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

Direction Générale de la Comptabilité et des Systèmes d'Information
Direction des Infrastructures Informatiques et des Réseaux

Réponses aux demandes de complément d'information relatives à l'appel d'offres N°AO/Z00/DBA/054/2026 pour la fourniture et le déploiement d'une plateforme unifiée de détection, d'analyse et de réponse aux incidents de cybersécurité en faveur de la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO)

Question 1 :

Dans le cadre de votre appel d'offres relatif à la fourniture et le déploiement d'une plateforme unifiée de détection, d'analyse et de réponse aux incidents de cybersécurité 100% on-premise, pourriez-vous nous préciser le nombre d'assets que vous prévoyez de superviser ?

Réponse 1 :

La solution devra intégrer l'ensemble des actifs numériques de la BCEAO. Conformément aux exigences de la section II.2, la solution devra gérer un nombre illimité de devices / IP / sources de logs, sans restriction de licence sur le nombre d'actifs supervisés.

Les soumissionnaires sont invités à préciser dans leur offre la capacité de leur solution en termes du nombre d'actifs supervisés.

Question 2 :

Concernant le dimensionnement de la solution, nous vous saurions gré de bien vouloir nous préciser, dans la mesure du possible :

- Le nombre estimatif d'adresses IP, d'équipements et de sources de logs à superviser ;
- Le volume journalier moyen des logs ainsi que le volume de pointe attendu, si ces informations sont disponibles ;
- La répartition prévisionnelle des sources de logs entre le Siège et l'Agence Principale de Dakar.

Réponse 2 :

Le Siège à Dakar constitue le site principal, concentrant l'essentiel des sources de logs. L'agence principale de Dakar est le site de haute disponibilité secondaire. Les sources de logs comprennent le siège et toutes les agences de la banque à travers les 8 pays de l'UEMOA.

Et conformément aux exigences de la section II.2, la solution devra gérer un nombre illimité de devices / IP / sources de logs, sans restriction de licence sur le nombre d'actifs supervisés avec une estimation minimale de 15 000 EPS/MPS par seconde permettant d'avoir une valeur estimative du volume de données.

Les soumissionnaires sont invités à préciser dans leur offre la capacité de leur solution en termes du nombre d'actifs supervisés.

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

Question 3 :

Le cahier des charges précise une durée minimale de licences d'un (1) an et une durée minimale de support de trente-six (36) mois. Ces deux durées créent une asymétrie contractuelle et financière qui ne nous permet pas de fonder un chiffrage cohérent sur la durée totale du marché. Nous souhaitons savoir :

(i) Quelle est la durée ferme du contrat ?

(ii) Les licences sont-elles attendues pour une (1) année renouvelable, ou pour la durée intégrale du marché (36 mois) ?

(iii) En cas de licence annuelle, la reconduction est-elle automatique ou conditionnée à un avenant ?

Question 4 :

Concernant les licences, le support et la maintenance, nous avons relevé que la partie relative à l'offre financière mentionne une solution avec licences et support technique d'une durée minimale d'un (1) an, tandis que les spécifications techniques exigent un support éditeur minimum de trente-six (36) mois ainsi qu'une durée minimale de support et maintenance de trente-six (36) mois.

Aussi, nous vous remercions de bien vouloir nous confirmer si l'offre attendue doit être établie sur la base :

- D'une durée minimale d' un (1) an pour les licences et le support technique ; ou
- D'un engagement couvrant trente-six (36) mois pour les licences, le support éditeur et la maintenance, conformément aux exigences techniques du dossier.

Réponse 3 & 4 :

La durée ferme du contrat est fixée à un (1) an.

Les licences, pour la première année de mise en service, sont valables pour une durée d'un (1) an, avec une activation qui devra intervenir uniquement à l'issue des installations.

Une proposition de support technique et de maintenance, d'une durée de trente-six (36) mois, est également requise.

Question 5 :

L'item 34 du tableau d'évaluation des offres techniques requiert un module intitulé «True Identity». Ce terme désigne un module propriétaire et une marque déposée d'un éditeur spécifique du marché SIEM.

