Expertise Réseaux, Sécurité et Cloud

Ingénieur Sécurité – Pen Testing

Lugos, société d'expertise en Réseaux, Sécurité et Cloud Computing, 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 et à l'exploitation pour nos clients grands comptes et opérateurs.

Notre expertise est aujourd'hui reconnue sur les projets d'amélioration 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 3 ingénieurs expérimentés pour nous accompagner dans la réalisation de nos projets sur 2015. Présent à Paris et Nantes, nous recherchons aujourd'hui un(e) Ingénieur Sécurité (H/F) pour renforcer notre équipe Parisienne et à court terme notre équipe Nantaise.

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 SOC (Security Operating Center), de Pen Pesting, de déploiement / intégration sécurité, ou de support avancé en sécurité. Vous avez une bonne maîtrise des solutions technologiques du marché (réseaux et sécurité).

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.

Expertise Réseaux, Sécurité et Cloud

Missions

Au sein de l'équipe de la direction technique de Lugos, vous intervenez chez nos clients et prenez en charge les missions suivantes :

- Vous intervenez sur les infrastructures réseau et/ou sécurité de nos clients dans le cadre d'un projet d'évolution ou de déploiement d'infrastructures de sécurité. Votre champ d'action couvre les outils de Pen Testing et les scanners de vulnérabilités. Vous pouvez intervenir dans le cadre d'un Security Operating Center pour la recherche d'intrusion à froid ou la remédiation (incident response) en cas de détection d'intrusion avérée,
- Prise de connaissance de l'existant et des enjeux associés au projet,
- Analyse fine des besoins et des contraintes,
- Conception de l'architecture permettant de répondre à l'ensemble des besoins fonctionnels,
- Définition de l'ingénierie et des modes opératoires des tests,
- Rédaction de la documentation : spécifications techniques, modes opératoires, documents d'exploitations,…
- Mise en place de maquettes, labs, pilotes,
- Réalisation de tests d'intrusions avec ou sans connaissance de l'environnement cible (tests et préconisations associées)
- Déploiement de solutions de scanner de vulnérabilités (réalisation des actions, paramétrage des rapports, préconisation d'actions, suivi des actions correctives)
- Suivi des vulnérabilités (Patch management)
- Prise en charge d'incidents de sécurité (analyse, traitement / coordination, investigations numériques, suivi)
- Préconisations de changements de sécurité (ajout de règles, analyse de matrice existante,…)
- Analyse des logs des firewalls, des fichiers d'audit Firewall (rapport Tufin, Algosec, Playflows,…)
- Transfert de compétences vers les équipes d'exploitation,
- Support technique de niveau 3 aux équipes d'exploitation et relations avec les constructeurs,
- 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 :

- Tests d'intrusion : Nessus Vulnerability scanner, Qualys, Metasploit, OpenVAS
- Firewalls et répartiteurs de charge : Checkpoint, Fortinet, Palo Alto, Web Gateway, F5, Stonesoft,…
- Connaissances des sujets d'Authentification AD, LDAP, Radius, PKI, Accès distants (Citrix, Direct Access, VPN,…)

- Composants techniques de sécurité : Proxy, Antivirus, Firewalls, IDS / IPS, DDOS, DLP, NAC, SIEM,…

Vous avez éventuellement une certification sur le sujet PEN Testing (GIAC Penetration Tester (GPEN) ou Offensive Security Certified Professional (OSCP)) ou en sécurité globale (CISSP).

Bonne connaissance des environnements suivants :

- 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.

Informations complémentaires

Début souhaité :	Immédiat
Type de contrat :	CDI
Statut :	Cadre
Horaires :	Temps plein
	Réalisation occasionnelle d'opérations en HNO
Rémunération :	35/55 K€ (selon expérience)
Lieu :	Paris et région Parisienne.
	Ou Nantes et région Nantaise après une période de 12 mois sur Paris.
	Déplacements en France Métropolitaine à prévoir (1 à 2 / mois)

Vous êtes titulaire du permis B