Architecte Cybersécurité Senior

Profil

Objectif du poste : Concevoir, faire évoluer et challenger l'architecture de cybersécurité de notre client afin de traduire les exigences de sécurité, de risque et de conformité en solutions techniques robustes, réalistes et maintenables. Le rôle s'exerce en collaboration directe avec les équipes IT du client, dans une logique de conseil, de co-construction, de transfert de compétences et d'orientation client. Toute évolution proposée est soumise à la validation préalable de notre client avant sa mise en œuvre.

En tant qu'Architecte Cybersécurité Senior, vous occupez un rôle transverse entre la gouvernance de la sécurité, l'architecture IT et les équipes techniques. Vous analysez l'existant, définissez des architectures cibles, évaluez les risques et impacts, comparez les options possibles et formulez des recommandations applicables dans un environnement IT complexe et fortement interconnecté.

Vous appliquez notamment les principes de Security by Design, Security by Default, Zero Trust, moindre privilège, défense en profondeur, segmentation et résilience. Vous veillez à rechercher un équilibre entre sécurité, disponibilité, besoins métiers, maintenabilité et contraintes opérationnelles.

Normes et certifications :

- Expertise des normes **ISO 27001, ISO 27002 et ISO 27005 (version 2022)** avec capacité à traduire les exigences en architectures de sécurité et contrôles techniques.
- Bonne connaissance des réglementations et référentiels de cybersécurité : **NIS2, RGPD, CyberFundamentals (CyFun®), NIST CSF et CIS Controls**.
- Maîtrise du framework **CyFun® du CCB**, de ses niveaux d'assurance et de son articulation avec **NIS2** et **ISO 27001**.
- Capacité à intégrer les enjeux de **gestion des risques**, de conformité et de sécurité dans les choix d'architecture.
- Atout : connaissance des référentiels liés à la **continuité d'activité**, la **gestion des incidents** et la **sécurité cloud**.
- Certification **CISSP** (ou équivalent senior) fortement attendue.
- Certifications **ISSAP** et/ou **SABSA** fortement appréciées pour l'architecture de sécurité.
- Certifications **ISO 27001 Lead Implementer/Lead Auditor** et **ISO 27005 Risk Manager** considérées comme des plus.

- Certifications complémentaires valorisées : **TOGAF Enterprise Architecture Practitioner** et/ou **CCSP**.
- Expérience démontrée dans la conception, la justification, la documentation et l'évolution d'architectures de cybersécurité complexes.
- Les certifications doivent être complétées par des **réalisations concrètes en architecture de sécurité**.

Missions et contributions attendues :

- Analyse de l'architecture cybersécurité existante et formulation de recommandations d'évolution alignées sur l'architecture IT et les objectifs de l'organisation.
- Identification des **risques, vulnérabilités, dépendances et points de faiblesse**, avec propositions d'améliorations priorisées.
- Réalisation de **revues d'architecture de sécurité** pour les projets, migrations et changements majeurs.
- Définition de principes d'architecture sécurisée : **segmentation réseau, contrôle des flux, gestion des accès, résilience et défense en profondeur**.
- Analyse et recommandations sur les sujets **IAM** (Identity & Access Management), authentification, comptes à privilèges et mécanismes de confiance.
- Conseil sur les besoins de **journalisation, supervision, détection et traçabilité** des événements de sécurité.
- Élaboration de **standards, patterns de sécurité, règles de hardening et exigences techniques réutilisables**.
- Évaluation critique des propositions de fournisseurs et intégrateurs, avec analyse des **impacts, risques, dépendances et alternatives**.
- Support expert lors d'analyses liées aux **incidents majeurs**, à la **résilience**, à la **continuité d'activité** et à la **reprise après sinistre**.
- Veille technologique et réglementaire avec recommandations sur les évolutions pertinentes et leur valeur ajoutée.
- Accompagnement des équipes IT dans l'analyse et la préparation de la mise en œuvre des recommandations validées.
- Transfert de compétences et partage de connaissances afin de renforcer l'autonomie des équipes internes et limiter la dépendance aux prestataires externes.

Gouvernance des changements et validation :

L'Architecte Cybersécurité agit en qualité de conseil et d'expert. Il formule des recommandations et propose des architectures ; les décisions, priorités et validations restent de la responsabilité du client.

• Toute proposition de modification significative doit être documentée et soumise à la validation préalable des responsables désignés par le client.

• Les impacts techniques, opérationnels et sécurité, les dépendances, les risques, les prérequis et les alternatives doivent être explicités avant décision.

• Lorsque pertinent, les propositions incluent les modalités de test, les critères d'acceptation, le plan d'implémentation et la procédure de retour arrière.

