



SAB

CONSULTANTE SSI / ASSISTANTE RSSI (N3)

DOMAINES DE COMPÉTENCES

Savoir-faire	Activités GRC <ul style="list-style-type: none">• Gestion et Pilotage de projets de Cybersécurité• Intégration de la sécurité dans les projets• Accompagnement à la certification : ISO27001• Participation à l'accompagnement à la mise en conformité : NIS2• Revue de documentation techniques et règlementaires• Production des livrables et Indicateurs• Proof of Concept• Animation de réunion• Veille réglementaire : DORA, PCI-DSS
	Gestion de crise <ul style="list-style-type: none">• Identification des cellules et production de procédures• Exercice de simulation d'exercices de crise• Identification de scénarios• Préparation et formation des équipes
	RUN et Sécurité Opérationnelle <ul style="list-style-type: none">• Gestion d'incident• Gestion des accès et Habilitations• Suivi des vulnérabilités : CVE / Plan de remédiations
	Sensibilisation et formation <ul style="list-style-type: none">• Animation de formation en Cybersécurité et Ebios RM• Accompagnement des utilisateurs (Métiers et Collaborateurs)• Campagne de sensibilisation aux bonnes pratiques
Outils	Fortinet, Alert Crisis, Risk'ntic, EGERIE RM, All4tech
Normes et Méthodes	ISO27001, ISO22301, EBIOS RM, NIS2, DORA

DIPLÔMES

- 2019 : Master 2 Cybersécurité et E-santé
- 2017 : Double Licence en Sécurité des Réseaux & Informatique

FORMATIONS PROFESSIONNELLES & CERTIFICATIONS

- 2025 : NIS2 Lead Implementer
- 2021 : EBIOS RISK MANAGER
- EGERIE RISK MANAGEMENT
- FORTINET NSE1 & NSE2

LANGUES

- **Anglais** : Courant

EXPÉRIENCES PROFESSIONNELLES

CONSULTANTE GRC | CYBERDIAN GROUPE

 Depuis Mars 2025

Contexte : En tant que consultante Gouvernance, j'interviens pour la préparation à la certification ISO 27001 et d'autres projets internes. Mon rôle est d'accompagner l'organisation tout au long du processus de mise en conformité avec les exigences de cette norme de sécurité de l'information en collaboration avec le R-SMSI.

Missions :

ACCOMPAGNEMENT NIS2

- Étude du besoin
- Identification des étapes clefs
- Structuration de l'approche de l'accompagnement à la mise en conformité à la directive NIS2
- Production d'un macroplanning pour un déploiement efficace et structuré
- Identification de la documentation à produire par étapes (Feuille de route, rapports, politiques...)
- Identification des procédures de test et simulation de crise
- Formation et sensibilisation

CERTIFICATION ISO27001

- Gap Analysis : Évaluation de l'existant par rapport aux exigences
- Relecture des politiques
- Recensement des exigences par politiques
- Définition des politiques répondant à ces exigences
- Participation aux réunions de suivi
- Reporting

Formation

- Animation de formation EBIOS RM
- Préparation des supports de formation : EBIOS RM
- Accompagnement pédagogique

Environnement Technique : NIS2, ISO27001, ISO27005, ISO22301

CONSULTANTE / REFERENTE GRC | CEGEDIM BUSINESS SERVICES

 Février à Novembre 2024

Contexte : En tant que consultant intervenant chez Cegedim Business Services, j'ai contribué à la gestion et à l'amélioration de la sécurité des systèmes d'information, en accompagnant les équipes dans la mise en conformité ISO 27001 et en pilotant des projets liés au plan de traitement des risques.

Missions :

Production et Gestion des Politiques de Sécurité

- Élaboration de la politique globale, charte, et les différentes politiques et procédures spécifiques.
- Identification des plans de zonages pour définir les niveaux d'accès aux différentes zones sensibles.
- Rédaction d'un guide des bonnes pratiques en matière de sécurité.
- Gestion des incidents de sécurité : identification et résolution des incidents

Gestion des Exceptions et Suivi des Accès

- Mise en place et gestion des exceptions pour les accès applicatifs.
- Révocation des exceptions en fonction des besoins et des évolutions de sécurité.

- Production de fichiers de suivi trimestriels pour assurer une supervision continue des accès.

Protection des Données et Prévention des Fuites (DLP)

- Implémentation de mesures de protection des données, incluant le blocage des ports USB.
- Contrôle et gestion des accès aux supports amovibles pour limiter les risques de fuite d'informations.

