Ingénieur Cybersécurité

75013 Paris · 0 à 1 an d'expérience · Réf. 2610281658

Ma recherche

Contrat recherché : Tout contrat
Zone : Toute la France
Mobilité : sur toute la france
Rémunération : A étudier
Secteur : Bâtiment

Formations

2023-12-31 — Bac +5 — INSA / UPHF, Valenciennes
Master Cyberdéfense et Sécurité de l'Information

Expériences professionnelles

2026-05-01 - 2026-12-31 — Consultant Cybersécurité & Support IT — Indépendant (Freelance)

Accompagnement indépendant d'un établissement de restauration dans la sécurisation de son système d'information, le support informatique quotidien et la continuité d'activité. • Cybersécurité : évaluation des vulnérabilités et sécurisation des accès ; gestion des sauvegardes et des mots de passe ; sensibilisation du personnel à la prévention phishing / malwares et assistance en cas d'incident. • Support informatique : assistance et diagnostic en cas d'incident ; accompagnement lors du déploiement de nouveaux équipements. • Réseau : résolution des problèmes de connexion et recommandations d'optimisation des performances réseau. • Conseil : accompagnement sur le renouvellement de matériel, le choix de logiciels, la protection des données et la continuité d'activité.

2026-02-01 - 2026-05-31 — Consultant Cybersécurité — GRC, Formation & Sensibilisation (Freelance)

Accompagnement d'une petite entreprise sur la structuration de sa démarche cybersécurité, avec un focus sur la gouvernance, la formation et la sensibilisation. • Mise en place d'une politique de sensibilisation à la cybersécurité adaptée aux équipes de l'entreprise. • Animation de sessions de formation cybersécurité (bonnes pratiques, phishing, gestion des mots de passe) auprès du personnel. • Accompagnement dans le choix des prestataires informatiques et de sécurité : définition des critères, mise en concurrence, suivi. • Conseil sur la structuration d'une démarche de sécurité adaptée à une petite structure.

2024-03-01 - 2025-12-31 — Ingénieur Cybersécurité — Gouvernance SSI & Sécurité Opérationnelle (CDD)

Mise en place d'une gouvernance SSI complète et gestion opérationnelle de la sécurité du SI d'une collectivité territoriale (~500 agents, organisme public). • Pilotage du SMSI ISO 27001 : élaboration et maintien de la PSSI, PCA, PRA ; suivi du plan de conformité et des actions d'amélioration continue. • Analyse des risques (EBIOS RM) : identification des scénarios de menace, évaluation, définition et suivi des mesures de traitement ; tenue du Risk Register. • Conduite des audits de sécurité et pilotage des plans d'action correctifs ; intégration des exigences NIS2 et RGPD dans les politiques internes. • Animation de campagnes de sensibilisation et formations cybersécurité auprès des agents ; communication sur les cybermenaces. • Surveillance et analyse des alertes de sécurité (DLP, phishing, EDR, SIEM, IDS/IPS) ; traitement et reporting des incidents. • Administration et MCO des solutions de sécurité ; gestion des correctifs, des vulnérabilités et des plans de remédiation. • Gestion des environnements Microsoft : Active Directory, Azure, Office 365 ; administration des droits d'accès et des configurations de sécurité. • Intégration des exigences SSI dans les projets SI ; coordination des prestataires techniques et contrôle de leur mise en œuvre.

2021-10-01 - 2023-12-31 — Ingénieur Cybersécurité — AMOA Sécurité & Conformité (Alternance)

Accompagnement de clients multisectoriels (finance, santé, services) dans la sécurisation de leurs SI, la conformité réglementaire et la structuration de leur gouvernance SSI. • Participation au maintien et à l'évolution du SMSI clients (ISO 27001) : PSSI, procédures, politiques de sécurité et suivi des plans d'amélioration continue. • Animation d'ateliers de sensibilisation pour des interlocuteurs variés (technique, métier, direction) ; vérification des exigences sécurité dans les projets SI. • Conduite d'analyses des risques (EBIOS RM) ; coordination des audits techniques et élaboration des plans d'action associés. • Mise en œuvre des référentiels NIS2, DORA et RGPD au sein des politiques de sécurité ; rédaction de livrables à destination des RSSI et directions. • Surveillance de la sécurité des points de terminaison et analyse des alertes ; participation aux instances sécurité opérationnelles. • Conseil et accompagnement des équipes

R&D et infrastructure sur la sécurité applicative (OWASP Top 10) et les bonnes pratiques SSI.

2019-10-01 - 2021-04-30 — Analyste en Sécurité Informatique (Alternance)

Gestion de la sécurité opérationnelle des systèmes et réseaux ; amélioration du traitement des vulnérabilités. • Surveillance des systèmes et réseaux : pare-feu, EDR, SIEM, IDS/IPS ; analyse, priorisation et traitement des alertes de sécurité. • Participation à la gestion des incidents de sécurité et intervention sur les vulnérabilités critiques ; remédiation et suivi des correctifs applicatifs et systèmes. • Mise à jour de la cartographie des risques techniques ; contribution aux rapports de surveillance cybersécurité et veille sur les nouvelles failles.

Langues

Français (Langue maternelle), Anglais (Bilingue)

Atouts

Governance, ISO 27001, Norme ISO 27002, Directive NIS, DORA, RGPD, EBIOS Risk Manager, Gestion des risques, Auditing, Policy Development, Intervention en cas d'incident, SOC (Security Operations Center), EDR (Endpoint Detection and Response), SIEM, IDS/IPS, Pare-feu (Firewall), DLP, Phishing Awareness, Training & Awareness, Windows Server, Linux, Active Directory, Microsoft 365, Microsoft Azure, AWS, PowerShell, OWASP, Gestion de projet, Communication, Pédagogie, Gestion des vulnérabilités, Plan de continuité d'activité (PCA), Disaster Recovery Planning, Conformité réglementaire, Protection des données personnelles, Optimisation de réseaux, Support technique

Fiche anonyme — l'identité et les coordonnées du candidat sont communiquées aux recruteurs qui en font la demande sur pmebtp.com.