• Aucune modification directe d'un environnement de production ne peut être réalisée sur la seule initiative de l'architecte ; les processus de change management du client doivent être respectés

Collaboration, transfert de compétences et orientation client :

La mission doit renforcer durablement les compétences internes. L'architecte travaille avec les équipes IT du client et non en silo. Le partage de connaissances et la co-construction font partie intégrante de la mission.

• Travailler en collaboration directe avec les équipes IT, sécurité, infrastructure, systèmes, réseau, exploitation et projets.

• Associer les équipes internes aux analyses, choix d'architecture, revues, tests et validations afin de favoriser la compréhension et l'appropriation des décisions.

• Organiser des ateliers techniques, revues d'architecture, sessions de partage de connaissances et handovers adaptés au niveau des équipes.

• Produire une documentation claire, structurée, maintenable et exploitable de manière autonome par notre client.

• Veiller à ne pas créer de dépendance inutile vis-à-vis d'un consultant, d'un fournisseur ou d'un constructeur.

Savoir-être et posture professionnelle :

• Orientation client : Comprendre les besoins, contraintes et priorités de notre client avant de proposer une solution ; rechercher une réponse sécurisée, proportionnée, exploitable et maintenable.

• Écoute et collaboration : Travailler dans un esprit de partenariat et valoriser la connaissance de l'environnement détenue par les équipes internes.

• Communication et pédagogie : Expliquer clairement des sujets complexes à des interlocuteurs techniques ou non techniques et adapter le niveau de détail au public.

• Esprit critique constructif : Savoir challenger une solution sans imposer une réponse ; argumenter sur la base des risques, des faits et des bonnes pratiques et proposer des alternatives.

• Pragmatisme : Éviter les architectures théoriques ou surdimensionnées et rechercher le meilleur équilibre entre sécurité, disponibilité, coûts, exploitation et besoins métiers.

• Transparence et intégrité : Communiquer les hypothèses, limites, risques et incertitudes et signaler rapidement toute décision nécessitant un arbitrage.

• Rigueur : Travailler de manière structurée, traçable et documentée, avec une attention particulière à la qualité des livrables et au suivi des décisions.

• Autonomie responsable : Mener ses analyses avec autonomie tout en respectant les responsabilités, processus de validation et décisions de notre client.

• Transmission : Partager activement son savoir-faire et contribuer à l'autonomie progressive des équipes internes.

• Neutralité technologique : Conseiller dans l'intérêt de notre client et évaluer objectivement plusieurs options lorsque cela est pertinent.

Skills

- **10+ ans d'expérience IT**, dont **7+ ans en cybersécurité** et **5+ ans minimum en tant qu'Architecte Sécurité/Cybersécurité**.
- Expérience confirmée dans la **conception, la revue et l'évolution d'architectures de cybersécurité complexes**.
- Expertise couvrant plusieurs domaines : **réseau, connectivité, datacenter, IAM, sécurité périmétrique, accès distant, cloud/hybride et supervision de sécurité**.
- Capacité à produire et maintenir la documentation d'architecture : **schémas, flux, matrices de communication, segmentation, exigences et décisions d'architecture**.
- Excellente compréhension des technologies de sécurité d'entreprise avec une approche **indépendante des fournisseurs et constructeurs**.
- Solide maîtrise des solutions d'**identité et gestion des accès (IAM, MFA, PAM, PKI, certificats, authentification forte)**.
- Bonne compréhension des architectures **réseau** : segmentation, routage, haute disponibilité, interconnexions, accès distants et contrôle des flux.
- Bonne connaissance des environnements **systèmes, virtualisation, datacenter, cloud/hybride**, ainsi que des enjeux de **continuité et résilience**.
- Expérience des architectures de **journalisation, SIEM/SOC et supervision de sécurité** (collecte, corrélation, détection, rétention et traçabilité).
- Capacité à mener des **analyses de risques techniques**, challenger les solutions proposées par les fournisseurs et formuler des recommandations pragmatiques.
- Aptitude à traduire les exigences de **conformité, gouvernance et gestion des risques** en contrôles de sécurité et décisions d'architecture.
- Les expériences purement orientées **administration, exploitation, SOC, ingénierie sécurité ou expertise produit** ne sont pas considérées comme équivalentes à une fonction

Others

- Master en Informatique, Cybersécurité, Sécurité des Systèmes d'information, Réseaux et Télécommunications, Sciences de l'Ingénieur ou formation équivalente.
- Une expérience professionnelle particulièrement significative et démontrable en architecture cybersécurité peut être prise en considération comme équivalente, sous réserve que le candidat réponde au niveau d'expertise et de séniorité attendu.