Nous souhaitons savoir :

(i) ce terme renvoie-t-il à une fonctionnalité générique que le soumissionnaire peut couvrir avec une dénomination différente ? Si oui, quelle définition fonctionnelle la Banque retient-elle (corrélation d'identité multi-comptes, résolution d'entité unifiée, identité comportementale ?) ;

(ii) Ou s'agit-il d'un module spécifiquement développé par un éditeur désigné, auquel cas la Banque est invitée à préciser si une clause d'équivalence fonctionnelle est applicable ?

Réponse 5 :

La BCEAO confirme que l'exigence « True Identity » (item 34) doit être interprétée de manière fonctionnelle et non comme une référence à un produit d'un éditeur spécifique.

La fonctionnalité attendue est la résolution d'identité unifiée et multi-sources.Tout soumissionnaire proposant une solution couvrant nativement ces fonctionnalités, sous quelque dénomination commerciale que ce soit, sera évalué sur la base de la couverture fonctionnelle.

Question 6 :

La solution devant être déployée 100 % on-premise sur serveurs virtuels, nous avons besoin des éléments suivants pour proposer une architecture de déploiement conforme :

(i) Technologie d'hyperviseur en place (VMware vSphere, Microsoft Hyper-V, Nutanix AHV, KVM/Proxmox ou autre) ;
(ii) Version de l'hyperviseur ;
(iii) Ressources disponibles ou allouables à la plateforme (vCPU, RAM, stockage local ou SAN) ;
(iv) Topologie réseau entre le Siège et l'Agence Principale de Dakar (bande passante, latence, liens redondants).

Réponse 6 :

(i) Hyperviseur : L'infrastructure de virtualisation reposera sur (VMware vSphere ou Nutanix).

(ii) La version précise sera communiquée lors de la phase de déploiement après attribution du marché.

(iii) Ressources : La BCEAO mettra à disposition les ressources d'infrastructures systèmes nécessaires au déploiement de la solution.

(iv) Topologie réseau : Les soumissionnaires sont invités à fonder leur dimensionnement sur les prérequis systèmes recommandés par l'éditeur de la solution proposée et à documenter clairement les ressources nécessaires dans leur offre technique.

Question 7 :

La solution devra assurer une rétention minimale de six (6) mois en ligne et douze (12) mois en archive, avec support NAS/SAN/NFS. Sur la base du seuil de performance exigé (15 000 EPS/MPS), le volume de stockage nécessaire peut être estimé entre 50 et 80 téraoctets sur dix-huit mois, selon la verbosité moyenne des sources.
Nous souhaitons savoir :
(i) Quelle est la capacité de stockage NAS/SAN/NFS disponible ou provisionnée pour cette plateforme ?

(ii) Un investissement en infrastructure de stockage est-il attendu du prestataire ou est-il àla charge de la Banque ?

Réponse 7 :

(i) Infrastructure de stockage : Dans le cadre du présent appel d'offres, il n'est pas attendu d'offre relative à une infrastructure de stockage. Toutefois, les soumissionnaires sont invités à préciser dans leur offre la capacité minimale de stockage à fournir pour supporter la durée de rétention exprimée.

(ii) Dimensionnement : Les soumissionnaires devront inclure dans leur offre technique un plan de dimensionnement du stockage précisant le volume estimé nécessaire pour la rétention 6 mois online + 12 mois archive.

(iii) Architecture de stockage : La solution devra supporter les protocoles NAS/SAN/NFS conformément à la section II.7. Le prestataire devra documenter la configuration requise (taille des volumes, protocoles, IOPS minimum)

Question 8 :

La section II.18 du cahier des charges énumère les solutions existantes à intégrer, en utilisant le terme « notamment ». Ce terme non limitatif expose le prestataire à un risque de périmètre indéfini, pouvant conduire à des demandes d'intégration supplémentaires non chiffrées après la signature du marché. Nous souhaitons obtenir :

(i) La liste exhaustive et limitative des solutions à intégrer, avec leurs noms d'éditeurs et versions ;

(ii) Confirmation que toute intégration non listée dans cette liste fera l'objet d'un avenant tarifaire distinct.

