Fonction
PENTESTEUR IV.A (H/F)

Évolutions possibles

Au sein du métier

- RSSI IV.A (H/F)
- RSSI IV.B (H/F)
- ADMINISTRATEUR SOLUTIONS DE SECURITE III.3 (H/F)
- ADMINISTRATEUR SOLUTIONS DE SECURITE IV.A (H/F)
- ANALYSTE DE LA MENACE III.3 (H/F)
- ANALYSTE DE LA MENACE IV.A (H/F)
- ANALYSTE REPONSE INCIDENT III.3 (H/F)
- ANALYSTE REPONSE INCIDENT IV.A (H/F)
- ANALYSTE SOC III.2 (H/F)
- ANALYSTE SOC III.3 (H/F)
- ANALYSTE SOC IV.A (H/F)
- CORRESPONDANT SECURITE III.2 (H/F)
- CORRESPONDANT SECURITE III.3 (H/F)
- CORRESPONDANT SECURITE IV.A (H/F)
- EXPERT CYBER IV.B (H/F)
- PENTESTEUR III.3 (H/F)
- PENTESTEUR IV.A (H/F)
- RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.A (H/F)
- RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.B (H/F)
- RESPONSABLE PROJET DE SECURITE III.3 (H/F)
- RESPONSABLE PROJET DE SECURITE IV.A (H/F)
- EXPERT CYBER IV.A (H/F)

Raisons d'être

Le Pentesteur réalise des évaluations techniques de la sécurité d’environnements informatiques.

Il identifie les vulnérabilités et propose des actions de remédiation.

Il peut réaliser différents types d’audits en fonction de son périmètre d’activité (tests d’intrusion, revue de code, revue de configuration, etc.).

Le Pentesteur peut être amené à réaliser des tests de type "**red team"** qui visent à simuler des attaques en grandeur réelle dans le but de tester les défenses de l’organisation.

Il peut également être amené à réaliser des tests dans une approche "**purple team"** afin d’entrainer les équipes de détection des incidents de cybersécurité.

Une évolution professionnelle est possible vers les fonctions de RSSI – Expert Cyber – Responsable détection et réponse – Analyste SOC – Analyste réponse à incident – Administrateur solution sécurité – responsable projet de sécurité – Correspondant sécurité de projet

Missions

Réalisation des audits

- Adopter une vision globale du système d’information à évaluer
- Définir les plans de tests au sein du SI de l’organisation
- Exécuter et documenter des tests de sécurité sur différents environnements informatiques, en s’assurant du respect du cadre réglementaire encadrant ces pratiques

- Collecter les éléments de configuration des équipements à tester et réaliser une revue des configurations
- Collecter les éléments d’architecture des systèmes à auditer et réaliser une revue de l’architecture
- Réaliser une revue du code source des composants de l’environnement
- Définir les scénarios d’attaques et réaliser des attaques sur l’environnement cible (tests d’intrusion)

Réaliser ou piloter la mise en œuvre de des scans de vulnérabilités et de contrôles techniques en continu et automatisés

- Procéder à des interviews des équipes pour évaluer les impacts des vulnérabilités détectées pour l'organisation
- Rédiger des rapports incorporant une analyse des vulnérabilités rencontrées et une identification des causes et mettre en évidence et évaluer les risques de sécurité et les impacts pour les métiers
- Définir les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes
- Collaborer avec les équipes informatiques pour mettre en œuvre les recommandations techniques
- Produire des tableaux de bord du niveau de sécurité et de conformité

Veille technique et conception d'outils d'audit

- Assurer une veille permanente vis-à-vis des scénarios d'attaques, des nouvelles menaces et des vulnérabilités associées et vis-à-vis du développement de nouveaux contextes de tests
- Élaborer des outils utilisés pour les audits
- Identifier de nouveaux moyens pour détecter des failles qui peuvent toucher un système

Compétences

Comportementales Socles

Orientation client
: Enrichir l'expérience client en adoptant une posture de service et de conseil et développer une relation de confiance durable. Anticiper, analyser, comprendre les besoins et attentes de ses clients pour apporter des réponses personnalisées. S'appliquer à améliorer la satisfaction client et mesurer son niveau de satisfaction.

Culture du changement et de l'innovation
: Encourager et accompagner le changement et les initiatives d'amélioration dans un environnement complexe et incertain. Expérimenter, tester, évaluer en s'appuyant sur de nouvelles méthodes, y compris numériques. Comprendre et susciter l'innovation en remettant en question les usages et en osant être pionnier. Etre dans une dynamique d'identification et d'apport de nouveautés dans son activité en osant sortir du cadre pour penser le problème en dehors de ses limites et de ses moyens lorsque la situation le demande.

