

CONSULTANTE SENIOR

7 ans d'expérience

Cybersécurité

IAM

Cloud AWS

DevSecOps

Gouvernance sécurité

Consultante senior en cybersécurité / cheffe de projet sécurité. Mission récente IDFM : pilotage sécurité cloud & coordination multi-équipes sur migration AWS. Compétences clés : pilotage projets & Copil, gouvernance sécurité & reporting, intégration DevSecOps. Opérationnelle rapidement, forte appétence pour contexte groupe BPCE multi-entités.

FORMATIONS ET CERTIFICATIONS

2018 : Mastère en Cybersécurité et Gestion des Risques - ISFA Institut des Sciences Financières et d'Assurance, Lyon

2016 : Ingénieur en Réseaux Informatiques et Télécom - ENSA, Tanger, Maroc

COMPÉTENCES TECHNIQUES ET FONCTIONNELLES

Cloud : AWS, Azure

Gestion des identités et accès : IAM, SailPoint, Okta, Active Directory

Sécurité : PKI, HSM, Zero Trust, MFA

Langages de programmation : Java

Intégration continue (CI) : GitLab

Troubleshooting : Splunk

Outils : Nessus, Qualys

Méthodes : DevSecOps, Devops

EXPÉRIENCES PROFESSIONNELLES

IDFM, de mars 2025 à mars 2026

Consultante senior en sécurité cloud

Contexte du projet :

Sécurisation des migrations des assets vers cloud et renforcement de la sécurité cloud. Dans le cadre de la migration des actifs informatiques vers le cloud, la mission consistait à concevoir et mettre en œuvre des architectures de sécurité robustes, à assurer la conformité réglementaire et à renforcer la gouvernance de la sécurité dans un environnement cloud AWS.

- Conception et mise en œuvre d'architectures de sécurité adaptées aux exigences métiers, réglementaires et techniques
 - gestion des identités (IAM)
 - infrastructure à clés publiques (PKI)
 - chiffrement des données
 - gestion des clés
 - utilisation de modules matériels de sécurité (HSM)
 - application du modèle Zero Trust
- Élaboration et déploiement de la stratégie de sécurité Cloud AWS dans le cadre de la migration des actifs informatiques vers le cloud
- Réalisation d'analyses de risques cryptographiques portant sur l'exposition des clés, le choix des algorithmes et la gestion du cycle de vie des secrets
- Mise en place et gouvernance de la gestion des composants cryptographiques
 - gestion des certificats
 - gestion des clés
 - processus de rotation et de révocation
 - contrôle de la conformité des usages
- Coordination transverse entre les équipes sécurité et les chefs de projet techniques pour garantir la conformité et la sécurité des infrastructures et des migrations Cloud
 - équipes audit
 - SOC
 - RGPD
 - contrôle interne
- Animation de comités de pilotage (Copil), de comités de projet (Coproj) et de workshops pour assurer le suivi hebdomadaire et mensuel des projets de sécurité
- Pilotage de projets d'intégration de solutions de sécurité et de conformité
 - IAM
 - IDS/IPS
 - PAM
 - EDR CrowdStrike
 - Qualys
 - durcissement des environnements Cloud
- Définition et intégration des exigences de sécurité dans les processus d'exploitation et de livraison continue CI/CD en mode devSecOps
- Mise en place d'une gouvernance sécurité avec élaboration de tableaux de bord, définition d'indicateurs, suivi des plans de remédiation et reporting régulier
- Validation de la conformité des solutions avec les standards et référentiels réglementaires

- RGPD
- ISO 27001
- NIS2
- Accompagnement des projets selon une approche Crypto et security by Design
 - choix des algorithmes
 - définition des modèles de confiance
 - gestion du cycle de vie des secrets
- Conduite de Proof of Concept (POC) pour l'évaluation de solutions cryptographiques
 - HSM
 - KMS
 - PKI
 - chiffrement applicatif
 - tokenisation
- Contribution à l'amélioration continue des mécanismes de protection des données, des applications et des échanges

Environnement technique :

AWS, IAM, PKI, HSM, ZERO TRUST, CROWDSTRIKE, QUALYS, IDS/IPS, PAM, CI/CD, DEVSECOPS, RGPD, ISO 27001, NIS2

CA, de juin 2024 à décembre 2024***Consultante senior SSI*****Contexte du projet :**

Design et sécurisation des applications dans des environnements cloud hybrides. Projet de sécurisation et de design d'applications dans des environnements cloud hybrides, avec un accent sur la gestion des identités, la cryptographie, la conformité réglementaire et la gestion des vulnérabilités.

