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

AVIS N° 4

FOURNITURE ET 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 - AO/Z00/DBA/054/2026

Question 1 :
Concernant le nombre des analystes simultanés souhaité pour le SOAR, est-ce un nombre défini ou la licence doit être illimitée en nombre d'analystes ?

Réponse 1 :
Le nombre d'analystes simultanés doit être illimité, afin de permettre une utilisation flexible du SOAR sans contrainte de licence.

Question 2 :
Pour le UEBA, Le nombre d'utilisateurs à couvrir est-il prédéfini, ou la solution doit couvrir un nombre illimité d'utilisateurs sans limitation de licence ?

Réponse 2 :
La licence UEBA doit couvrir un nombre illimité d'utilisateurs, afin de répondre aux besoins actuels et futurs de la banque sans restriction.

Question 3 :
Quelle est la taille moyenne de chaque logs à prendre en compte pour le dimensionnement de la solution ?

Réponse 3 :
La taille moyenne des logs à considérer pour le dimensionnement est d'environ 800 bytes par log.

Question 4 :
Vous avez mentionné un minimum de 15 000 EPS. Est-ce que cela veut dire que la solution doit être capable de gérer des pics au-delà de ce seuil de manière soutenue, sans perte de logs, sans dégradation des performances de recherche et sans recours à des mécanismes de mise en cache ou de buffering ?

Réponse 4 :
La solution doit supporter un minimum de 15 000 EPS, avec la capacité de gérer des pics au-delà de ce seuil de manière continue, sans perte de logs, sans dégradation des performances de recherche, sans mise en cache, et sans coût additionnel.

Question 5 :
Est-il requis que l'ensemble des composants d'intelligence artificielle, y compris les modèles et les LLM, soient déployés on-premise ?

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

Réponse 5 :
Oui, l'ensemble des composants d'intelligence artificielle, y compris les modèles et les LLM, doivent être entièrement déployés on-premise, sans aucune communication avec le cloud. Le fonctionnement complet de l'IA ne doit nécessiter aucune connexion externe.

Question 6 :
Le niveau de détail attendu pour les documents de procédures (haut niveau vs opérationnel détaillé).

Réponse 6 :
Les documents de procédures attendus devront être de niveau opérationnel détaillés, exploitables directement par les équipes SOC de la Banque sans adaptation majeure.
Ils devront décrire les étapes précises, les acteurs impliqués, les outils utilisés et les critères de décision.

Question 7 :
Le périmètre exact (exploitation SIEM, gestion des incidents, SOAR, etc.) ;

Réponse 7 :
Le périmètre minimal attendu (en cohérence avec les livrables de la section II.16) :
- Procédures d'exploitation SIEM (collecte, normalisation, corrélation, gestion des alertes) ;
- Procédures de gestion des incidents de sécurité ;
- Procédures d'utilisation des playbooks SOAR ;
- Procédures d'administration de la plateforme ;
- Procédures de maintenance et de sauvegarde.

Question 8 :
L'existence éventuelle d'un modèle ou template interne à respecter.

Réponse 8 :
La BCEAO n'impose pas de template interne. Les soumissionnaires proposeront leurs propres modèles de documents dans le cadre de leur offre, qui seront validés par les équipes de la Banque lors du déploiement.

Question 9 :
Pourriez-vous préciser le nombre de personnes à former, la répartition par profil (administrateurs, analystes SOC, exploitants, etc.) ainsi que le format attendu des formations (présentiel, distanciel, certifiant) ?

Réponse 9 :

Le nombre total de participants est fixé à 11 personnes, comprenant des analystes SOC, des administrateurs SOC ainsi que le Chef du service SOC.

Les formations relatives à la plateforme proposée, notamment les formations administrateur, analyste, investigation, création de playbooks et exploitation des fonctionnalités UEBA, concernent l'ensemble des 11 participants. Elles seront dispensées selon le format proposé par le soumissionnaire, tous frais compris dans l'offre.

Les formations certifiantes de type SANS/GIAC, ou toute certification équivalente reconnue à l'international, devront être réalisées en ligne ou dans un centre de formation spécialisé .

Les formations et certifications visées sont notamment les suivantes :

- SEC511 – Continuous Monitoring & Security Operations : 4 participants
- SEC545 – GenAI and LLM Application Security : 4 participants

- SEC555 – SIEM with Tactical Analytics : 4 participants
- LDR551 – Building and Leading Security Operations Centers : 1 participant

Question 10 :
Concernant l'exclusion des technologies ELK/OpenSearch, nous souhaiterions comprendre les motivations sous-jacentes à cette exigence. Notre plateforme SIEM repose sur une architecture ELK mature. Nous souhaiterions respectueusement demander la révision, voire la suppression de cette clause.

Réponse 10 :
La BCEAO recherche avant tout une solution simple à maintenir, homogène dans son architecture et limitée en nombre d'outils, tout en garantissant les niveaux de performance requis. Une plateforme SIEM native développée par un éditeur unique répondant à cet objectif est attendue, en évitant la complexité et les risques opérationnels liés aux assemblages hétérogènes.

Cette clause est une exigence ferme du présent appel d'offres.

Question 11 :
« Moteur Big Data natif intégré » : quelles sont les attentes précises derrière cette exigence (technologies, performances, architecture) ?

Réponse 11 :

« Moteur Big Data natif intégré »
La BCEAO attend un moteur de traitement et d'indexation des événements de sécurité développé nativement par l'éditeur de la solution, capable d'ingérer et de corréler en temps réel un minimum de 15 000 EPS/MPS sans perte de données, avec une capacité de recherche sur l'historique (6 mois online) sans dégradation des performances.

« True Machine Learning AI »
La BCEAO attend un moteur d'apprentissage automatique capable de détecter des comportements anormaux, de générer des scores de risque dynamiques et d'identifier des menaces inconnues, en s'améliorant progressivement grâce aux retours des analystes SOC et le comportement des utilisateurs. Le tout devra fonctionner entièrement on-premise sans dépendance cloud.

« True Identity »
Il s'agit d'une fonctionnalité de résolution d'identité unifiée et multi-sources, permettant de corréler les différents comptes et identifiants d'un même utilisateur (AD, LDAP, VPN, messagerie, badge) afin d'avoir une vue consolidée de son activité. Une clause d'équivalence fonctionnelle est applicable.

Question 12 :

Afin d'adapter au mieux notre proposition, nous souhaiterions disposer de précisions complémentaires concernant :

- Le nombre d'actifs à superviser (postes, serveurs, équipements réseau)
- Les volumes de logs attendus (EPS / Go par jour)
- Le nombre de sites ou segments réseau concernés

Réponse 12 :

Nombre d'actifs à superviser
Conformément à la section II.2 du cahier des charges, la solution devra gérer un nombre illimité d'actifs / IP / sources de logs sans restriction de licence. Le périmètre couvre le Siège et

les agences Principales et Auxiliaires de la Banque, mais la solution sera déployée au siège de la banque et sur le site de l'agence principale de Dakar (section II.18) pour assurer une haute disponibilité.

Volumes de logs attendus
Le seuil minimal de performance requis est de 15 000 EPS/MPS (section II.2). Pour le dimensionnement, les soumissionnaires pourront retenir les hypothèses suivantes :

- Volume minimal : 15 000 EPS
- Volume de stockage estimé : entre 50 et 80 To sur 18 mois fournie par la banque, sur la base d'une rétention de 6 mois online et 12 mois en archive (section II.7)

Le Directeur du Budget et des Approvisionnements