrir les enjeux de cybersécurité des différents pôles d'activité du cabinet d'expertise-comptable et des systèmes d'information internes

Développement de l'activité, veille « métier » et technologique

- S'appuie sur un travail de veille régulier pour alimenter sa pratique : veille « métier » sur les évolutions des problématiques de ses clients particulièrement dans le domaine des systèmes d'information et veille technologique sur l'évolution des techniques de cybersécurité
- Participe au développement des prestations du cabinet en se positionnant comme expert cybersécurité auprès des pôles d'activité du cabinet (expertise comptable, audit, conseil)
- Entretient un réseau professionnel (dirigeants, consultants…) et met en valeur l'activité du cabinet en participant à des évènements et projets du cabinet (études, séminaires, rencontres professionnelles…)

Consultant cybersécurité

Compétences

Légende

1 Niveau de base | 2 Niveau avancé | 3 Niveau confirmé | 4 Niveau expert

Macro-compétences spécifiques

Macro-compétence	Niveau attendu sur la macro-compétence et compétence associée	Exemple d'application
Concepts spécifiques au domaine de spécialité	4 Anticiper les tendances et faire évoluer les offres et process de travail en fonction	*Se former aux techniques de cybersécurité émergentes et faire les offres commerciales en fonction*
Collecte des informations nécessaires à la production d'une mission	3 Adapter les modes de collecte et de classification aux spécificités des clients et exigences de la mission	*Mettre en place les conditions d'accès aux systèmes client dans le cadre de tests de vulnérabilité*
Process et méthodologies de travail spécifiques au domaine de spécialité	4 Intégrer les évolutions réglementaires, économiques et technologiques pour créer et diffuser de nouveaux process et modes de travail	*Appliquer les étapes principales de stratégies d'intrusion dans un système d'information client*
Production de livrables répondant à une problématique client	3 Réaliser et formaliser des analyses s'appuyant sur une variété de matériaux et des préconisations articulées aux problématiques spécifiques du client	*Réaliser la cartographie des risques d'un système d'information client*
Sécurité des échanges de données avec l'externe	4 Définir une stratégie de sécurisation des échanges de données à l'échelle du cabinet ou d'une structure cliente	*Proposer une stratégie de protection des données basée sur un diagnostic des vulnérabilités*
Gestion et exploitation d'une base de données	3 Conduire des analyses avancées, identifier et utiliser les outils d'exploitation adaptés	*Analyser des données dans le cadre de tests de vulnérabilité et synthétiser les résultats obtenus*
Gestion d'une architecture fonctionnelle SI	4 Définir et piloter la stratégie d'intégration d'un SI en tenant compte des besoins métiers, des contraintes techniques et de cybersécurité	*Identifier les vulnérabilités d'un système d'information et formuler des mesures de gestion des risques*
Accompagnement des projets de transformation	4 Faire converger les acteurs autour de la finalité du projet et mettre en valeur les avancées	*Faire converger un client autour d'une stratégie de cybersécurité*

Macro compétences transverses

Pilotage de missions	3 Piloter une ou plusieurs phases et équipes projets	*Gérer les étapes d'une mission de cybersécurité selon les contraintes budgétaires et les attentes du client*
Sens commercial	3 Piloter la construction d'offres commerciales, entretenir un réseau de partenaires et apporteurs d'affaires	*Construire une offre commerciale en cybersécurité en tenant compte de l'évolution des technologies*
Communication écrite et orale	3 Développer des mises en forme écrites élaborées, schématiser des idées complexes	*Expliciter des notions de cybersécurité complexes à l'oral et à travers des schémas*
Organisation et planification du travail	3 Planifier son organisation du travail selon les priorités sur ses différents dossiers d'intervention	*Prendre en compte les spécificités du SI client pour établir un diagnostic de cybersécurité*
Anglais professionnel	4 Diriger des débats techniques et un projet en anglais	*Conduire une mission de conseil en anglais auprès d'une clientèle internationale*

Consultant cybersécurité

Variabilité du métier

Selon la taille du cabinet

- Dans les cabinets de petite taille, le Consultant cybersécurité peut également intervenir fréquemment sur des missions de conseil SI, d'audit SI et en tant qu'expert en matière de SI et d'analyse des données sur des dossiers d'expertise-comptable, d'audit….
- Dans les grands cabinets, il est le plus souvent rattaché à un pôle dédié spécialisé et intervient sur une variété de secteurs d'activités et de problématiques de cybersécurité : protection des données, gestion de crise, cartographie des risques…

Selon les spécialités du cabinet

- Selon le degré de spécialisation des cabinets en cybersécurité, les missions de cybersécurité peuvent être ponctuelles, intégrées dans des missions de conseil en SI et plus ou moins poussées (pôle d'activité spécifique dans le cabinet, technologies variées et de pointe…).

Selon l'expérience du professionnel

- Après quelques années d'expérience, le Consultant en cybersécurité peut encadrer des collaborateurs juniors, piloter un périmètre plus large des missions (cadrage de la mission, négociation commerciale..), interagir davantage avec le client et intervenir sur des missions de cybersécurité de nature plus complexe.

Conditions d'exercice

- *Relations professionnelles internes* : Consultant d'autres spécialités (SI, Finance…) et autres métiers des cabinets si besoin d'une expertise particulière (Expert-comptable, Juriste fiscal…)
- *Relations professionnelles externes* : dirigeants, Directeur des systèmes d'information, Chef de projet cybersécurité, prestataires informatiques des clients…
- *Télétravail* : possible sur une partie significative des activités, mais variable selon la nécessité d'intervenir sur les outils clients ou dans des conditions sécurisées.

Prérequis pour l'exercice du métier

Formation initiale

- Bac+5 en informatique, sécurité des réseaux ou cybersécurité obtenu à l'université ou en École d'ingénieur

Profil recommandé pour le personnel expérimenté s'orientant vers ce métier

- Consultant en SI en ESN (Entreprise de Services Numériques) ou cabinet avec spécialisation sur les enjeux de cybersécurité
- Expert cybersécurité en entreprise
- Responsable SI ou chargé de projet SI en entreprise avec spécialisation sur les enjeux de cybersécurité

Formations prioritaires en cours de carrière

- Formation à l'évolution des technologies de cybersécurité et des réglementations en matière de protection des données (RGPD…)
- Formation aux méthodes et techniques de conseil et accompagnement du changement : méthode agile, matrices d'analyse, design thinking…
- Formation aux logiciels d'analyse de données

Tendances d'évolution du métier

- Spécialisation croissante des consultants dans les différentes méthodes de cybersécurité en raison de l'évolution rapide des technologies et des besoins des clients
- Développement des compétences d'animation, de communication et de facilitation de groupes de travail afin de développer la créativité dans l'identification des stratégies de piratage informatique, les stratégies de prévention des risques adaptées aux pratiques professionnelles d'un client…

Perspectives professionnelles

- Responsable cybersécurité et autres métiers des SI (Directeur SI…) en entreprise
- Métiers du conseil en systèmes d'information et de l'analyse de données (Data Analyst) sous condition de renforcement des compétences en techniques statistiques et logiciels de programmation adaptés