- Renforcement de la sécurité des applications cloud et M365 à travers Entra AD, avec intégration de mécanismes cryptographiques d'authentification forte
 - certificats
 - clés
 - tokens
 - MFA
- Évaluation des risques de sécurité cloud en collaboration avec les équipes
 - gestion de l'exposition des secrets
 - gestion des clés et certificats
 - configuration des protocoles TLS
 - conformité des algorithmes utilisés
- Pilotage et participation à l'intégration de solutions de cryptographie
 - PKI
 - gestion de clés (KMS/HSM)
 - signature électronique
 - chiffrement des données au repos
 - chiffrement en transit
 - chiffrement applicatif
- Gestion et implémentation des patches de sécurité suite aux tests d'intrusion réalisés en recette, préproduction et production

- Planification et priorisation des activités de maintenance pour garantir la disponibilité et la performance des services de sécurité
- Préparation, installation, paramétrage et validation des nouvelles versions des composants cryptographiques lors des évolutions techniques
- Veille technologique et suivi des alertes de sécurité pour anticiper les vulnérabilités et les évolutions des produits cryptographiques
- Planification et déploiement des correctifs de sécurité dans le respect des exigences de continuité de service
- Recommandation et mise en œuvre de contre-mesures
 - IAM
 - WAF
 - XDS
 - RBAC
 - MFA
 - définition des alertes basées sur les risques et menaces
- Contribution à la mise à jour de la politique de sécurité (PSSI) et des stratégies de sécurité des accès à privilèges
- Élaboration des plans d'action et suivi de la mise en œuvre des mesures de sécurité, participation aux investigations et réponses aux incidents
- Scripting et automatisation des scans, tests d'intrusion et analyses d'audits techniques des infrastructures
 - Nessus
 - Burp Suite
- Gestion des vulnérabilités
 - Microsoft Defender
 - Qualys
 - Tenable
- Formation des équipes aux bonnes pratiques de sécurité et cloud
- Analyse et ajout de règles et configurations de sécurité
 - Splunk
 - Microsoft Sentinel
 - Azure Policy (playbooks, logs, alertes, events)
- Mise en place de règles de rotation des mots de passe et d'accès Just-In-Time (JIT)
- Rédaction de rapports, recommandations et documentation technique
 - DAT
 - HLD
 - LLD

Environnement technique :

ENTRA AD, M365, PKI, KMS, HSM, TLS, IAM, WAF, XDS, RBAC, MFA, MICROSOFT DEFENDER, QUALYS, TENABLE, NESSUS, BURP SUITE, SPLUNK, MICROSOFT SENTINEL, AZURE POLICY, CI/CD

AXA FRANCE, de juin 2022 à décembre 2023**Consultante senior en cybersécurité****Contexte du projet :**

Migration vers One Account et renforcement de la sécurité cloud. Projet de migration vers une solution centralisée de gestion des identités et des accès (One Account) et renforcement de la sécurité cloud pour les applications métiers et l'infrastructure hybride.

- Participation à la réalisation d'un Proof of Concept (POC) pour la migration du Web Access Control (WAC) vers la solution One Account, permettant la gestion centralisée des identités et des accès
- Renforcement des mécanismes d'authentification et d'autorisation
 - MFA
 - OTP
 - SSO
 - SSL/TLS
 - Kerberos
 - certificats X509
 - SAML
 - OIDC
- Participation à la conception et au déploiement d'une architecture hybride intégrant PingIdentity, Active Directory on-premises et Entra ID
- Pilotage de l'intégration d'applications métier dans Entra ID et Office 365, en conformité avec les règles de sécurité
- Configuration et implémentation des politiques de sécurité, des workflows, des groupes et des rôles RBAC, ainsi que des outils Ms Defender et Azure Key Vault
- Conception et mutualisation des données utilisateurs dans l'Active Directory (AD)
- Contribution à la migration des applications web vers une infrastructure multi-tenant
- Sécurisation des applications web dans les environnements CaaS et proposition de correctifs de sécurité
- Collaboration avec les équipes DevOps pour automatiser les déploiements WAC et garantir la conformité avec les normes de sécurité
- Participation à la rédaction des documents HLD, LLD et production de la documentation projet incluant les exigences et l'étude de budget

