

On recherche un **Architecte Cybersécurité** Senior capable de concevoir, faire évoluer et challenger des architectures de cybersécurité complexes au sein d'environnements IT d'entreprise fortement interconnectés. Le consultant intervient comme expert et conseiller entre la gouvernance sécurité, l'architecture IT et les équipes techniques afin de traduire les exigences de sécurité, de risque, de conformité et de résilience en architectures, standards et recommandations concrètes.

Le rôle requiert une forte expertise en architecture cybersécurité, une vision transverse des infrastructures et des technologies de sécurité, ainsi qu'une capacité à évaluer les risques, comparer les options techniques, documenter les décisions d'architecture et accompagner les équipes dans une logique de transfert de compétences.

Le consultant agit dans une posture de conseil. Il formule des recommandations mais ne détient pas le pouvoir de décision sur les priorités, les changements ou les architectures validées.

Vos missions:

- Analyser l'architecture cybersécurité existante et proposer des évolutions cohérentes avec l'architecture IT globale.
- Définir des architectures cibles, principes d'architecture et standards de sécurité.
- Traduire les exigences de sécurité, de conformité et de gestion des risques en contrôles techniques et décisions d'architecture.
- Réaliser des analyses de risques techniques et évaluer l'impact des choix architecturaux.
- Identifier vulnérabilités, dépendances, faiblesses et points de fragilité de l'environnement.
- Réaliser des revues d'architecture de sécurité dans le cadre de projets, migrations ou changements majeurs.
- Challenger les propositions de fournisseurs, intégrateurs et partenaires.
- Définir des recommandations en matière de segmentation, contrôle des flux, accès, résilience et défense en profondeur.
- Accompagner les réflexions autour des architectures IAM, MFA, PAM, PKI, authentification forte et gestion des comptes privilégiés.
- Conseiller sur les architectures de journalisation, supervision, traçabilité, détection et intégration SIEM/SOC.
- Formaliser standards de sécurité, patterns de sécurité, exigences techniques et principes de hardening.
- Participer aux analyses techniques liées aux incidents majeurs, à la continuité d'activité, à la reprise et à la résilience.
- Assurer une veille technologique et réglementaire continue.
- Accompagner les équipes dans la compréhension et la préparation des implémentations approuvées.
- Assurer le transfert de connaissances et renforcer durablement les compétences internes.

Vos activités:

Architecture et sécurité

- Concevoir et maintenir des architectures de cybersécurité de haut niveau et détaillées.
- Produire schémas d'architecture, flux de communication, matrices de communication, principes de segmentation et documents de décision.

- Définir des architectures alignées sur les principes :
- Security by Design.
- Security by Default.
- Zero Trust.
- Least Privilege.
- Defense in Depth.
- Segmentation.
- Résilience.

Analyse et gestion des risques

- Réaliser des analyses de risques techniques.
- Évaluer impacts, prérequis, contraintes et dépendances.
- Identifier vulnérabilités et risques de sécurité.
- Émettre des recommandations documentées et proportionnées.

Revue et gouvernance

- Réaliser des security architecture reviews.
- Challenger les choix techniques et les architectures proposées.
- Justifier les recommandations sur base des risques, faits et bonnes pratiques.
- Préparer les dossiers de décision.
- Définir critères d'acceptation, scénarios de tests, plans d'implémentation et procédures de rollback lorsque nécessaire.
- Respecter les processus de change management.

IAM et contrôle d'accès

Analyser les besoins liés :

- à l'identité numérique ;
- à l'authentification ;
- aux accès ;
- aux comptes privilégiés ;
- aux mécanismes de confiance.

Définir les recommandations architecturales associées.

Supervision et détection

- Conseiller sur :
- la journalisation ;
- la collecte ;
- la corrélation ;
- la détection ;
- la rétention ;
- la traçabilité ;
- les architectures SIEM ;
- les organisations SOC.

Documentation

- Produire une documentation :
- claire ;
- structurée ;
- maintenable ;
- exploitable de manière autonome.

Collaboration et transfert de connaissances

- Organiser ateliers techniques.
- Animer revues d'architecture.
- Réaliser sessions de partage de connaissances.
- Réaliser handovers.

- Associer les équipes aux analyses, choix techniques, tests et validations.
- Favoriser l'autonomie des équipes internes.
- Éviter toute dépendance excessive à un consultant ou fournisseur.

Vos compétences:

Expérience

- Minimum 10 ans d'expérience en environnements IT d'entreprise complexes.
- Minimum 7 ans en cybersécurité.
- Minimum 5 ans comme Architecte Sécurité ou Architecte Cybersécurité.
- Expérience démontrable de conception, revue et évolution d'architectures de cybersécurité complexes.
- Expérience multi-domaines :
- Réseau et connectivité.
- Datacenter.
- IAM.
- Sécurité périmétrique.
- Accès distants.
- Cloud.
- Environnements hybrides.
- Supervision de sécurité.

Architecture Cybersécurité

- Architecture de sécurité d'entreprise.
- Security by Design.
- Security by Default.
- Zero Trust.
- Least Privilege.
- Defense in Depth.
- Segmentation réseau.
- Résilience.
- Haute disponibilité.
- Contrôle des flux.
- Architecture cloud et hybride.
- Architecture datacenter.
- Virtualisation.

IAM & Trust Services

- IAM.
- MFA.
- PAM.
- PKI.
- Certificats.
- Authentification forte.
- Gestion des comptes privilégiés.

Réseaux

- Réseaux d'entreprise.
- Segmentation.
- Routage.
- Interconnexions.
- Contrôle des flux.
- Accès distants.

- Firewalls.
- Haute disponibilité.

Supervision Sécurité

- SIEM.
- SOC.
- Logging.
- Monitoring.
- Détection.
- Corrélation.
- Rétention.
- Traçabilité.

Gouvernance & Risques

- Analyse des risques.
- Gestion des risques.
- Architecture basée sur les risques.
- Traduction des exigences réglementaires en contrôles techniques.
- Gestion de la conformité.
- Évaluation de fournisseurs.
- Security Architecture Review.

Normes & Référentiels

- ISO/IEC 27001:2022 (maîtrise).
- ISO/IEC 27002:2022.
- ISO/IEC 27005:2022.
- NIS2.
- RGPD.
- CyberFundamentals (CyFun®) du CCB.
- NIST Cybersecurity Framework.
- CIS Controls.
- Référentiels de continuité d'activité.
- Référentiels de gestion d'incidents.
- Référentiels de sécurité cloud.

Certifications recherchées

- CISSP (fortement attendue).
- ISSAP (fortement appréciée).
- SABSA (fortement appréciée).
- ISO 27001 Lead Implementer.
- ISO 27001 Lead Auditor.
- ISO 27005 / Risk Manager.
- TOGAF Enterprise Architecture Practitioner.
- CCSP.

Soft Skills

- Orientation client.
- Écoute active.
- Collaboration.
- Communication.
- Pédagogie.
- Esprit critique constructif.
- Pragmatisme.
- Transparence.
- Intégrité.

- Rigueur.
- Autonomie responsable.
- Transmission des connaissances.
- Neutralité technologique.

Formation

- Master en Informatique ou en Cybersécurité ou en Sécurité des Systèmes d'Information ou en Réseaux et Télécommunications ou en Sciences de l'Ingénieur ou expérience équivalente démontrable en architecture cybersécurité.