



GESTION DE PROJET CYBERSÉCURITÉ COMPLIANCE

PCI DSS | LPM | DORA | SOC IT/OT WORLDWIDE

- MISE EN PLACE D'UN SOC EUROPÉEN (BANQUE DE FRANCE, BUNDESBANK, BANCA D'ITALIA & ESPANIA)
- MISE EN PLACE D'UN SOC OT EN ENVIRONNEMENT INDUSTRIELLE (TRANSDEV)
- DEPLOIEMENT SECURITE (WORLDLINE/INGENICO)
- MISE EN PLACE D'UN SOC IT/OT (MANUTAN)
- TRANSFORMATION RÉSEAU ET SECURITE (APHP)
- GOUVERNANCE SECURITE (STIME / LES MOUSQUETAIRES)
- TRANSFORMATION RESEAU (ERAMET)
- DÉMÉNAGEMENT DATACENTER (HSBC)
- CERTIFICATION PCI DSS (EXPEDIA)
- CERTIFICATION PCI DSS (BANQUE ALAHLI – ARABIE SAOUDITE)
- LUTTE ANTI TERRORISME DÉPLOIEMENT CCTV (SAUDI TELECOM COMPANY)
- DÉPLOIEMENT RÉSEAU ET SECURITE AU NIVEAU NATIONAL (ACCENTURE)
- GESTION DES OBSOLESCENCES / CARVE-IN CARVE-OUT (NATEXIS BLEICHROEDER)
- DÉPLOIEMENT SECURITE À INTERNATIONAL (BOUYGUES CONSTRUCTION)
- REFONTE LAN/WAN ET DÉPLOIEMENT SECURITE À L'INTERNATIONAL (COFACE)
- REFONTE LAN/MAN CARVE-IN ET MCO RESEAU SALLE DES MARCHES (BANQUE ING FERRI BBL)
- INDUSTRIALISATION/DURCISSEMENT POSTE DE TRAVAIL ET SERVEURS (KODAK PATHE)
- INGÉNIERIE RESEAU LAN/WAN (INDOSUEZ CARR FUTURES)
- AUDIT RESEAU ET FORMATION (FONDS DE DÉVELOPPEMENT SOCIAL DU CONSEIL DE L'EUROPE)
- INGÉNIERIE RESEAU LAN/MAN (BOURSE DE PARIS)
- INGÉNIERIE RESEAU (TDT FRANCOM)

