BCEAO
BANQUE CENTRALE DES ÉTATS DE L'AFRIQUE DE L'OUEST

Avis N° 1 - Réponses aux questions formulées et report de la date limite de dépôt pour la Demande de Propositions relative à la "Sélection d'un prestataire pour les tests d'intrusion de la BCEAO" - DP/Z00/DBA/096/2025

I. Périmètre externe

Question 1 :

Combien d'adresses IP publiques ou d'URL exposées sur Internet doivent être incluses dans les tests ? Merci de distinguer les ressources relevant du périmètre PCI DSS et celles du périmètre étendu.

Réponse 1 :

- Périmètre PCI-DSS : 10 adresses IP publiques à tester.
- Périmètre étendu : Plus de 20 adresses IP/URL supplémentaires.

II. Tests applicatifs

Question 2 :

- Combien de profils utilisateurs doivent être évalués dans le cadre des tests applicatifs ? (par exemple : administrateur, utilisateur standard, modérateur, etc.)
- Quel est le nombre approximatif d'API exposées à auditer ?
- Merci d'indiquer les éléments correspondant au périmètre PCI DSS et ceux du périmètre étendu.

Réponse 2 :

- Périmètre PCI-DSS :
    - 1 application avec 1 profil utilisateur à tester.
    - Aucune API n'est à auditer dans ce cadre.
- Périmètre étendu :
    - Il est attendu que le prestataire identifie les profils utilisateurs et les API exposées lors de la mission.

III. Périmètre interne

Question 3 :

- Combien de VLANs sont actuellement configurés dans votre réseau interne ?
- Combien d'hôtes estimez-vous en moyenne par VLAN ?

Avenue Abdoulaye FADIGA
BP 3108 – Dakar - Sénégal
Tél. (221) 33 839 05 00 / Fax. (221) 33 823 93 35
courrier.bceao@bceao.int - www.bceao.int

- Merci de fournir ces informations pour le périmètre PCI DSS ainsi que pour le périmètre étendu.

Réponse 3 :

- Pour le périmètre PCI-DSS
    - 10 Vlans avec moins de 10 hôtes par VLAN
- Pour le périmètre étendu
    - 22 Vlans avec en moyenne 18 hôtes par VLAN

Question 4 :

Le soumissionnaire doit-il obligatoirement posséder l'ensemble de ces certifications (OSCP, CEH, CISSP, PCI-ASV) ?

Réponse 4 :

Le prestataire doit proposer une équipe d'experts disposant de certifications pertinentes en cybersécurité et tests d'intrusion (OSCP, CEH, CISSP, PCI-ASV, etc.). La possession de toutes ces certifications n'est pas obligatoire, mais le prestataire doit justifier des compétences requises pour la mission.

Question 5 :

La certification PCI-ASV est-elle obligatoire ? (En rappel, nous précisons que nos outils de scans de vulnérabilités sont certifiés PCI-ASV, mais la question concerne la qualification des intervenants.)

Réponse 5 :

Cette certification n'est pas imposée aux intervenants. Toutefois, une expertise équivalente en tests de vulnérabilités PCI-DSS est attendue.

Question 6 :

Dans le cadre de la phase d'ingénierie sociale (Lot 2), trois méthodologies sont mentionnées : phishing, vishing, smishing. Le prestataire a-t-il la liberté d'en appliquer une seule ou doit-il impérativement mettre en œuvre les trois approches ?

Réponse 6 :

Le prestataire peut proposer une ou plusieurs méthodes (phishing, vishing, smishing etc.) selon ses capacités. Aucune approche n'est imposée, mais la justification technique des choix est requise.

Question 7 :

À la page 7, section I.25, il est indiqué que « le délai d'exécution devra être mentionné dans la soumission » et qu'il commence à courir à la date de signature du marché. Or, à la page 10, section Lot 2 : Objectif, il est précisé que les activités peuvent être planifiées sur douze mois et réalisées en deux phases. Pourriez-vous clarifier les délais d'exécution attendus pour chaque lot et la façon dont ces passages doivent être interprétés ?

Réponse 7 :

Le prestataire doit indiquer dans sa soumission un calendrier détaillé (dates de début/fin par phase). Bien que les activités puissent s'étaler sur 12 mois (Lot 2), le délai contractuel court dès la signature.