Question 9 :

L'intégration avec l'écosystème existant (XDR/NDR, PAM, FIM, scanner de vulnérabilités, messagerie, ITSM, Cyber Range, pare-feux, IDS/IPS, systèmes d'authentification) est une composante majeure du marché.

La faisabilité et le chiffrage de ces intégrations dépendent directement des éditeurs et versions déployés.

Nous sollicitons pour chaque famille de solutions : le nom de l'éditeur, le nom du produit et sa version actuellement en production.

Réponse 8 & 9 :

Pour des raisons de confidentialité, les noms d'éditeurs et versions des solutions de sécurité actuellement en production ne peuvent être communiqués.

Toutefois il est précisé que :

- La solution proposée devra offrir plus de 1 000 intégrations natives de règles de détections et réponses (cf. section II.2), pouvant s'intégrer avec les principales solutions du marché pour chaque famille technologique listée à la section II.18 ;
- La disponibilité des connecteurs natifs pour les éditeurs majeurs du marché sera évaluée lors de l'analyse technique des offres ;
- Les soumissionnaires devront documenter la liste complète de leurs connecteurs natifs;
- Le prestataire retenu aura accès aux informations détaillées de l'environnement lors de la phase de cadrage post-attribution.

L'évaluation technique portera notamment sur la richesse de l'écosystème de connecteurs natifs.

Question 10 :

Le cahier des charges exige un support technique 24/7 pendant au moins 36 mois. La qualification du dispositif de support requis dépend de la contrainte géographique attendue par la Banque.

Nous souhaitons savoir :

(i) le support 24/7 doit-il être assuré par des ressources physiquement présentes en Afrique de l'Ouest ou localisées à Dakar ?

(ii) ou un centre de support international avec disponibilité 24/7 en langue française est-il acceptable ?

(iii) les délais d'intervention sur site sont-ils définis (GTI / GTR) ?

Réponse 10 :

Les soumissionnaires devront préciser dans leur offre les détails du support technique proposé.

Question 11 :

Le programme de formation couvre cinq modules (administration plateforme, analyste SOC, investigation SIEM, création de playbooks SOAR, exploitation UEBA) et doit inclure des formations certifiantes de niveau SANS/GIAC ou équivalent.

Afin de dimensionner le programme et d'identifier les accréditations de formation requises, nous souhaitons connaître :

(i) Le nombre de participants envisagés par profil (administrateurs, analystes N1, N2, RSS) ;
(ii) Si les formations certifiantes sont attendues pour l'ensemble des participants ou pour un sous-ensemble désigné ;
(iii) Les formations sont-elles prévues dans les locaux de la Banque (Dakar) ou des déplacements des participants sont-ils envisagés ?

Réponse 11 :
Nombre de participants : 11 dont 2 administrateurs système et 9 analystes SOC.
Les soumissionnaires sont invités à faire des propositions de formation au format adéquat.

Question 12 :
Les modules Network Forensics, Network Monitoring et Network Behavior Analytics, ainsi que l'action SOAR d'extraction PCAP, nécessitent des points de capture réseau (pots SPAN ou sondes TAP).

Nous souhaitons savoir :
(i) des ports SPAN ou des TAP sont-ils déjà en place sur les équipements réseau critiques (cœur de réseau, DMZ, liaisons inter-sites) ?

(ii) Si non, leur mise en place est-elle incluse dans le périmètre du présent marché ou reste-t-elle à la charge de la Banque ?

Réponse 12 :
Les soumissionnaires sont invités à préciser dans leur offre les prérequis nécessaires, ainsi que la répartition des prestations à la charge des différentes parties.

Question 13 :
Le cahier des charges prévoit un plan de migration SIEM parmi les livrables attendus. La complexité et le coût de cette migration dépendent directement du volume d'historique à transférer et des formats de données de la solution existante.
Nous souhaitons savoir :
(i) Quel est le SIEM/SOAR actuellement en production (éditeur, produit, version) ?
(ii) La migration de l'historique des logs est-elle attendue, et si oui, sur quelle durée (3 derniers mois ? 6 mois ? totalité) ?
(iii) La migration des règles de corrélation et des configurations existantes est-elle également dans le périmètre ?