- Dirige et gère des projets de cybersécurité en mettant en œuvre des Framework de sécurité robustes, en gérant les risques et en garantissant la conformité aux standards de sécurité. Supervise l'infrastructure de sécurité, la sécurité du cloud et la sécurité des applications tout en garantissant l'alignement avec les objectifs informatiques de l'organisation et les exigences réglementaires (PCI DSS, LPM, DORA, NIS2). Capacité et compétences en tant que gestionnaire de projet avec de grandes compétences techniques pour diriger la cybersécurité des applications et infrastructure informatique. Outils de gestion de projet (service now, jira, confluence, msproject, fichier excel)
- **Stratégie et gouvernance de la cybersécurité** :Élabore et met en œuvre des politiques de cybersécurité, des cadres de gouvernance et des stratégies de gestion des risques de sécurité. Assure le respect des normes de conformité telles que ISO 27001, NIST, GDPR, SOC 2. Organise des audits de sécurité (EBIOS RM), des tests de pénétration (Nessus, Nmap, Burp, ...) et des évaluations de vulnérabilité pour identifier et atténuer les risques (Qualys). Supervision de la mise en œuvre de l'architecture Zero Trust (ZTA) (Zscaler/Cloudflare) et des contrôles d'accès basés sur les rôles (RBAC) pour améliorer la sécurité.
- **Infrastructure de sécurité et sécurité du cloud** : supervise la conception, la mise en œuvre et la maintenance des solutions de sécurité pour les environnements LAN, WAN, VPN, pare-feu et cloud (AWS, Azure, GCP). Mise en œuvre SIEM (Splunk, IBM QRadar, Microsoft Sentinel) pour la surveillance de la sécurité en temps réel et la détection des menaces. Gestion des systèmes de détection/prévention des intrusions (IDS/IPS), des pare-feu (Palo Alto, Cisco ASA, Fortinet, Checkpoint) et des solutions de sécurité des terminaux (CrowdStrike, Symantec, McAfee). Mise en œuvre des stratégies de segmentation du réseau, de micro segmentation et d'atténuation des attaques DDoS. Sécurisation des charges de travail cloud, des conteneurs Kubernetes et des fonctions sans serveur (serverless).
- **Sécurité des applications et protection des données** : Travaille en étroite collaboration avec les développeurs pour mettre en œuvre le DevSecOps, des pratiques de codage sécurisées et la sécurité des API (OWASP Top 10, SAST, DAST). Gère les projets de gestion des identités et des accès (IAM Forgerock / Okta), notamment MFA (RSA / Yubikey), SSO (Okta SSO) et la gestion des accès privilégiés (PAM). Déploiement de solution Data Loss Prevention, (symantec, forcepoint, Mcafee), le chiffrement des bases de données (TDE, AES-256) et des solutions de sauvegarde sécurisées pour protéger les informations sensibles. Mise en place d'un plan de réponse aux incidents (IRP) et des procédures d'analyse pour gérer efficacement les cybermenaces.
- **Gestion de projet et coordination des fournisseurs** : Supervision des projets liés à la sécurité dans les systèmes ERP (SAP, Oracle), des portails Web, des applications mobiles et d'infrastructure informatique. Collaboration avec les équipes fonctionnelles, DevOps, opérationnelles, conformité et prestataires, pour intégrer la sécurité à tous les niveaux. Évaluation et acquisition de solution de sécurité, des outils et des services de sécurité auprès des fournisseurs tiers. Gestion des échéanciers, des budgets et des évaluations des risques projets pour garantir une livraison dans les délais et à moindre coût.
- Cybersécurité IT et OT, risques et conformité (PCI DSS, RGPD, DORA TPRM, LPM OIV/OSE). Comitologie (CoPil, CoProj, CoSuivi, MoM). Solutions de Sécurité utilisées: IDS/IPS, SIEM (Splunk/QRadar), EDR (SentinelOne, Symantec Endpoint Protection, Carbon Black), IAM (Ping Identity, Okta) ; PAM (Cyberark, Symantec), MFA. Audit & Compliance : Mise en œuvre des normes ISO27001, Analyse 27005 , NIS2, PCI DSS. GRC : Mise en place et suivi des réalisations (livrables). Management d'Équipes : Leadership d'équipes locales et internationales (5 à 60 personnes). Communication : Reporting stratégique et rédaction de RFP/RFQ. Budget : construction et maintien / Négociation (2 à 30 M€)

LANGUE

-  Anglais : (Courant) ;  Japonais (Notions) ;  Français (Langue maternelle)

CERTIFICATIONS ET DIPLÔMES



- Maîtrise - EPITA (1987) CCNA/CCNP/CEH v7 (2012 – 2013) ITIL/PRINCE2/CISSP (2014 – 2015)

CONTEXTE : MISE EN PLACE D'UN SOC EUROPÉEN

Gestion d'un projet de SOC IT Européen entre plusieurs banques centrales. Compliance BCE & ACPR

RÉALISATIONS :

- Mise en œuvre des process commun pour SOC Tier1, Tier2, DFIR, CTI
- Mise en exécution du framework (MITRE ATT&CK / TTP, TIBER EU, NIST)
- Recrutement des analystes (Blue Team / Red Team) au niveau européen
- Suivi des exigences de la Banque Centrale Européenne
- Mise en place de scenario de cybercrise (matrice raci, process/procédure)
- Campagne de pentesting, phishing, hacking, etc...
- Mise en place de la conformité DORA 5 piliers (ACPR) et gouvernementale
- Gestion de projet (comitologie, reporting, suivi, ateliers, etc...

