sdoyen@expertrisk-cybertech.fr

06.61.61.31.70
8 rue Paul BROCA
66100 Perpignan

Stéphane DOYEN

Consultant Cybersécurité

Résumé Professionnel

Spécialiste en cybersécurité avec plus de 30 ans d'expérience, j'ai une expertise dans la gestion des risques et des crises complexes. J'ai dirigé avec succès des projets de conformité dans des secteurs critiques et j'ai orchestré la gestion de crises cyber pour plusieurs entités dans le domaine de la santé. J'ai également occupé le rôle de DPO pour plusieurs entités. Mon approche stratégique, alliée à une gestion d'équipes transversales, me permet de relever les défis les plus complexes tout en collaborant étroitement avec les directions et chefs de département pour assurer la transformation digitale et la sécurité de l'entreprise.

Soft Kills

Fort d'une approche méthodique et rigoureuse, j'allie autonomie et diplomatie pour naviguer avec aisance dans des milieux complexes, résoudre des problèmes de manière efficace et maintenir une dynamique de progression constante. Ma capacité à prioriser les tâches en fonction des enjeux stratégiques assure des prises de décision judicieuses, alignées avec les objectifs d'entreprise.

Compétences Métier

Gouvernance, Risque et Conformité (GRC)	• Réglementation : LPM, NIS, IGI 1300, II901 • Norme ISO 27001, HDS, ISO 27005 • Évaluation des risques Ebios-RM • Rédaction de politiques et de procédures • Elaboration PRA/PCA
Cybersécurité	• ISP – Intégration de la sécurité dans les projets • Gestion de crise • Analyse Forensic • Pilotage de sécurité opérationnelle
Management de la Sécurité et des Risques	• Collaboration étroite avec les équipes dirigeantes pour déployer une approche basée sur les risques, incluant l'analyse de l'environnement juridique et l'anticipation des menaces. • Définition et mise en place de capacités de gestion de crise. • Coordination des tests d'intrusion et des contrôles de sécurité, ainsi que la gestion des incidents de sécurité et des crises en cybersécurité
Communication et Formation en Cybersécurité	• Sensibilisation et formation aux politiques de sécurité, soutien et conseil pour assurer une compréhension approfondie de la sécurité au sein de l'entreprise. • Support en cybersécurité pour les demandes clients, y compris lors des phases d'appel d'offres.
Techniques Avancées	• Outils de réponse à incident et forensic (Kali, SIFT, FTK Imager, Volatility, etc.). • Pentests : SQLMap, Burpsuite • Monitoring : Splunk, Snort, Elasticsearch. • Administration système & réseau adapté aux exigences de sécurité.

Certifications

ISO 27001 Lead Implementer — *2019*

ISO 27005 Risk Manager — *2019*

PECB Data Protection Officer — *2019*

Diplômes – Formations

eMBA 2021 - Ecole de Guerre Economique Paris

Management des Risques, Sureté internationale, Cybersécurité

Product Manager Efficom Lille

Titre RNCP 34394 - Niveau 7

Greta Toulon - Administration des Systèmes d'Information Expert 400 h
Niveau 6 Dév. Avancé Génie logiciel

Formation informatique système CNAM - Paris
Informatique Cycle B Niveau 6

Diplôme de qualification supérieure Ministère de la Défense
Systèmes informatiques répartis, Administration de Systèmes locaux

Bénévolat

Club Ebios - Membre

Club ISO 27001 – Membre

Publication

[Le ferroviaire : instrument de puissance : Souveraineté, sécurité numérique]

