BCEAO

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

DOSSIER D'APPEL D'OFFRES N° AO/Z00/DBA/054/2026

SÉLECTION D'UN PRESTATAIRE POUR LA FOURNITURE ET LE DÉPLOIEMENT D'UNE PLATEFORME UNIFIÉE DE DÉTECTION, D'ANALYSE ET DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ

Mars 2026

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

PREMIÈRE PARTIE : INSTRUCTIONS AUX SOUMISSIONNAIRES

Préambule

La Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) est l'Institut d'émission commun aux huit (8) Etats membres de l'Union Monétaire Ouest Africaine (UMOA), à savoir le Bénin, le Burkina, la Côte d'Ivoire, la Guinée-Bissau, le Mali, le Niger, le Sénégal et le Togo.

La BCEAO exerce ses activités à travers :

- le Siège, à Dakar (Sénégal) ;
- une Direction Nationale dans chacun des Etats membres, comprenant une Agence Principale et une ou plusieurs Agences Auxiliaires ;
- le Secrétariat Général de la Commission Bancaire (SGCB) de l'UMOA, sis à Abidjan ;
- le Centre de Traitement Fiduciaire (CTF), sis à Yamoussoukro ;
- la Représentation auprès des Institutions Européennes de Coopération (RIEC), sise à Paris.

SECTION I : DISPOSITIONS GENERALES

I.1. Conditions de participation

La participation au présent appel à concurrence est ouverte à tous les soumissionnaires éligibles, disposant de qualifications techniques et financières correspondant aux exigences du cahier des charges.

Toutefois, les sociétés impliquées dans des activités illégales, notamment le blanchiment des capitaux, le financement du terrorisme, la corruption, les pratiques collusoires, frauduleuses ou coercitives, ne sont pas autorisées à prendre part au présent appel à concurrence.

En outre, tout candidat en situation de conflit d'intérêt devra en informer la Banque Centrale dans sa lettre de soumission, en précisant les termes dudit conflit d'intérêt.

I.2. Frais de soumission

Il n'est pas exigé de garantie de soumission.

Le soumissionnaire supportera tous les frais afférents à la préparation et à la présentation de son offre. La Banque Centrale ne sera en aucun cas responsable de ces frais, ni tenue de les régler, quels que soient le déroulement et l’issue de la procédure d’appel d’offres.

I.3. Monnaie de soumission et de paiement

La monnaie utilisée est le franc CFA. Toutefois, les soumissions valorisées en euros seront acceptées pour les fournisseurs établis hors de la zone UMOA. Cependant, pour des besoins de comparaison, toutes les offres seront converties en francs CFA.

I.4. Régime fiscal

En vertu des dispositions des articles 28 du Traité de l’Union Monétaire Ouest Africaine (UMOA), du 20 janvier 2007, 7 des Statuts de la BCEAO, 10, paragraphe 10-1 du Protocole relatif aux privilèges et immunités de la BCEAO, annexés audit Traité, [8 de l'Accord de Siège conclu le 21 mars 1977 entre le Gouvernement de la République du Sénégal et la BCEAO], et 11 de l'Accord de coopération entre la République Française et les Républiques membres de l'UMOA, du 4 décembre 1973, la Banque Centrale bénéficie, dans le cadre de ce marché, du régime de l’exonération de tous impôts, droits, taxes et prélèvements d'effet équivalent dus dans les Etats membres de l’UMOA.

A ce titre, les formalités d’obtention du titre d’exonération seront accomplies par le transitaire du fournisseur en relation avec les services compétents de la BCEAO, le cas échéant.

I.5. Langue de soumission

Les offres et tous les documents concernant la soumission, échangés entre le soumissionnaire et la Banque Centrale, devront être rédigés en langue française.

I.6. Groupement

Les groupements sont autorisés dans le cadre du présent appel d'offres. Toutefois, seule la forme “groupement solidaire” est acceptée.

A ce titre, les entreprises concernées devront présenter, dans leur soumission, l'acte constitutif du groupement signé par les Parties. Ce document devra indiquer, en outre, le chef de file dudit groupement.

Ainsi, l’absence dudit document dans la soumission constituerait un motif de rejet de celle-ci, le cas échéant.

I.7. Sous-traitance

La sous-traitance est subordonnée à l'accord préalable écrit de la Banque Centrale. Si elle est autorisée, la sous-traitance ne pourra excéder trente pour cent (30%) de la valeur du contrat de base.

I.8. Conformité des offres

Toute offre qui ne répondra pas explicitement aux exigences du présent dossier d'appel d'offres sera déclarée non conforme.

I.9. Evaluation des offres

Une Commission des Marchés procédera à la vérification de la conformité technique, à l'évaluation financière et au classement des offres reçues.