IV. Lot 1 : Tests d'intrusion PCI-DSS

Question 8 :

Tests de la couche réseau externe

- Combien d'adresses IP sont incluses dans le périmètre ?
- Existe-t-il d'autres types d'actifs à tester (applications web, API, etc.) ? Si oui, merci d'indiquer leur nature et leur nombre.
- Concernant les tests en mode Grey Box, pourriez-vous indiquer les informations que vous seriez disposés à partager (ex. : identifiants, documentation, etc.) ?

Réponse 8 :

- Nombre d'IPs à tester : 10 IPs publiques.
- Autres actifs : 1 application web avec un profil utilisateur.

Question 9 :

Tests de la couche réseau interne

- Combien de segments réseau ou VLAN composent le CDE ?
- Combien de serveurs internes, imprimantes et équipements IoT sont inclus dans le périmètre ?

Réponse 9 :

Pour le périmètre PCI-DSS il existe 10 Vlans avec moins de 10 hôtes par VLAN. Les identifiants et documentation technique seront transmis au prestataire retenu.

Question 10 :

Tests d'intrusion applicatifs

- Combien de profils utilisateurs l'application Monétique comporte-t-elle ?
- Si l'application utilise un système d'accès basé sur des droits plutôt que des profils fixes, merci de nous le préciser.

Réponse 10 :

- Un profil utilisateur est prévu.
- Pour toute spécificité (droits personnalisés), des précisions seront fournies au prestataire retenu.

V. Lot 2 : Tests d'intrusion étendus

Question 11 :

Tests externes

- Combien d'API, de serveurs web, d'URLs ou d'applications accessibles depuis Internet sont concernés ?
- Merci de préciser tout autre actif à tester, ainsi que leur type (ex. : adresses IP) et leur nombre.

Réponse 11 :
La mission inclut la découverte des d'API, de serveurs web, d'URLs ou d'applications accessibles depuis Internet.

Question 12 :

Tests internes : Applications internes (Grey Box)

- Nombre exact d'**applications** à tester ?
- Pour chaque application, quels sont les profils d'accès (administrateur, utilisateur, contrôleur, etc.) ?
- Si l'accès est basé sur des droits personnalisés, merci de nous le confirmer.

Réponse 12 :

La mission inclut la découverte du nombre d'applications et des profils d'accès (admin, utilisateur, etc.). Les droits personnalisés relèvent également de cette phase. Les informations relatives aux connaissances partielles des systèmes seront communiquées aux testeurs durant les travaux.

Question 13 :

Tests internes : Réseaux internes (Grey Box) - Merci d'indiquer le nombre de **VLAN**, de **plages d'adresses réseau** ou, si possible, le nombre d'**adresses IP** à tester.

Réponse 13 :

En moyenne il y'a 22 Vlans avec en moyenne 18 hôtes par VLAN

Question 14 :

Tests d'intrusion de la couche réseau interne

- Cible : Infrastructure interne du périmètre CDE (réseaux locaux, commutateurs, serveurs internes, imprimantes, équipements IoT etc).

Test de segmentation réseau

- Cible : Vérification de l'isolation du périmètre PCI-DSS par rapport aux autres zones du réseau.

Ces tests se réalisent uniquement sur un de leurs locaux ou sur différents sites ?

Réponse 14 :

Les tests seront réalisés à partir du siège et pourront être étendus à d'autres sites.

Question 15 :

Tests d'intrusion internes : Applications internes (Grey Box)

- Cible : Applications métier critiques (RH, financier, gestion).

Il s'agit ici de tests d'applications Web je suppose, combien d'applications seront testées (le nombre exact) ?

Réponse 15 :

La mission inclut la découverte des applications, des serveurs web, des URL accessibles ainsi que la démonstration de l'exploitation des failles identifiées. Les informations relatives aux connaissances partielles des applications seront communiquées aux testeurs durant les travaux.

Question 16 :

Tests d'intrusion internes : Systèmes (Grey Box)

- Cible : OS (Windows/Linux), serveurs, postes de travail, bases de données.
- Méthodologie : Élévation de privilèges, exploitation des vulnérabilités non patchées.

Il s'agit sur ce dernier point d'un audit de configuration. Serait-il possible d'avoir une idée sur la liste exhaustive des technologies à analyser et leur quantité ?

Réponse 16 :

La mission inclut la découverte des serveurs, postes de travail et bases de données, accessibles ainsi que la démonstration de l'exploitation des failles identifiées. Les informations relatives aux connaissances partielles des systèmes seront communiquées aux testeurs durant les travaux.

NB : la date limite de dépôt des offres fixée initialement au 18 juin 2025 est reportée au 27 juin 2025.

Le Directeur du Budget et des Approvisionnements