

## Fonction

### ARCHITECTE SECURITE IV.B (H/F)

## Évolutions possibles

### Au sein du métier

- [ARCHITECTE D ENTREPRISE IV.B \(H/F\)](#)
- [ARCHITECTE SOLUTION IV.A \(H/F\)](#)
- [ARCHITECTE SOLUTION IV.B \(H/F\)](#)
- [ARCHITECTE TECHNIQUE IV.A \(H/F\)](#)
- [ARCHITECTE TECHNIQUE IV.B \(H/F\)](#)
- [ARCHITECTE DATA IV.A \(H/F\)](#)
- [ARCHITECTE SECURITE IV.A \(H/F\)](#)
- [ARCHITECTE SECURITE IV.B \(H/F\)](#)
- [ARCHITECTE FONCTIONNEL IV.A \(H/F\)](#)

## Raisons d'être

Il constitue l'autorité technique sur les architectures de sécurité, définit les modèles de sécurité et accompagne le développement des architectures de sécurité au sein du SI, en cohérence avec la stratégie IT et les politiques de sécurité de l'organisation.

## Missions

L'architecte sécurité des SI s'assure que les choix techniques et technologiques des projets IT et métiers respectent les exigences de sécurité de l'organisation. Ses missions consistent à :

- Coordonner les actions de mise en œuvre de la cybersécurité sur l'ensemble des couches d'architecture
- Contribuer à la mise en œuvre d'une sécurité différenciée en prenant en compte les enjeux métier et les risques
- Concevoir et mettre en œuvre le socle d'architecture transverse soutenant la sécurité du SI (les composants de référence réutilisables et à intégrer dans les solutions SI)
- Identifier et qualifier les risques sécurité d'une solution et formuler des préconisations

Les activités clés sont :

- Établir la stratégie des architectures de sécurité des SI en lien avec la stratégie globale métier et contribuer à la déclinaison des principes du modèle de sécurité globale
- Définir l'architecture du socle transverse de sécurité (ex. gestion des identités et des accès), ainsi que les architectures types et les composants réutilisables de sécurité (ex. pour l'authentification)
- Contribuer et /ou réaliser les analyses de risques sécurité SI menées par les acteurs sous la responsabilité SSI
- Collaborer avec les RSSI, garants de la sécurité des SI, pour définir des réponses aux risques cyber
  - Contribuer à la définition des politiques et règles de sécurité
  - Encadrer et apporter son support aux architectes de solutions et aux équipes de développement lors des projets sur les aspects sécurité
  - Contribuer à l'alimentation et à l'entretien du cadre de référence sécurité
- Conseiller sur l'utilisation et la combinaison des briques de sécurité existantes.
- Analyser les risques de sécurité liés à l'introduction de nouvelles technologies ou de nouveaux systèmes d'information.
- Assurer une veille sur les nouvelles menaces et en tenir compte dans la définition des architectures de sécurité.
- Maintenir des relations avec les fournisseurs pour assurer une veille technologique sur les innovations

et les outils de sécurité en vue de les intégrer dans les architectures de sécurité le cas échéant

- Contribuer à la montée en maturité des architectes techniques et des urbanistes en matière de sécurité des SI Collaborer avec les spécialistes techniques de sécurité pour consolider une vue globale de la sécurité.

## Compétences

### Comportementales Socles

#### Orientation client

Enrichir l'expérience client en adoptant une posture de service et de conseil et développer une relation de confiance durable. Anticiper, analyser, comprendre les besoins et attentes de ses clients pour apporter des réponses personnalisées. S'appliquer à améliorer la satisfaction client et mesurer son niveau de satisfaction.

#### Culture du changement et de l'innovation

Encourager et accompagner le changement et les initiatives d'amélioration dans un environnement complexe et incertain. Expérimenter, tester, évaluer en s'appuyant sur de nouvelles méthodes, y compris numériques. Comprendre et susciter l'innovation en remettant en question les usages et en osant être pionnier. Etre dans une dynamique d'identification et d'apport de nouveautés dans son activité en osant sortir du cadre pour penser le problème en dehors de ses limites et de ses moyens lorsque la situation le demande.