Préalablement à l'évaluation des offres, la BCEAO se réserve le droit de procéder à la vérification de l'éligibilité des soumissionnaires, eu égard notamment aux législations relatives à la lutte contre les activités illégales visées à l’article I.1, alinéa 2, en vigueur dans l'espace UMOA.

L'évaluation des offres se fera sur la base de l’examen de leur conformité aux spécifications techniques du dossier d’appel d’offres, d'une part, de l'analyse et la comparaison des prix proposés, d’autre part.

Il sera procédé à des ajustements de prix en cas d'erreurs arithmétiques. De même, s’il y a contradiction entre le prix indiqué en lettres et en chiffres, le montant en lettres fera foi.

A l'issue du dépouillement, le marché pourra faire l'objet de négociations commerciales avec le soumissionnaire pressenti.

Le montant de l'offre du soumissionnaire devra correspondre à cent pour cent (100%) des livrables proposés.

I.10. Vérification de la qualification des soumissionnaires

La Banque Centrale se réserve le droit de vérifier par tous les moyens appropriés les capacités technique et financière, notamment la solvabilité, du fournisseur classé premier à exécuter le marché de façon satisfaisante.

Cette vérification sera fondée sur l'examen des preuves de qualification que la Banque Centrale jugera nécessaires. Si le résultat n'est pas satisfaisant, le soumissionnaire est déclaré non qualifié au profit de celui classé second, qui sera soumis aux mêmes contrôles.

I.11. Attribution du marché

Le marché sera attribué à un soumissionnaire dont l’offre est jugée économiquement avantageuse pour la Banque Centrale au terme de l'analyse des spécifications techniques et des prix unitaires proposés.

La BCEAO se réserve le droit d'accepter ou de refuser toute offre, et d'annuler l'appel d'offres en rejetant toutes les offres, à tout moment, avant l'attribution du marché.

Préalablement à l'attribution du marché, la BCEAO s’autorise de procéder à une vérification du caractère raisonnable des prix proposés dans le cadre de la présente procédure. Une conclusion négative (des prix déraisonnablement élevés ou bas) constitue un motif de rejet de l'offre, à la discrétion de la BCEAO. Dans ce cas, elle invitera le soumissionnaire classé deuxième à l'issue de l'évaluation technique et financière des offres pour des négociations.

I.12. Publication des résultats et notification du marché

Les résultats de l'appel d'offres seront publiés sur le site internet de la BCEAO.

A cet égard, tout candidat pourra former un recours gracieux par écrit, adressé au Directeur Général de l'Administration et des Ressources Humaines dans un délai maximum de cinq (5) jours ouvrés, à compter de la publication des résultats.

Le recours ne pourra porter que sur l'attribution du marché. Le délai de réponse de la BCEAO sera de dix (10) jours maximum. Passé ce délai et sans une réponse de la BCEAO, le recours devra être considéré comme rejeté.

L'attribution du marché sera notifiée au soumissionnaire retenu. Un contrat lui sera soumis pour signature. La date de signature du contrat par les deux Parties constitue le point de départ des délais contractuels d'exécution du marché.

I.13. Confidentialité

Dans le cadre de la présente procédure, chaque partie s'engage à préserver le caractère confidentiel de toute information communiquée comme telle. Ainsi, le prestataire sera tenu notamment de :

- garder confidentiels tous documents et informations de quelque nature qu'ils soient, qui lui auront été communiqués par la BCEAO ou dont il aura eu connaissance, quels qu'en soient la forme, le support et le contenu, dans le cadre de l'exécution de ses prestations ;
- n'utiliser ces documents et informations qu'aux seules fins d'exécuter le marché. En conséquence, même après la cessation du contrat, le prestataire ne peut les communiquer à des tiers ou les exploiter dans ses relations avec ceux-ci, sans avoir obtenu, au préalable, l'autorisation écrite de la BCEAO ;
- prendre toutes les dispositions nécessaires, notamment auprès des membres de son personnel appelés à prendre connaissance de ces documents ou à connaître ces informations, et dont le prestataire répond entièrement en la matière, pour prévenir et éviter leur divulgation à des tiers, de quelque manière que ce soit ;
- restituer ou détruire, sans délai à la BCEAO, à sa demande, au terme de l'exécution de la présente mission ou à la date de prise d'effet de la protection, les documents, rapports et données et autres informations qu'elle juge confidentiels.

I.14. Assurance

Le soumissionnaire retenu et/ou son sous-contractant éventuel devront, à leur charge, souscrire des polices d'assurance valables pendant toute la durée du contrat et couvrant au moins les risques de transport et de livraison.

I.15. Litiges et contestations

Les Parties s'efforceront de régler à l'amiable tout différend né de l'exécution ou de l'interprétation du marché.

A défaut de règlement à l'amiable, le différend sera, de convention expresse, soumis à l'arbitrage selon le Règlement d'arbitrage de la Cour Commune de Justice et d'Arbitrage (CCJA) de l'Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA), et tranché par un (1) arbitre ad hoc désigné conformément à ce Règlement.