Évaluation des risques

- Coordination des experts pour assurer l'avancement du plan de traitement des risques
- Gestion d'obsolescences des applicatifs et des serveurs

Sensibilisation

- Fournir des recommandations et former les équipes pour renforcer la sécurité globale
- Scénarios de phishing
- Campagne de sensibilisation (classification de données, bonnes pratiques de sécurité et satisfaction collaborateurs).

Environnement Technique : ISO27001, ISO27005, ISO22301

CHEF DE PROJET/ CONSULTANTE CYBERSECURITE I LA POSTE MOBILE

 **Mai 2023 à Août 2023**

Contexte : En tant qu'ingénieure cybersécurité, j'étais chargé de piloter le projet de mise en place de la clef de sécurité Yubikey, pour tous les collaborateurs de La Poste Mobile. Ce projet visait à renforcer la sécurité des authentifications des utilisateurs et faciliter l'usage.

Missions :

MISE EN PLACE D'UNE AUTHENTIFICATION MULTIFACTORIELLE (MFA) :

- Analyse des besoins de sécurité de l'entreprise et définition des scénarios d'utilisation du MFA.
- Configuration et déploiement d'une solution d'authentification forte pour renforcer les accès sécurisés.
- Réalisation de tests pour valider la robustesse et la compatibilité de la solution MFA avec l'environnement existant.

INTÉGRATION D'UNE SOLUTION D'AUTHENTIFICATION POUR LA CONNEXION SÉCURISÉE À WINDOWS VIA LE PROTOCOLE PIV :

- Déploiement du protocole PIV (Personal Identity Vérification) pour permettre une authentification forte sur les terminaux Windows.
- Configuration des certificats d'authentification et des clés privées sur les supports de sécurité.
- Pilotage de la mise en place d'une PKI.
- Formation des utilisateurs à l'utilisation de la clef de sécurité Yubikey..

DÉPLOIEMENT D'UNE SOLUTION (ONE-TIME PASSWORD) :

- Paramétrage de dispositifs d'authentification pour générer des mots de passe à usage unique.
- Intégration du protocole OTP avec les systèmes existants pour simplifier et sécuriser la gestion des mots de passe.
- Rédaction de guides techniques pour accompagner les équipes IT dans l'utilisation de la clef de sécurité avec le gestionnaire de mots de passe.

Encadrement d'une Équipe Projet :

- Planification et suivi des tâches des membres de l'équipe pour respecter les échéances et les livrables.
- Animation des réunions de projet pour assurer la bonne communication entre les parties prenantes.
- Gestion des risques et résolution des problèmes rencontrés durant le projet.

Réalisation des livrables et présentation à la direction :

- Élaboration de rapports détaillant les objectifs atteints, les bénéfices des solutions

- déployées et les étapes futures.
- Présentation des livrables et des résultats techniques à la direction, en mettant en avant les gains en sécurité et en productivité.
- Proposition de recommandations pour de futurs projets d'amélioration de la sécurité.
- Rédaction de la procédure d'accompagnement à l'implémentation de l'outil (à destination des équipes techniques)
- Rédaction de la procédure d'accompagnement à l'utilisation de l'outil (à destination des collaborateurs)

ENSEIGNANTE CYBERSECURITE | CAMPUS DE CRETEIL IAE GUSTAVE EIFFEL

 Depuis Janvier 2022

Missions :

- Production des supports pédagogique de cours (Master 1 et 2 sécurités du SI)
- Production des tests et évaluations (TP, TD, examens)

CONSULTANTE / CHEF DE PROJET CYBERSECURITE | KERING TECH

 Janvier à Décembre 2021

Contexte : Au sein de l'entreprise Kering Tech, entreprise de l'univers du luxe, mon rôle est de piloter et de structurer le projet de gestion de crise et DRP au sein de l'organisation. L'objectif est d'assurer la résilience face aux incidents majeurs en définissant un cadre clair, en formant les équipes et en mettant en place des outils et processus adaptés. Ces projets s'inscrivent dans une démarche globale visant à renforcer la sécurité et la réactivité de l'entreprise face aux cybermenaces et incidents critiques.

Missions :

PILOTAGE DE PROJET DE GESTION DE CRISE

- Cadrage des besoins et étude de l'existant en matière de gestion de crise.
- Identification des cellules de crise et de leurs membres (décisionnelle, opérationnelle et régionale).
- Formation des équipes sur la gestion de crise et les processus associés.
- Mise en place d'une solution d'alerting adaptée à l'environnement de Kering :
 - Organisation et pilotage du projet de bout en bout.
 - Adaptation de la solution aux contraintes internes et aux besoins métiers.
 - Coordination avec les équipes techniques pour l'intégration et les tests.
 - Production des guides Key holders pour faciliter les actions en situation d'urgence.
- Mise en place d'un canal de gestion de crise à distance pour assurer la continuité des échanges.
- Définition et formalisation du processus d'escalade d'un incident à une crise.
- Identification de la documentation clé pour la gestion de crise :
 - Fiches réflexes pour guider les actions immédiates.
 - Logbook pour le suivi en temps réel des événements.
 - Plan d'action pour structurer la réponse et le retour à la normale.