#### Coopération et ouverture

Construire et faire vivre des réseaux informels ou structurés d'individus ou de groupes en s'appuyant sur les outils collaboratifs comme les réseaux sociaux internes. Participer individuellement à l'atteinte d'un résultat collectif en favorisant l'entraide et le partage de connaissances. Savoir fédérer les parties prenantes d'un projet autour d'un objectif commun et établir des partenariats. Faire preuve d'écoute active vis-à-vis de ses interlocuteurs et prendre en compte leurs problématiques et les objections émises dans ses actions et prises de décision. Etre ouvert(e) d'esprit et curieux(se) au sein de son environnement.

#### Orientation résultats

Engager des actions et mobiliser en toute autonomie des ressources (financières, matérielles, techniques, numériques et humaines) pour atteindre des performances durables dans le respect des principes éthiques, de qualité de vie et de RSE. Savoir être proactif et fixer, pour soi et/ou pour d'autres, des objectifs ambitieux et exploiter des opportunités pour aller au-delà des attendus.

## Cyber Sécurité

### Sécurité des réseaux et protocoles

Mettre en place, maintenir et améliorer les pratiques établies en matière de sécurité des réseaux (ex : NIPS, anti-malware, restriction/empêchement dispositifs externes, filtres anti-spam) et des protocoles. Maîtriser des outils d'analyse de réseau pour identifier les vulnérabilités (ex : fuzzing, nmap, etc.). Reconnaître et interpréter une activité réseau malveillante dans le trafic. Maîtriser l'utilisation d'analyseurs de protocoles. Maîtriser la configuration et l'utilisation des composants de protection des réseaux (par exemple, pare-feu, VPN, systèmes de détection des intrusions dans les réseaux)

### Sécurité des systèmes d'exploitation

Maîtriser la sécurité des systèmes d'exploitation (poste de travail, serveur, mobile) connus sur le marché (Windows, Linux, iOS, Android, etc.) : méthodes de durcissement, connaissance des outils de sécurité natifs, connaissance des principales attaques.

### Sécurité des architectures

Concevoir des architectures de sécurité qui répondent aux besoins fonctionnels et techniques exprimés par les projets, en respectant le modèle d'architecture de l'entreprise et la PSSI. Supporter les équipes de conception et intégration des solutions jusqu'à la mise en oeuvre. Contribuer aux analyses de risques. Partager ses connaissances pour la rédaction de politiques

## Efficacité professionnelle

### Synthèse

Savoir trier, analyser et isoler les informations essentielles des informations accessoires. Consolider des informations pour réaliser une synthèse.

### Animation fonctionnelle

Animer des groupes de travail et/ou un réseau. Faciliter la communication au sein de l'équipe en faisant circuler les informations relatives à l'activité.

### Transfert de compétences

Maîtriser l'ensemble des techniques et outils et les leviers d'action permettant de faire preuve de pédagogie. Savoir transmettre des connaissances.

### Langues étrangères

Comprendre une / plusieurs langues et s'exprimer oralement et à l'écrit avec clarté et précision de façon à se faire comprendre de ses interlocuteurs.

## Analyse du besoin Client / Partenaire / Collaborateur

Comprendre, analyser et challenger les besoins et attentes de ses clients / partenaires / collaborateurs, en prenant en considération leurs contraintes et les risques associés. Conseiller et alerter au regard de leurs choix.

## Pilotage et gestion de l'activité

### Analyse de la performance et rentabilité

Analyser la performance d'un projet à un instant t (analyse et contrôle des coûts, des données budgétaires réalisées vs prévisionnelles, du Cash Flow, analyse d'un compte de résultats, calcul de coûts unitaires, calcul de prix de revient...) et optimiser sa rentabilité à moyen et long terme (gestion prévisionnelle et estimation des coûts, scénarios prédictifs, simulation d'impacts, résultats prospectifs, etc.).