CONTEXTE : MISE EN PLACE D'UN SOC OT EN ENVIRONNEMENT INDUSTRIELLE

Gestion d'un projet de SOC OT

RÉALISATIONS :

- Gestion d'un projet de mise en place d'un SOC en environnement OT pour l'ensemble du parc de transports et consolidation de la sécurité
- Définition du scoping et inventaire de l'environnement OT, gestion de l'obsolescence, contacts avec les différents fabricant pour les solutions de remédiation
- Gestion du patching et mise à niveau le cas échéant (hardening & segmentation, PCM, ECM, ECU, TCM)
- Planning de déploiement et gestion des changements/rollback
- Rédaction de rfp en anglais (environnement international)
- Mise en place de la conformité gouvernementale.
- Négociation avec les métiers pour les différents planning de déploiement sur chacun des pays.

CONTEXTE : DÉPLOIEMENT SECURITE

Gestion de projet sécurité pour la mise en conformité des activités de WorldLine/Ingenico

RÉALISATIONS :

- Gestion de projet mondial sécurité.
- Déploiement de solution sécurité (chiffrement, authentification forte, durcissement).
- Reporting par zoning géographique.
- Revue de la conformité gouvernementale.

CONTEXTE : MISE EN PLACE D'UN SOC IT/OT

Gestion de projet sécurité pour l'ensemble du groupe Manutan (environnement internationale)

RÉALISATIONS :

- Mise en place d'un SOC global centralisé.
- RFP/RFQ, recrutement d'experts interne/externe et sélection d'intégrateurs.
- Négociation des contrats et gestion des budgets
- Mise en place de la conformité gouvernementale.

CONTEXTE : TRANSFORMATION RÉSEAU ET SECURITE

Gestion de projet réseau LAN/WAN et sécurité pour l'ensemble du groupe hospitalier APHP

RÉALISATIONS :

- Gestion de projet autour de la solution IPAM, Firewall Checkpoint et Cisco.
- Mise en place de solution de protection contre la fuite des données (DLP) et EDR.
- Mise en place de la conformité gouvernementale.
- Support et maintien en condition opérationnelle sur l'ensemble de l'infrastructure réseau et sécurité.

CONTEXTE : GOUVERNANCE SECURITE

Amélioration des process sécurité pour l'ensemble du groupe Stime / Intermarché

RÉALISATIONS :

- Audit sécurité pour l'ensemble du groupe.
- Remédiation suite à l'audit avec toutes les parties prenantes.
- Mise en place des process de gouvernance et comitologie.

CONTEXTE : TRANSFORMATION RÉSEAU

Déploiement de solution proxy cloud au niveau mondiale

RÉALISATIONS :

- Définition du scope et planning mondiale.
- Définition d'un POC document d'architecture, procédure de déploiement et retour d'expérience
- Déploiement de la solution proxy Zscaler par continent

CONTEXTE : DÉMÉNAGEMENT DATACENTER

Gestion de la sécurité au siège ainsi que toutes les filiales et sociétés partenaires ainsi que la gestion de plusieurs déménagement de datacenters à l'étranger

RÉALISATIONS :

- Installation/Configuration/troubleshooting/Optimisation des règles de sécurité du Cluster de Firewall
- Gestion des Proxy (ISA, Squid, Optenet)
- Déménagement de Datacenters de France vers UK ensuite de UK vers l'Inde
- Support niveau 3, process ITIL

CONTEXTE : CERTIFICATION PCI DSS

Gestion d'un projet de certification PCI DSS (primordiale pour l'activité métiers)

RÉALISATIONS :

- Gestion des équipes réseau et sécurité sur différents projets
- Rédaction des documents d'architecture des flux
- Optimisation des datacenters pour une complète redondance

CONTEXTE : CERTIFICATION PCI DSS

Gestion d'un projet de certification PCI DSS

RÉALISATIONS :

- Mise en œuvre des exigences pour la certification PCI DSS
- Déploiement EDR, MFA, IAM/PAM,
- Durcissement de l'infrastructure

CONTEXTE : LUTTE ANTI TERRORISME DÉPLOIEMENT CCTV

Conseil technique sur les aspects sécurités des liaisons.