Simulation et exercices de gestion de crise

- Identification de scénarios impactant plusieurs régions et leurs implications.
- Sélection des applicatifs critiques et des membres à tester.
- Configuration des canaux et supports (fiches de rôle, politique de gestion de crise, slides de formation).
- Suivi du déroulement de l'exercice et gestion des incidents simulés.
- Participation à la production du rapport de gestion de crise avec recommandations.

Coordination et communication

- Animation et participation aux réunions de suivi avec le Top Management.

- Présentation des avancées du projet et des enseignements tirés des exercices.
- Sensibilisation des parties prenantes à l'importance d'une gestion de crise efficace.

EXERCICE DE REPLI – DRP (DISASTER RECOVERY PLAN)

Planification et coordination des exercices de repli :

- Assurer la coordination des bascules dans le cadre des exercices de continuité de service
- Identification des impacts potentiels et coordination avec les équipes techniques et métiers.
- Participation à l'élaboration d'un planning détaillé pour assurer la fluidité des opérations et limiter les perturbations.

Participation aux activités opérationnelles du DRP :

- Coordination et communication avec les parties prenantes pour garantir une compréhension commune des objectifs et des processus.
- Rédaction et mise à jour des supports de communication pour les comités de suivi.
- Documentation et formalisation des retours d'expérience pour améliorer continuellement la stratégie DRP.
- Mise en place des actions correctives nécessaires pour garantir la résilience du SI.

Environnement technique : ISO22301

CONSULTANTE CYBERSECURITE/ ASSISTANTE-RSSI | COPARTIS FILIALE DE BNP PARIBAS

 Aout 2019 à Décembre 2020

Contexte : En tant qu'Adjointe RSSI chez Copartis, entreprise spécialisée dans le routage de flux bancaires, mon rôle consiste à épauler le Responsable de la Sécurité des Systèmes d'Information (RSSI) dans la mise en place et le suivi de la stratégie de cybersécurité.

Missions :

Business Impact Analysis (BIA)

- Animation des workshops pour la construction des BIA (Finance, RH,...) conformément aux exigences du groupe BNP.
- Sensibilisation des parties prenantes sur les enjeux des BIA.
- Alignement des critères d'impact business avec les RTO des infrastructures de la DSI.
- Mise à jour des tableaux de bord pour reporting au RSSI et au groupe.

Habilitation (Gestion des accès)

- Validation des accès via l'outil interne d'habilitation.
- Revue trimestrielle des habilitations avec les responsables métiers.
- Administration de la solution de transfert de fichiers sécurisé (SecureFileSharing).

Fiche de Sécurité de Projet (ISP)

- Accompagnement des équipes projet sur la mise en place de nouveaux projets DSI.
- Analyse des risques avec les responsables métiers et les porteurs de projet.
- Recommandations sur les aspects de sécurité (authentification, chiffrement, etc.).
- Soumission et validation des risques résiduels au RSSI (gestion des dérogations).
- Application de la méthodologie de gestion des risques EBIOS RM et évolution du template de fiche de sécurité.
- Utilisation des outils Risk'nTick & Egerie.

RGPD (Rattaché au DPO du groupe)

- Création et mise à jour du registre des traitements (article 30).
- Collaboration avec chaque responsable métier (12 personnes) pour identifier et localiser les données personnelles.
- Création de procédures spécifiques basées sur les politiques générales du RSSI (Alignement avec la norme ISO 27001)
- Classification des données.
- Gestion des mots de passe des utilisateurs lambda.
- Mise à jour et gestion des habilitations.

- Gestion des accès administrateurs.

Reporting au DG et DGA

- Suivi de l'état d'avancement des BIA, fiches de sécurité, politiques de sécurité et contrôles en place.
- Rédaction des rapports sur les sujets de cybersécurité (nouveaux projets, réalisations, conformité).

Analyse des CVE

- Surveillance des vulnérabilités et redirection des alertes vers les équipes IT concernées.

Sensibilisation

- Rédaction de Newsletter cyber Trimestrielle
- Animation de session de sensibilisation
 - Plateforme de Gestion de mot de passe
 - Bons pratiques sur l'utilisation d'internet
 - Clean Desk (Bureau propre)
 - Classification des données

Environnement technique : ISO27001, EBIOS RM, EGERIE, Risk'ntic, ISO22301, SharePoint,