## Techniques SI

### Méthodes et principes de mise en production

Connaître les Normes et Standards Informatiques Internes (SNI), les méthodes, principes, contraintes de mise en production et d'exploitation ainsi que les méthodes suivant un processus itératif (méthode agile, devops) ou cycle en V. . .

### Gestion de la livraison des services

Maîtriser l'enregistrement et le suivi des données de fiabilité. Gérer l'escalade, les recommandations, la maintenance des outils de contrôle . . .

### Stratégie et gouvernance SI

Définir et aligner la stratégie de gouvernance du SI en l'intégrant dans la stratégie de gouvernance de l'entreprise. Adapter la stratégie de gouvernance du SI en tenant compte des nouveaux événements majeurs issus des domaines juridiques, économiques, politiques, commerciaux, technologiques ou environnementaux.

### Conception et promotion d'une solution conforme aux demandes du client

Construire le volet technique de l'offre de services et expliquer au client les choix effectués.

### Qualification du risque Métier associé à une solution

Savoir qualifier le risque métier d'une solution à travers : - PCA (Plan de continuité d'activité). - PRA (Plan de reprise d'activité). - Réversibilité des contrats

### Technologies et solutions de l'architecture technique et de production

Connaître les technologies et solutions suivantes : - Solutions de développement logiciel (plateforme IDE Eclipse, intégration continue. . .) - Solutions du Décisionnel (Powercenter, BOXI, BI,...) et du domaine digital (Big Data) - Interfaces (ETL, API, Exposition de Services, temps réel. . .) - Réseaux, impression, services de messagerie, bus applicatif. . . - Solutions d'infrastructures (socles scalables et performants, cloud management) - Solutions réseaux (DSL, ATM, RNIS, 3G, offres opérateurs télécom. . .) - Solutions de bases de données et d'échange de données (structurées et non structurées) Concevoir, créer et déployer les infrastructures Big Data - Solutions d'archivage et de stockage (SAN, NAS, Baie et Interco. . .) - Solutions de déploiement, d'ordonnancement et de supervision - Solutions de virtualisation et d'automatisation (Cloud computing, SaaS, PaaS, IaaS. . .)

### Cartographie, principes et composants de l'architecture fonctionnelle et applicative

Maîtriser la cartographie, les principes et composants de l'architecture fonctionnelle et applicative : - Cartographies : fonctionnelles, applicatives, de flux, de référentiel et d'utilisateurs - Couverture fonctionnelle d'un domaine Métier et des éléments communs aux autres domaines - Référentiels de données et applications partagées par plusieurs domaines

### Cartographie, principes et composants de l'architecture technique et de production

Maîtriser les cartographies, principes et composants de l'architecture technique et de production : - Cartographie réseaux, impression, services de messagerie, bus applicatif.. - Architecture de partage, serveurs et outils distribués, implémentation CCU et RSE - SI internes/externes et cartographies des déploiements des services sur le Cloud - Référentiels d'entreprise - Urbanisation à l'échelle de l'entreprise, vision globale - Coexistence des processus internes et de l'outsourcing (BPO, ITO)

### Gestion des incidents et des problèmes

Identifier et qualifier les incidents et les problèmes. Maîtriser la méthode ITIL / GDI. Gérer la résolution des incidents (Priorisation/arbitrage, mobilisation des moyens et compétences nécessaires, escalade, activation mode dégradé. . .). Réaliser un rapport sur les incidents et les problèmes dans le cadre des processus et contrats définis.

## Prérequis

L'architecte sécurité doit être capable d'appréhender la complexification et la rapidité d'évolution des systèmes d'information, aussi bien sur un plan technique que fonctionnel.

Maîtriser les concepts d'architecture de sécurité dans des environnements en évolution (Cloud, virtualisation, API...).

## Environnement de travail

Cette fonction est exercée en relation, notamment, avec les experts sécurité ou les architectes informatiques couvrant tout le périmètre de la cybersécurité

### Famille

---

### Filière

---

### Métier

---

### Effectif de la fonction

De 1 à 9