RÉALISATIONS :

- Étude des différentes solutions de sécurités proposées par les fournisseurs
- Gestion des appels d'offres
- Déploiement CCTV au niveau nationale (projet lutte anti terroriste)

CONTEXTE : DÉPLOIEMENT RÉSEAU ET SECURITE AU NIVEAU NATIONAL

Gestion de projet LAN WAN pour les clients d'Accenture.

RÉALISATIONS :

- Gestion d'un projet de déploiement VPN à l'international
- Gestion de Projet pour le déploiement du wifi sur différents bureaux

CONTEXTE : GESTION DES OBSOLESCENCES / CARVE-IN CARVE-OUT

Gestion de la sécurité au siège ainsi que toutes les filiales et sociétés partenaires.

RÉALISATIONS :

- Installation/Configuration/troubleshooting/Optimisation des règles de sécurité du Cluster de Firewall
- Mise en place d'architecture haute dispo pour des flux financiers
- Préparation/inventaire de l'infrastructure en vue de la fusion (Natexis + Ixis CIB)

CONTEXTE : DÉPLOIEMENT SECURITE À INTERNATIONAL

Consultation en sécurité pour divers projets.

RÉALISATIONS :

- Analyse/Audit des flux et optimisation des règles de sécurité sur cluster
- Cleansing de firewall (passage de 5000 règles à 3000)
- Déploiement de firewall à travers le monde (75 pays)
- Mise en place de VPN site à site

CONTEXTE : REFONTE LAN/WAN ET DÉPLOIEMENT SECURITE À L'INTERNATIONAL

Gestion de la sécurité au siège ainsi que toutes les filiales et sociétés partenaires.

RÉALISATIONS :

- Gestion de plusieurs projets de déménagements de filiales
- Rédaction de RFP et RFQ
- Refonte du LAN (ATM/FDDI vers GigabitEthernet)
- Migration de liaison Spécialisé vers VPN site à site (64 pays)

CONTEXTE : REFONTE LAN/MAN CARVE-IN ET MCO SALLE DES MARCHES

Gestion d'un réseau bancaire et salle des marchés.

RÉALISATIONS :

- Gestion des interconnexions MAN & WAN entre plusieurs villes de France et interconnexion avec les bureaux de l'étranger
- Préparation pour les différentes fusion/acquisitions de nouveaux bureaux

CONTEXTE : INDUSTRIALISATION/DURCISSEMENT POSTE DE TRAVAIL ET SERVEURS

Ingénierie système et réseau pour Kodak Pathe.

RÉALISATIONS :

- Support niveau 3 (industrialisation des postes de travail)

CONTEXTE : INGÉNIERIE RESEAU LAN/WAN

Ingénierie réseau pour la Banque Indosuez et salle des marchés Carr Futures

RÉALISATIONS :

- Gestion du réseau LAN & WAN et flux financiers

CONTEXTE : AUDIT RÉSEAU ET FORMATION

Ingénierie réseau pour le Conseil de l'Europe.

RÉALISATIONS :

- Consultant expert sur réseau Novell Netware, audit & formation des admins sur les serveurs novell
- Création de poste de travail bureautique remastérisé, industrialisation des installations des nouveaux postes de travail

CONTEXTE : INGÉNIERIE RESEAU LAN/MAN

Gestion du réseau de la bourse MONEP en temps réel et astreinte 24/7

RÉALISATIONS :

- Maintien en condition opérationnel des liaisons spécialisées vers toutes les banques et société de bourse travaillant sur le marché des options négociables.
- Chef de projet pour le lancement du projet EPFS (European Price Feeds Service) serveur mettant à disposition tous les cours de bourse européen (MONEP, MATIF, DTB, LIFFE, MEFF) récupéré préalablement par plusieurs passerelles multi protocole programmé automatiquement par CFT.
- Expert sur CFT, transaction boursière (swift, etebac)

CONTEXTE : INGÉNIERIE RÉSEAU

Constructeur de carte de communication pour émulation de terminaux Bull et IBM sur PC.

RÉALISATIONS :

- Installation d'équipements réseaux d'interconnexion sur BULL et IBM. Laboratoire de test & POC à Miami. Support technique après-vente. Réponse à RFP et RFQ.

REFERENCES

<https://www.linkedin.com/in/cyberfreelance>