Réponse 13 :
(i) SIEM/SOAR existant : Pour des raisons de confidentialité, les informations relatives au SIEM/SOAR actuellement en exploitation ne peuvent être communiquées.
(ii) Migration des logs historiques : La migration de l'historique des logs n'est pas exigée. Le plan de migration SIEM attendu comme livrable (section II.16) porte principalement sur le plan de transition opérationnelle entre l'ancienne et la nouvelle plateforme.
(iii) Migration des règles de corrélation : La migration des règles de corrélation n'est pas exigée. Le prestataire devra configurer les règles natives de la nouvelle plateforme et les adapter à l'environnement de la Banque (section II.18), en s'appuyant sur les use cases prédéfinis et les nouveaux use cases.
Par contre, pour la continuité de service : le prestataire devra proposer dans son plan de migration un schéma de transition assurant la continuité de la supervision de sécurité pendant le déploiement.

Question 14 :

En application de la section I.28 du dossier, le versement d'une avance au démarrage est conditionné à la fourniture d'une lettre de garantie à première demande délivrée par un établissement de crédit reconnu par la BCEAO.

Nous souhaitons obtenir :

(i) La liste ou les critères permettant d'identifier les établissements de crédit reconnus par la Banque pour l'émission de cette garantie ;

(ii) Les établissements hors zone UMOA peuvent-ils émettre cette garantie (par exemple via une banque correspondante en zone UMOA) ?

Réponse 14 :

La BCEAO communiquera au soumissionnaire retenu les informations relatives à l'établissement de la lettre de garantie.

Question 15 :

Le cahier des charges liste parmi les actions automatisées SOAR des opérations à fort impact sur l'infrastructure de production : désactivation de comptes Active Directory, mise en quarantaine de machines, suppression de fichiers malveillants, extraction de dumps mémoire.

Nous souhaitons comprendre :

(i) La Banque attend-elle une automatisation complète de ces actions (sans intervention humaine) ou un processus de validation par un analyste est-il requis pour tout ou partie de ces actions ?

(ii) Des matrices de décision (seuils de score de risque déclenchant l'automatisation vs l'escalade) sont-elles déjà définies ou sont-elles à proposer par le prestataire ?

Réponse 15 : Les soumissionnaires sont invités à préciser dans leur offre les prestations associées à la mise en œuvre de leur solution au regard des exigences du cahier des charges, notamment le niveau d'automatisation atteignable au terme du déploiement.

Question 16 :

La section I.26 du dossier précise que la prestation aura lieu au Siège de la BCEAO et à l'Agence Principale de Dakar. La BCEAO opère également à travers huit (8) Directions Nationales réparties dans les États membres de l'UMOA.

Nous souhaitons confirmer :

(i) Le périmètre du présent marché est-il strictement limité aux deux sites de Dakar (Siège + Agence Principale) ?

(ii) Le déploiement dans les Directions Nationales est-il exclu du marché actuel ou envisagé dans une seconde phase ?

(iii) Si une extension est envisagée, peut-elle faire l'objet d'options dans l'offre ?

Réponse 16 :

La BCEAO confirme les éléments suivants :

Le présent marché s'applique à l'ensemble des sites de la BCEAO répartis dans les huit pays de l'Union.

Question 17 :

La BCEAO, en tant que régulateur monétaire et superviseur bancaire de l'UMOA, est soumise à des exigences de reporting en matière de gestion des risques informatiques (directives COBAC, recommandations de la Commission Bancaire de l'UMOA).

Nous souhaitons savoir si la plateforme devra produire des rapports de conformité réglementaire (tableaux de bord RSSI, rapports d'audit, indicateurs de maturité cybersécurité)

à destination de la Direction Générale ou des autorités de tutelle, et si oui, selon quels formats et référentiels.

Réponse 17 :
Les soumissionnaires sont invités à préciser dans leur offre, les fonctionnalités de reporting de leur solution, notamment les types de rapports produits.

