

**AVIS D'APPEL A CANDIDATURE**

N°2022-5025/APDP/PI/DA/SA/AB

CONTEXTE

L'Autorité de Protection des Données à caractère Personnel (APDP) est une autorité administrative indépendante créée par la loi n°2017-20 du 20 avril 2018 portant code du numérique en République du Bénin telle que modifiée par la loi n°2020- 35 du 06 janvier 2021. Elle est chargée de veiller à la protection des données personnelles nécessaire à celle de la vie privée et des libertés individuelles.

Dans le but de renforcer ses capacités opérationnelles, l'APDP recherche un Informaticien, immédiatement disponible pour emploi au Service Contrôle et Contentieux et pour formation complémentaire.

MISSION DU POSTE

L'Informaticien en poste au Service Contrôle et Contentieux de l'APDP a pour mission :

1. d'effectuer le contrôle des systèmes d'information et l'investigation, informatique numérique ou internetique et d'assister les suites contentieuses ;
2. d'assurer la gestion des plaintes, réclamations et litiges relatifs à la protection des données personnelles et de la vie privée ;
3. de développer au profit du bureau le contrôle de sécurité des applications et réseaux et de transmettre l'expertise en test d'intrusion, méthodes et outils d'analyse, exploitation de vulnérabilités, recherche de compromission à l'échelle d'un parc, équipement réseau, téléphone mobile, analyse matérielle, etc... et les outils d'investigation numérique.

ACTIVITES PRINCIPALES

En tant qu'expert technique en investigation informatique, numérique et internetique au sein du Service Contrôle et Contentieux de l'APDP, vous serez responsable de :

- l'analyse forensique de systèmes d'information : analyse de relevés

- techniques, d'images disques, d'images mémoires, de journaux d'événements et de traces système, réseau et applicatives, ainsi que l'analyse statique et dynamique de codes et documents malveillants.
- la recherche, l'identification et le traitement d'incident et les analyses techniques nécessaires au traitement de signalement de sécurité ou de violation de données personnelles
 - l'analyse de systèmes d'information : logiciels, parc informatique, matériels, équipement réseau, SCADA, téléphonie, etc et des mesures de remédiation
 - la conception et la réalisation des outils pour améliorer les opérations d'investigation et de contrôle
 - l'entretien et du développement de l'expertise en techniques et outils d'investigation, exploitation de vulnérabilités, méthodes et outils d'analyse.

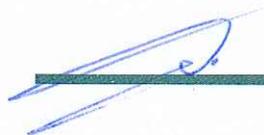
COMPETENCES TECHNIQUES

- Avoir de bonnes connaissances dans les domaines suivants :
 - informatiques et de la sécurité des systèmes d'information ;
 - systèmes d'exploitation ;
 - applications et leurs vulnérabilités
 - attaques et activités malveillantes ;
 - outils d'investigation numérique ;
 - protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation ;
 - langages de programmation de bas niveau et langages de scripts.
 - téléphones mobiles (systèmes d'exploitation, acquisition de données techniques, etc...) ;
 - équipements réseaux (systèmes d'exploitation, configuration, etc);
 - analyse matérielle (JTAG, acquisition et analyse de firmware, etc);
 - en programmation (Python, C/C++...) y compris d'un langage de programmation web (Java, PHP...)
 - SCADA (architecture, protocole réseau, etc...).
- Maîtriser l'environnement PC, Mac, Android
- Maîtriser l'utilisation des systèmes d'exploitation et réseaux et l'administration des réseaux informatiques
- Maîtriser la plupart des outils du Web 2.0 ;
- Maîtriser le langage HTML ;
- Connaître les techniques d'administration d'un réseau (LAN/WAN) ;

- Connaître les aspects techniques, fonctionnels et juridiques de la SSI et maîtriser le management et la sécurité informatique ;
- Être capable d'administrer et gérer des bases de données (SQL/MySQL/ACCESS) ;
- Capacité à assurer la gestion et le suivi des réseaux sociaux (en connaître les avantages et les inconvénients) ;
- Maîtriser l'incertitude d'une démarche rétrodictive;
- Maîtriser l'apport des diverses traces dans un contexte investigation de renseignement ou de démarche probatoire;
- Maîtriser les types de traces numériques (ordinateurs et appareils mobiles) et internetiques
- Maîtriser les problématiques liées au traitement de la preuve informatique : saisie du média ou de l'équipement suspect, sécurisation des données, préparation des traitements, analyse, archivage.
- Être capable :
 - d'appliquer des techniques et des protocoles d'investigation pour la collecte, l'identification, la description, la sécurisation, l'extraction, l'authentification, l'analyse, l'interprétation et l'explication des données numériques contenues dans des systèmes informatiques et dans des périphériques de stockage.
 - de capturer et d'analyser des données volatiles, notamment des séances actives de réseaux et des processus en cours. Collecte d'informations des navigateurs Web.
 - de réaliser des audits de code, de configuration, d'architecture et l'audit organisationnel

PROFIL DU TITULAIRE DU POSTE

Formation	BAC+4 ou plus en Informatique, Technologies, ingénieur en sécurité opérationnelle, Master of Science (MSc) in Forensic Science, Orientation Digital Investigation and Identification ou Certificate of Advanced Studies (CAS) en Investigation Numérique et Analyse de Données ou équivalent. Certification OSCP (Offensive security certified professional).
------------------	--



Expériences professionnelles	Justifier d'un minimum d'expérience opérationnelle à un poste similaire ou dans une fonction de pentester, ou dans la conception informatique et technologique.
-------------------------------------	---

APTITUDES PROFESSIONNELLES

- Disponibilité sur trois ans au moins ;
- Courtoisie et bonne éthique ;
- Initiative, Autonomie et rigueur ;
- Créativité et sens de l'innovation ;
- Confidentialité et intégrité ;
- Sens du travail bien fait.

DOSSIER A FOURNIR ET DATE LIMITE DE DEPOT DES DOSSIERS.

Les personnes intéressées par le présent avis devront présenter sous pli fermé, avec la mention « **CANDIDATURE AU POSTE D'INFORMATICIEN A L'APDP** » un dossier comprenant :

1. Une lettre de motivation adressée au Président de l'APDP ;
2. Un CV actualisé avec mention de trois (03) personnes de référence ;
3. Une copie légalisée du ou des diplôme(s) ;
4. Une copie simple des attestations de travail ou certificat de bonne fin ou tout document prouvant les expériences contenues dans le CV.

Le dossier présenté sous plis fermé est à déposer au **Secrétariat Administratif de l'APDP sis au 1^{er} étage du bâtiment EL- MARZOUK Joel parcelle I ilot 847 quartier Aïdjèdo, 01 BP 04837, Tél : (+229) 69 55 00 00** ou à envoyer par mail en version PDF à l'adresse contact@apdp.bj au plus tard le **21 Novembre 2022 à 17 heures** à la montre du hall d'entrée de l'APDP

MODALITES ET PROCESSUS DE SELECTION

- La sélection des candidats se fera par un Comité de sélection mis en place par décision du Président de l'APDP ;
- Seuls les candidats sélectionnés seront contactés pour apprécier les attentes et convenir d'une date d'entretien oral ou un test technique le cas échéant.
-

- Les entretiens de sélection pourront être menés en visio-conférence ou en présentiel.

Au terme des différents tests et après enquête de moralité, le candidat admissible, sera recruté. Le contrat comportera une période d'essai de trois (03) mois.



Yvon Detchenou
Yvon DETCHENOU

[Handwritten signature]