Co-auteur

Expériences professionnelles

10-2024	**ExpertRisk Cybertech** (Président) *Siren : 934 011 594* *RC Pro : HSXIN320053324A* Consultant Cybersécurité – GRC (Gourvernance – Risque – Conformité) ⇨ Audit de sécurité avec gestion de crise – **PKM Logistique** ⇨ Exercices de crise avec 3 niveaux - **Confidential**
2023-2024	**Consultant Senior Gouvernance Risques Conformité** Airbus Protect (Toulouse) ⇨ Mettre en place un cadre de gouvernance et de cybersécurité pour Airbus Defence and Space dans le domaine aérospatial, en veillant à la conformité et à la sécurisation dans un environnement industriel hautement réglementé et sensible (IGI 1300, II901, LPM). ⇨ Mission pour un client externe sur la refonte de l'Atelier 4 de Ebios RM, une méthode poussée par l'ANSSI. ⇨ Collaboration avec d' autres départements de sécurité corporative, des divisions et des filiales pour assurer la définition et le déploiement de la stratégie et de la politique de sécurité de l'entreprise. ⇨ S'assurer du déploiement de la politique de sécurité par la mise en place et la gestion de la gouvernance de la sécurité. ⇨ Définition et déploiement des capacités de gestion de crise.
2021-2023	**Cyber Risk Manager France – RSSI de transition** Transdev Business Information Solutions , j'ai assumé diverses responsabilités clés pour assurer la conformité, la sécurité et la gestion des risques liés à la cybersécurité, notamment : ⇨ Évaluation et conformité aux régulations (LPM, NIS) avec consulting pour réduire les écarts identifiés, homologation des SI ; ⇨ Analyse et élaboration des politiques de sécurité des systèmes d'information, des Plans de Continuité d'Activité (PCA) et des Plans de Reprise d'Activité (PRA) ; ⇨ Examen des clauses de cybersécurité dans les contrats de service, ainsi que l'évaluation de la maturité et de la conformité des sous-traitants ; ⇨ Réalisation d'analyses de risques conforme à ISO 27005 avec la méthodologie Ebios-RM ; ⇨ Orientation des appels d'offres en intégrant les aspects de cybersécurité ; ⇨ Mise en œuvre de la cybersécurité et des clauses de sécurité par défaut dans les contrats et les révisions contractuelles ; ⇨ Intégration de la sécurité dans les projets (ISP); ⇨ Coordination des tests d'intrusion et des contrôles de sécurité préalables à la mise en service ; ⇨ Application et suivi du processus de gestion des exceptions de risques ; ⇨ Gestion de crises en cybersécurité et réponse aux incidents de sécurité.
2015-2021	**Responsable des Systèmes d'Information** Transdev HealthCare, Santé mobilité Services, filiale santé du groupe TRANSDEV, Réseau Carius et Optimos, 355 Sociétés sur 70 départements. Dans le secteur de la santé, j'ai occupé un rôle clé en tant que membre du Comité de Direction et responsable de la cybersécurité. J'ai mis en œuvre des stratégies efficaces pour assurer la sécurité des systèmes d'information et la protection des données sensibles dans un contexte HDS. Les points forts de mon expérience dans le domaine de la santé incluent : ⇨ Participation active au CODIR et collaboration étroite avec la direction générale pour définir les orientations stratégiques en matière de systèmes d'information, tant internes qu'externes ; ⇨ Élaboration des politiques de sécurité informatique, garantissant la protection des données et la conformité aux régulations du secteur (ISO 27001, HDS, RGPD) ; ⇨ Gestion des budgets SI, pilotage des contrats et de la relation avec les prestataires, assurant une utilisation optimale des ressources ; ⇨ Management d'une équipe de 12 collaborateurs répartis en 3 pôles (projet, déploiement et helpdesk), favorisant la collaboration et l'efficacité ; ⇨ Développement et mise en œuvre des PSSI pour Transdev HealthCare ; ⇨ En tant que DPO, audit, élaboration du corpus et suivi de conformité RGPD pour 60 entreprises du réseau Carius ;
2018-2024	**Mentor accompagnateur et évaluateur** OpenClassRooms Accompagnement des étudiants dans la réalisation de parcours de haut niveau, incluant l'évaluation et le suivi pédagogique des apprenants du Master 2 **« Sciences, Technologies, Mention Ingénierie des Systèmes complexes, spécialité Sécurité des Systèmes d'Information »** (Université Technologique de Troyes) et des parcours certifiant RNCP de niveau 7, tels que **« Responsable de Projet Cybersécurité SI »** et **« Chef de Projet Cybersécurité ».**
2007-2013	**Responsable Manager Application,** *Économat des Armées, EPIC Centrale d'achat et de prestations de service, Pantin (93) (Ca 520 M€, 1100 salariés)*
2004-2006	**CEO / Fondateur,** Ingénierie Micro Vidéo, Nancy (54) Prestation informatique à destination des entreprises, déploiement de réseaux internes incluant serveurs et station de travail.
1987-2003	**Carrière au sein du ministère de la Défense**, *avec une fin de carrière dans les Unités des forces spéciales, Dieuze (57)*