Environnement technique :

ONE ACCOUNT, WAC, MFA, OTP, SSO, SSL/TLS, KERBEROS, X509, SAML, OIDC, PINGIDENTITY, ACTIVE DIRECTORY, ENTRA ID, OFFICE 365, RBAC, MS DEFENDER, AZURE KEY VAULT, CAAS, DEVOPS

AXA FRANCE, de septembre 2020 à mai 2022*Consultante experte en cybersécurité***Contexte du projet :**

IT Refresh - Move to cloud et Mise en conditions opérationnelles de l'infrastructure Private IAAS. Projet de migration massive d'applications vers le cloud privé (PIAAS) et mise en conditions opérationnelles de l'infrastructure, avec un focus sur la sécurité, la gestion des vulnérabilités et la continuité d'activité.

- Évaluation de la sécurité de l'infrastructure Private IAAS (PIAAS) et veille continue sur les vulnérabilités du Web Access Control (WAC)
- Onboarding des applications et pilotage de la migration vers le cloud PIAAS pour 321 applications, couvrant les environnements de recette, préproduction et production
- Réalisation d'un healthcheck avec l'éditeur Broadcom et application des correctifs sur les serveurs reverse proxies et les politiques IAM
- Évaluation des risques liés aux migrations afin de garantir la qualité de service
- Configuration du WAC et évaluation des impacts des changements en collaboration avec les responsables applicatifs, DevOps et testeurs
- Mise en place de cookies sécurisés et migration de 326 applications de HTTP vers HTTPS
- Analyse des causes racines, debugging, analyse des logs et résolution des incidents (support niveau 3, maintien en conditions opérationnelles)
- Protection des applications web via WAC, assurant une gestion sécurisée de l'authentification et de l'autorisation pour 357 applications
- Sécurisation du pipeline CI/CD pour les déploiements de configurations sur Azure DevOps
- Décommissionnement des serveurs reverse proxy et suppression des politiques obsolètes sur site
- Contribution aux opérations de disaster recovery et à la planification de la continuité des activités (BCP)

Environnement technique :

PIAAS, WAC, BROADCOM, IAM, AZURE DEVOPS, CI/CD, DEVOPS

ENGIE, de février 2020 à septembre 2020**Consultante en architecture & intégration des solutions****Contexte du projet :**

Intégration de la solution Saviynt et Okta. Projet d'intégration des solutions Saviynt et Okta pour la gestion des identités et des accès, incluant la migration depuis CA Identity et la mise en conformité avec les standards de sécurité de l'organisation.

- Conception, planification et supervision des tests d'intégration des solutions Saviynt et Okta
- Coordination avec l'équipe projet pour la bascule, l'installation et le suivi d'avancement des solutions
- Participation au projet MyIdentity pour la migration de CA Identity vers Saviynt
- Intégration de Saviynt dans l'infrastructure et les systèmes informatiques existants
- Gestion du référentiel LDAP
 - création de serveurs
 - création d'instances
 - création de schémas
 - réplication
 - monitoring
- Mise en place du MFA et configuration d'Okta avec Saviynt pour répondre aux standards de sécurité de l'organisation
- Organisation de sessions de formation pour les utilisateurs finaux sur l'utilisation des solutions intégrées Saviynt et Okta
- Rédaction de procédures techniques et de reporting

Environnement technique :

SAVIYNT, OKTA, LDAP, MFA

RTE, de octobre 2019 à janvier 2020**Architecture & Intégration****Contexte du projet :**

POC de migration vers SailPoint pour répondre aux exigences sécurité. Preuve de concept (POC) de migration vers SailPoint pour répondre aux exigences de sécurité et automatiser les processus de provisionnement des utilisateurs.

