Expertise Réseaux, Métrologie et Sécurité

Ingénieur Sécurité - SOC avec une expérience de SIEM

Lugos, société d'expertise en Réseaux, Métrologie et Sécurité accompagne les entreprises dans leurs projets d'évolution de leurs infrastructures IT : réseaux, télécommunications, solutions de sécurité, systèmes d'informations, … Nous réalisons des prestations d'audit, de conseil, d'architecture, d'ingénierie détaillée, d'accompagnement à la mise en œuvre, d'exploitation et de support Niveau 2 et 3 pour nos clients grands comptes et opérateurs.

Notre expertise est aujourd'hui reconnue sur les projets d'optimisation de la visibilité, de la performance et de la sécurité des infrastructures et applications ; Compétences primordiales lors de la mise en place de nouvelles applications, de solutions Cloud / SaaS, voix sur IP, visioconférence, sécurité, ...

Nous avons conclu plusieurs partenariats stratégiques assurant à Lugos un développement rapide et recrutons plusieurs ingénieurs expérimentés pour nous accompagner dans la réalisation de nos projets sur 2017. Présent à Paris et Nantes, nous recherchons aujourd'hui un(e) Ingénieur Sécurité (H/F) pour renforcer l'équipe de notre Security Operating Center (SOC) à Paris ou à Nantes.

Profil recherché

Idéalement issu(e) d'une formation d'Ingénieur ou équivalent (bac +4/5), vous disposez de 3 à 5 ans d'expérience dans des équipes de design, de déploiement, d'intégration ou de support en sécurité Réseaux chez des clients grands comptes, intégrateurs, opérateurs ou constructeurs. Vous avez une bonne maîtrise des solutions technologiques du marché (réseaux et sécurité) et en particulier des solutions de corrélation de log, Security information and event management (SIEM).

Vous êtes passionné(e) par la technique et l'expertise d'une manière générale. Vous souhaitez développer rapidement vos compétences en travaillant dans un environnement multi-projet, multi-clients et en participant au développement de solutions innovantes au sein d'une équipe dynamique.

Vos qualités humaines indispensables :

- Très bon relationnel
- Bonne capacité à travailler en équipe
- Esprit d'analyse et de synthèse
- Rigueur, autonomie
- Force de proposition, proactivité
- Curiosité technologique
- Qualités rédactionnelles

L'ingénieur sécurité doit, en plus de solides compétences techniques, avoir de réelles qualités dans la conduite de projets.

Missions

Au sein de l'équipe de la direction technique de Lugos, vous intervenez chez nos clients et prenez en charge des projets innovants d'évolution des infrastructures réseaux et sécurité.

Vous êtes en charge des missions suivantes :

- Prise de connaissance de l'existant et des enjeux associés au projet,
- Analyse fine des besoins et des contraintes,
- Conception de l'architecture niveau 1, 2 & 3 permettant de répondre à l'ensemble des besoins fonctionnels, de garantir un haut niveau de résilience et la sécurité de l'information, tout en s'intégrant dans les infrastructures, méthodes, référentiels et process existants,
- Définition de l'ingénierie détaillée des infrastructures réseau et sécurité,
- Rédaction de la documentation : HLD, LLD, spécifications techniques, mode opératoires, documents d'exploitations, …
- Mise en place de maquettes, labs, pilotes et réalisation de tests,
- Déploiement, en mode projet, de plateformes de sécurité complexes. Configuration et intégration des équipements dans les outils de gestion clients,
- Transfert de compétences vers les équipes d'exploitation,
- Support technique de niveau 3 aux équipes d'exploitation et relations avec les constructeurs,
- Transfert de connaissances sur les principaux référentiels, les normes et les réglementations relatifs à la sécurité des systèmes d'information (ISO 2700x, LPM, …),
- Evaluation ou réalisation de dossier de sécurité (analyse de risques, PSSI, procédures) afin de déterminer les manques et faiblesses,
- Comprendre les enjeux de la gouvernance SSI, la gestion des incidents, la continuité et la reprise des activités ainsi que l'organisation et les fonctions liées à la SSI,
- Avoir des connaissances techniques (sécurisation des systèmes d'exploitation, mécanismes de contrôle d'accès, architecture réseau, etc.), afin d'appréhender les vulnérabilités techniques pour en déterminer les causes organisationnelles,
- Veille technologique sur son domaine d'expertise.

Vous pouvez également être amené(e) à réaliser des études technologiques : analyse d'opportunité, cahier des charges, tests techniques, documentation et présentation des résultats.

Compétences requises

Maîtrise (design et implémentation) des technologies suivantes :

- Utilisation d'outils associés à des prestations de détection d'anomalies dans un environnement de Sécurity Operation Center de type SIEM, Anti DDoS, IPS, IDS.
- **Corrélation de log (SIEM) : Arcsight, QRadar, Splunk, LogRythm, …**
- Réalisation d'audits (architecture, configuration), tests d'intrusion, analyse de documents et de procédures, entretiens.
- Rédaction de rapports incorporant une analyse des vulnérabilités rencontrées et des préconisations techniques et organisationnelles.
- Formalisation et standardisation des procédures d'audits.
- Rédaction de fiches techniques sur des domaines SSI techniques ou plus généraux.
- Rédaction de recommandations génériques, destinées aux rapports d'audit, dans les domaines organisationnels (réglementation, gouvernance, intégration de la sécurité dans les projets, homologation, continuité des activités, etc.).
- Veille technologique active et ciblée dans ces domaines.
- Réalisation de support de cours ou de sensibilisation au profit du centre de formation ou des entités inspectées.
- Elaboration des outils utilisés pour les audits.
- Assistance à la reprise de contrôle d'un système d'information suite à un incident de grande envergure (présentations et soutien sur les démarches métier, participation à l'élaboration et au suivi des plans de durcissement et de reconstruction, etc.).

Bonne connaissance des environnements suivants :

- Firewalls et répartiteurs de charge : Checkpoint, Fortinet, Palo Alto, Web Gateway, F5, Stonesoft, …
- Composants techniques de sécurité : Proxy, PKI, Antivirus, Firewalls, IDS / IPS, DDOS, DLP, NAC,
- Authentifications : NTLM, SAMLv2, OTP, PKI, EAP, Radius, …
- Fondamentaux : modèle OSI, TCP/IP, IPv4 / IPv6, Firewall, Pen Test, VPN, PKI, IPSEC/SSL, Proxy, Web Application Firewall, Anti-Virus, Anti-Spam
- Technologies réseaux Niv2/3 : Cisco, Alcatel-Lucent, …
- Commutation, routage (BGP), …
- Solutions de supervision et de métrologie
- Architectures Datacenter : virtualisation, redondance de sites (PRA/PCA), …
- Architectures applicatives multi-tiers de type web, annuaires, …

Les compétences système Unix, scripting, développement web, sont un plus.

Maîtrise de l'anglais obligatoire.

Expertise Réseaux, Métrologie et Sécurité

Informations complémentaires

Début souhaité :	Immédiat
Type de contrat :	CDI
Statut :	Cadre
Horaires :	Temps plein
	Réalisation occasionnelle d'opérations en HNO
Rémunération :	40/55 K€ (selon expérience et localisation)
Lieu :	Paris et région Parisienne.
	Ou Nantes et région Nantaise.
	Déplacements en France Métropolitaine à prévoir (1 à 2 / mois)

Vous êtes titulaire du permis B