Missions

Dans le cadre de notre développement nous renforçant nos équipes sécurité. Nous vous proposons d'intégrer notre équipe de Consultant en Sécurité pour travailler sur projet devant répondre aux contraintes de sécurité du monde bancaire.

Activités principales

Vous serez amené à évoluer dans un environnement en perpétuel évolution (contrainte TTM) et dans un environnement fortement DevOps. Vos principales activités seront :

TTM:
Signigie Time to Market, c'est le temps que met une idée pour se transformer en fonctionnalité utilisée.

DevOps:
C'est une pratique technique visant à l'unification du développement logiciel et de l'administration des infrastructures informatiques . Les principes devops soutiennenet des cycles de développement plus courts, une augmentation de la fréquence des déploiements et des livraisons continues, pour une meilleure atteinte des objectifs économiques de l'entreprise.
Le développement, l'intégration, les tests, la livraison, le déploiement, l'exploitation et la maintenance des infrastructure.

- Etude et intégration de solutions de sécurité
  - Prendre en charge la partie technique des PoC (Proof of Concept) de solution de sécurité : gestion des secrets (hashicorp vault, bitwarden, passbolt, teampass, …), gestion d'identité (freeIAP, …), security compliance (OpenSCAP/Satellite), …
  - Réaliser l'intégration des solutions choisies ainsi que l'accompagenement à l'utilisation

Hashicorp Vault:
C'est un outil qui fournit plusieurs fonctionalités, telles que Gestion de secrets, Access basé sur l'identité, et encrypton des données application, pour réaliser des audits de secrets au niveau application, système et utilisateurs.

FreeIPA :
C'est un système de gestion d'identité FOSS. IPA signifie Identité, Politique et Audit. Elle comprend plusiers parties :

- **Fedora**
- **389 Directory Server**
- **MIT's Kerberos 5**
- **Appache HTTP Server**
- **Python**
- **Dogtag**

OpenSCAP :

C’est une implementation de SCAP qui signifie Security Content Automation Protocol, et qui comprend les vulnérabilités et les configurations liées à la sécurité. NVD (national vulnerability Database) est un repositoire des content national US.

- Vulnerability management / patch management
  - Détection des vulnérabilités par scan (NMAP, OSSIM, …) : réalisation des campagnes de détection de vulnérabilités des infrastructures et plateformes
  - Formalisation et suivi des plans d’actions associés, support à leur exécution
  - Reporting

OSSIM:
Signifie Open Source SIEM par AlienVault.

- Hardening des systèmes et des infrastructures
  - Audit technique des plateformes et infrastructures (CIS, NIST, …) : OS, middlewares, applicatifs et services des serveurs, équipements réseau et de sécurité
  - Formalisation et suivi des plans d’actions associés, support à leur exécution
  - Reporting

CIS:
Signifie Center for Internet Security, qui a développé des testes d’évaluation destinés à fournir des informations permettant aux organisations de prendre des décisions en matière de sécurité.

NIST:
Signifie Institut national des normes et de la technologie (National institute of Standards and Technology) est une agence appartenant au Département du Commerce des US.
Nist est aussi responsable de la création de guides de la sécurité pour la gouvernement fédéral des US.
Cette organisation conçoit un framework de cybersécurité (NIST CSF) qui se construit autour de 3 parties.

- Le Noyau, qui apporte une vision stratégique de la gestion du risque cyber au travers de 5 fonctions:identifier,protéger,détecter,répondre et récupérer.
- Les niveaux de mise en œuvre, qui permet d’identifier le niveau de maturité de l’entreprise en termes de cybersécurité. Et Nous pouvons qualifier et évaluer des mesures de cybersécurité à mettre en place.
- Le profil, qui précise la façon dont l’entreprise gère sa cybersécurité en fonctions de ses besoins et objectifs.

Compétences et qualités requises

- De formation Bac +5 (école d'ingénieurs ou équivalent universitaire), vous avez une expérience significative dans un poste similaire ou en administration système et réseau avec une forte volonté d’évoluer vers le domaine de la sécurité.

- Dans l’idéal vous avez une 1ère expérience sur les sujets suivants :
  - Virtualisation sous VMWare
  - Administration système (Linux) et sécurité (firewall, switch, routeur, …)

- Intégration, configuration et mise en œuvre d'applications/outils
- DevOps et son écosystème en sachant utiliser l'outillage associé : Git, automatisation via Ansible, chaine CI-CD, pipeline Jenkins, pilotage infra par le code/API …

Ansible:
C'est une plateforme logiciel libre pour la configuration et la gestion des ordinateurs. Elle combine le déploiement de logiciel multi-noeuds, l'exécution des taches ad-hoc, et la gestion de la configuration.

CI-CD :
Signifie Continuous integration et Continous delivery, pour le génie logiciel

Pipeline Jenkins:
C'est l'ensemble de plugins qui supporte Implementation et Integration pipeline vers Jenkins.

- L'environnement international, implique la parfaite maitrise du français, de l'anglais tant à l'écrit qu'à l'oral

  - Rigoureux, ayant l'esprit d'analyse et de synthèse, doté d'un excellent relationnel, vous êtes reconnu pour votre capacité d'écoute et votre orientation client
  - Pro actif et faisant preuve d'initiative, vous êtes apte à traiter des sujets transverses qui vont au-delà de vos compétences de base.

Le plus de l'offre

L'environnement international vous amènera à évoluer dans un contexte multi culturel avec une possibilité d'effectuer lors de votre parcours professionnel des missions à l'international.

Firewall:
Pare-feu est un logiciel ou matériel permettant de faire respecter la politique de sécurité du réseau. Il surveille et contrôle les applications et les flux de données.
On peut le classer en différentes catégories: Sans état et à états.

SSL:
Signifie Secure Sockets Layer, c'est un protocol de sécurisation des échanges sur Internet, devenue TSL en 2001.

TSL:
Signifie Transport Layer Security, c'est un protocol de sécurisation des échanges sur Internet. Il fonctionne un mode client-serveur. Il permet de satisfaire les objectifs de sécurité suivants:

- **l'authentification du serveur**
- **la confidentialité des données échangées**
- **l'intégrité des données échangées**

IDS:

Signifie Système de détection d'intrusion, c'est un mécanisme déstiné à repérer des activités anormales ou suspectes sur la cible analysée.

VLAN:

Signifie Réseau Local Virtuel, il présente les intérets suivants:

- **Améliorer la gestion du réseau**
- **Optimiser la bande passante**
- **Séparer les flux**
- **Segmentation: réduire la taille d'un domaine de broadcast**
- **Sécurité: permet de créer un ensemble logique isolé pour améliorer la sécurité.**

STP:

Signifie Spanning Tree Protocol, permet de déterminer une topologie réseau sans boucle.

SSH:

Signifie Secure Shell, c'est un protocol de communication sécurisée. Le protocol de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés.

Protocols de Routage:

Les protocols de routage externes (EGP), tels que BGP (Border Gateway Protocol), échangent des informations de routage entre AS systèmes autonomes.

Les protocols de routage interne (IGP) échangent des informations de routage à l'intérieur de AS, par les façons suivantes:

- **État de Lien, il transmettent la totalité des informations de routage à tous les routeurs participants et établissent des tables de voisins directs, c'est le cas de OSPF (Open Shortest Path First) et ISIS (Intermediate System to Intermediate System).**
- **Vecteur de distance, qui ne diffusent que leurs meilleures routes sur leurs interfaces, comme RIP(Routing Information Protocol) ou IGRP (Interior Gateway Routing Protocol).**