Coopération et ouverture
: Construire et faire vivre des réseaux informels ou structurés d'individus ou de groupes en s'appuyant sur les outils collaboratifs comme les réseaux sociaux internes. Participer individuellement à l'atteinte d'un résultat collectif en favorisant l'entraide et le partage de connaissances. Savoir fédérer les parties prenantes d'un projet autour d'un objectif commun et établir des partenariats. Faire preuve d'écoute active vis-à-vis de ses interlocuteurs et prendre en compte leurs problématiques et les objections émises dans ses actions et prises de décision. Etre ouvert(e) d'esprit et curieux(se) au sein de son environnement.

Orientation résultats
: Engager des actions et mobiliser en toute autonomie des ressources (financières, matérielles, techniques, numériques et humaines) pour atteindre des performances durables dans le respect des principes éthiques, de qualité de vie et de RSE. Savoir être proactif et fixer, pour soi et/ou pour d'autres, des objectifs ambitieux et exploiter des opportunités pour aller au-delà des attendus.

Cyber Sécurité

Vulnérabilités des environnements
: Maitriser les principes, méthodes et outils d'évaluation des vulnérabilités et identifier les contre-mesures appropriées

Techniques d'attaque et d'intrusion
: Maitriser les techniques employées par les attaquants pour compromettre un Système d'Information (ex : phishing via les réseaux sociaux, exploitation d'une vulnérabilité de l'OWASP), à toutes les étapes de la kill chain (reconnaissance, intrusion, exploitation, augmentation de privilèges, mouvement latéral, persistance, exfiltration, etc.)

Sécurité des systèmes d'exploitation
: Maitriser la sécurité des systèmes d'exploitation (poste de travail, serveur, mobile) connus sur le marché (Windows, Linux, iOS, Android, etc.) : méthodes de durcissement, connaissance des outils de sécurité natifs, connaissance des principales attaques.

Sécurité des réseaux et protocoles
: Mettre en place, maintenir et améliorer les pratiques établies en matière de sécurité des réseaux (ex : NIPS, anti-malware, restriction/empêchement dispositifs externes, filtres anti-spam) et des protocoles. Maitriser des outils d'analyse de réseau pour identifier les vulnérabilités (ex : fuzzing, nmap, etc.). Reconnaitre et interpréter une activité réseau malveillante dans le trafic. Maitriser l'utilisation

d'analyseurs de protocoles. Maitriser la configuration et l'utilisation des composants de protection des réseaux (par exemple, pare-feu, VPN, systèmes de détection des intrusions dans les réseaux)

Techniques de tests d'intrusion

Connaitre et mettre en application les techniques de tests d'intrusion (ex : scan de ports, injection SQL, etc.) sur différents types de systèmes (application web, client lourd, Active Directory, etc.) en conditions variées (boite blanche, boite grise, boite noire). Savoir utiliser les outils permettant de faciliter l'exécution de tests d'intrusion (ex : machine Kali Linux). Savoir restituer les résultats dans un rapport contenant une approche par les risques et des mesures de remédiation pour les couvrir.

Rétro-ingénierie de malwares

Maitriser les différentes techniques de rétro-ingénierie sur les malwares pour comprendre leur fonctionnement et contribuer à la réponse à incidents : analyse statique de binaires (désassemblage, décompilation, etc.), analyse dynamique de binaires (ex : dump de processus, etc.)

Sécurité applicative

Maitriser les techniques de sécurisation des applications : gestion des identités et des habilitations, sécurité dans les développements, chiffrement des données pendant l'échange et au stockage, gestion des certificats

Efficacité professionnelle

Veille / innovation / tendances

Se tenir informé(e) des tendances, des évolutions technologiques et des innovations en vigueur dans son domaine d'intervention en lien avec les enjeux de l'entreprise et attentes des clients / partenaires et à les intégrer dans son activité.

Transfert de compétences

Maîtriser l'ensemble des techniques et outils et les leviers d'action permettant de faire preuve de pédagogie. Savoir transmettre des connaissances.

Techniques SI

Contraintes légales et aspects juridiques liés à la sécurité

Niveau de maitrise attendu : 3 Connaitre et appliquer la charte d'utilisation en matière de sécurité informatique, CNIL, archivage légal de documents, externalisation des données, respecter le RGPD, la réglementation autour des données...

Famille

Filière

Métier

Répartition des effectifs

-

  Groupe - siege

Effectif de la fonction

De 1 à 9