Question 18 :

Le cahier des charges exige que la plateforme fonctionne entièrement on-premise sans dépendance cloud, tout en intégrant un véritable moteur d'apprentissage automatique. Les modèles d'IA/ML requièrent généralement des mises à jour régulières (enrichissement des modèles, correction de dérives).
Nous souhaitons savoir quel mécanisme de mise à jour des modèles IA/ML est accepté par la Banque :
(i) Mise à jour entièrement manuelle via support amovible ?
(ii) Mise à jour via un canal dédié sécurisé non public (proxy interne) ?
(iii) La Threat Intelligence externe peut-elle transiter par un proxy approuvé par la Banque ?

Réponse 18 :
Les soumissionnaires sont invités à préciser , dans leur offre technique, le mécanisme de mise à jour proposé, la fréquence prévue, ainsi que les prérequis éventuels.

Question 19 :
La conception des playbooks SOAR et des règles d'escalade dépend de l'organisation des équipes SOC internes. Nous souhaitons savoir si le SOC de la Banque fonctionne en mode 8x5 (horaires de bureau) ou en mode 24/7 avec des équipes en rotation, afin d'adapter les mécanismes d'astreinte et d'escalade automatique hors-heures.

Réponse 19 :
Les soumissionnaires sont invités à préciser dans leur offre, les fonctionnalités de leur solution qui spécifiques aux modes d'organisation d'un SOC (internes, hybride, externalisé).

Question 20 :
La plateforme intègre un module Threat Intelligence natif. L'efficacité de ce module repose en partie sur des flux de renseignements externes (IOC, TTPs, feeds spécialisés). Nous souhaitons savoir si la Banque dispose déjà d'abonnements à des flux de Threat Intelligence externe (ISAC,CERT, fournisseurs commerciaux) qui devront être intégrés à la plateforme.

Réponse 20:
Les soumissionnaires sont invités à préciser dans leur offre, les fonctionnalités de leur solution qui sont spécifiques à l'intégration des flux de Threat Intelligence externe, ainsi que les pré-requis pour la mise en œuvre des modules natifs de leur solution.

Question 21 :
Le cahier des charges prescrit un support 24/7 mais ne définit pas de niveaux de service (GTI, GTR, taux de disponibilité de la plateforme, délais de résolution par sévérité d'incident). Nous souhaitons savoir si la Banque a des SLA préétablis que le prestataire devra respecter, ou si les niveaux de service sont à proposer par le soumissionnaire dans le cadre de son offre.

Réponse 21 :
Les soumissionnaires sont invités à préciser les niveaux de service relatifs au support proposé.

Question 22 :
Le chiffrement de toutes les communications internes de la plateforme est exigé. Ce chiffrement repose sur des certificats TLS. Nous souhaitons savoir si la Banque dispose d'une infrastructure à clé publique (PKI) interne émettant des certificats pour les composants internes, ou si le prestataire devra proposer une stratégie de gestion des certificats dans le cadre du déploiement.

Réponse 22 :
Les soumissionnaires sont invités à préciser dans leur offre les prérequis relatifs à la mise en œuvre du chiffrement.

Question 23 :
La réussite du projet repose sur une collaboration étroite avec les équipes internes (équipes SOC, équipes système, équipes réseau, équipes applicatives). Nous souhaitons comprendre l'organisation prévue par la Banque pour la gouvernance du projet :
(i) Un chef de projet côté Banque sera-t-il désigné ?
(ii) Quelles équipes internes seront mobilisées et dans quelle mesure (temps plein, temps partiel) ?
(iii) Y a-t-il des périodes de congé ou d'indisponibilité connues sur les prochains mois qui pourraient contraindre le planning ?

Réponse 23 : Le volet relatif à la gestion du projet sera abordé en temps opportun avec le prestataire retenu. Toutefois les soumissionnaires sont invités à indiquer dans leur offre, l'organisation des équipes adéquate pour une exécution optimale des travaux.

Question 24 :
Pourriez-vous préciser si l'exigence d'un déploiement on-premise exclut les solutions basées sur le cloud ?
Question 25 : Un déploiement sur de l'infrastructure AWS serait-il acceptable au regard des exigences de déploiement du cahier des charges ?

Réponse 24 &25 : Il est attendu une offre pour une solution sur site. Toute solution dans le Cloud est exclue