- Identification et analyse des sources de données existantes pour préparer l'infrastructure cible
- Conception de l'architecture cible et rédaction du Dossier d'Architecture Technique (DAT)
- Installation, intégration et configuration de SailPoint IdentityNow
 - application
 - policy server
 - annuaire
 - référentiels
 - revues d'accès
- Test de la connectivité et de la synchronisation des données entre les systèmes
- Démonstration de l'implémentation de SailPoint et validation de sa capacité à automatiser les processus de provisionnement des utilisateurs
- Documentation de toutes les activités réalisées et formulation de recommandations pour le déploiement de SailPoint

Environnement technique :

SAILPOINT IDENTITYNOW, DAT

CAPS, de novembre 2018 à septembre 2019

DevSecOps

Contexte du projet :

Sécurisation des applications web et personnalisation de l'intégration. Projet de sécurisation des applications web et personnalisation de l'intégration IAM, avec un focus sur la conformité, l'automatisation et le support aux utilisateurs finaux.

- Configuration et mise en place des politiques de sécurité et des workflows pour les processus de gestion des identités et des accès
 - onboarding
 - approbation
 - recertification
- Customisation de SailPoint pour répondre aux exigences spécifiques de l'organisation
- Support de niveau 3 aux utilisateurs finaux et garantie du bon fonctionnement des systèmes IAM
- Application des politiques de sécurité et des normes de conformité IAM
- Déploiement des évolutions fonctionnelles et des patches de sécurité pour répondre aux normes de conformité IAM
- Intégration des pratiques de sécurité dans le pipeline DevOps, développement et déploiement des correctifs en Java via GitLab
- Automatisation, scripting et gestion du versioning avec GitLab
- Test, validation des livrables et rédaction de la documentation opérationnelle
- Gestion des identités, des habilitations et accompagnement client
- Documentation des processus, configurations et bonnes pratiques pour assurer le partage des connaissances

Environnement technique :

SAILPOINT, IAM, JAVA, GITLAB, DEVOPS

ENGIE, TOTAL ENERGIE, de janvier 2018 à septembre 2018

Security Analyst

- Client Engie - GAIA : Intégration d'une infrastructure IAM avec WSO2
Projet d'intégration d'une infrastructure IAM pour la gestion des identités et des accès, en utilisant WSO2 et Broadcom, avec une attention particulière à la sécurisation des applications et à la documentation technique.
 - Sécurisation des applications pour la gestion des identités et des accès à l'aide des solutions Broadcom
 - Définition des besoins et rédaction des spécifications techniques pour l'intégration IAM
 - Installation, configuration et déploiement des composants WSO2 pour la gestion des identités et des accès
 - Mise en place des workflows d'autorisation et de création de compte
 - Intégration des solutions ForgeRock pour la gestion de l'identité et des accès
 - Démonstration et documentation de l'ensemble du processus de mise en œuvre de l'implémentation
- Client Total Energie : Intégration IAM et développement d'une application de reporting en Java
Projet d'intégration d'une infrastructure IAM et développement d'une application de reporting en Java, avec automatisation des workflows et gestion du cycle de vie des identités.
 - Raccordement des applications pour la gestion des identités et des accès avec les solutions Broadcom
 - Identification des besoins en automatisation et rédaction des spécifications techniques pour le projet IAM
 - Conception, développement et déploiement d'une application Java dédiée au suivi de la configuration IAM
 - Intégration de l'API Talend pour automatiser les tâches de workflow, les notifications, ainsi que la génération et la distribution de rapports
 - Mise en place de fonctionnalités permettant de gérer et d'automatiser les changements de configuration dans les tâches Talend
 - Établissement des workflows de création de comptes et d'autorisations, et mise en œuvre des processus de cycle de vie des identités

- Automatisation des notifications, de la génération et de la distribution des rapports
- Test, validation de la livraison et rédaction de la documentation d'exploitation

Environnement technique :

WSO2, BROADCOM, FORGEROCK, JAVA, TALEND

Langues : Français (Courant), Anglais (Courant)

CERTIFICATIONS



**Certification Azure AZ500
Security Engineer 2024**



Prince 2 Foundation 2024



**Certification Azure AZ900
2023**



**Certified Ethical Hacker CEH
2023**



Certification ITIL V3 2019



**CCNA Associate Routing &
Switching 2017**



CCNA Academic 2016



HUAWEI SEEDS FOR THE FUTURE 2015