L'arbitrage se déroulera en langue française à Dakar (Sénégal), selon le droit sénégalais.

Les frais de l'arbitrage seront à la charge de la Partie succombante.

SECTION II : DISPOSITIONS PARTICULIERES

I.16. Objet

Le présent appel d'offres a pour objet la sélection d'un prestataire spécialisé en cybersécurité en vue de la fourniture et du déploiement d'une plateforme intégrée de détection, d'analyse et de réponse aux incidents de cybersécurité, incluant le transfert de compétences au profit des équipes en charge des opérations de cybersécurité.

Cette plateforme vise à remplacer la solution SIEM existante devenue obsolète par une plateforme de dernière génération en vue de la collecte centralisée, la corrélation avancée et l'analyse intelligente des événements de sécurité, ainsi que l'orchestration et l'automatisation des réponses aux incidents de cybersécurité.

I.17. Allotissement

Le présent appel d'offres est constitué d'un lot unique et indivisible.

I.18. Visite des lieux

Il n'est pas prévu de visite des lieux dans le cadre du présent appel d'offres.

I.19. Options

La proposition d'options est autorisée dans le cadre de cet appel d'offres. Toutefois, la validation de celles-ci reste à la discrétion de la Banque Centrale.

I.20. Variantes

Aucune variante n'est sollicitée dans le cadre de cet appel d'offres.

I.21. Présentation des soumissions

Les offres devront comprendre les quatre **(4) parties distinctes** ci-après :

- une lettre de soumission dûment signée par le responsable habilité ;
- une présentation du soumissionnaire ;
- une offre technique ;
- une offre financière.

I.21.1. Lettre de soumission

Le candidat devra produire une lettre de soumission selon le modèle joint en **Annexe 1**, précisant tous les éléments de son offre. Cette lettre devra être signée par le représentant dûment habilité de l'entreprise soumissionnaire.

I.21.2. Présentation du soumissionnaire

La présentation du soumissionnaire devrait comprendre au minimum les informations et documents ci-après :

- la fiche d'information du soumissionnaire dont le modèle est joint en **Annexe 2**.
- une présentation générale de la société (dénomination, adresse, zones de couverture) ainsi que les copies des documents attestant du statut juridique et du numéro d'immatriculation de la société au registre de commerce ;
- le nom du représentant local pour la prise en charge du service après-vente, le cas échéant ;
- l'attestation d'immatriculation et de paiement des cotisations à l'Institution de sécurité sociale et fiscale ;
- la liste d'au moins trois (3) références de projets similaires réalisés justifiées par des attestations de bonne exécution ;
- les états financiers des trois derniers exercices.

Par ailleurs, le soumissionnaire devra fournir un relevé d'identité bancaire conforme aux normes de codification bancaire internationales.

I.21.3. Offre technique

L'offre technique devrait comprendre :

- le tableau d'évaluation des offres techniques dûment renseigné (voir **Annexe 3**)
- la description de la prestation ;
- le planning détaillé des tâches à réaliser pour l'exécution de la mission ;
- une méthodologie claire et détaillée pour la mission, incluant des phases de diagnostic, de conception, de mise en œuvre et de validation ;
- la liste des livrables ;
- les références de missions similaires conduites auprès d'autres entités ;
- la durée de la prestation ;
- la charge de travail en jours/homme en fonction des profils ;
- l'organisation de l'équipe d'intervention et les C.V. et certificats Individuels des intervenants comportant un consultant côté éditeur qui va réaliser le déploiement et un Project Manager pour assurer le suivi des tâches ;
- les modèles de documents de procédures ;
- tout autre document que le prestataire juge nécessaire à la bonne compréhension et à la qualité de son offre.

I.21.4. Offre financière

L'offre financière doit être exprimée hors taxes et hors douane en franc CFA ou en euros. Elle devra inclure tous les frais de déplacement et de séjour.

Le prestataire doit proposer une offre portant sur une solution avec des licences et un support technique d'une durée d'au moins un (1) an.

La Banque Centrale ne s'occupera pas de l'organisation des déplacements et du séjour du prestataire qui devra évaluer les frais y afférents et les inclure dans son offre financière.

Les conditions devront être détaillées (en nombre ou volume horaire et prix) en faisant ressortir notamment les éléments ci-après :

- honoraires ;
- frais de déplacement ;
- frais de séjour ;
- frais de logistique (secrétariat, télécommunication, etc…).

Toute prestation ou service proposé par le prestataire dans son offre et pour lequel aucun prix n'est fourni sera considéré comme inclus dans l'offre principale et ne donnera lieu à aucune facturation supplémentaire.

I.22. Période de validité des offres

La validité des offres devra être d'au moins **120 jours à compter de la date limite de dépôt** de celles-ci.

I.23. Date et heure limite de transmission des offres

Les offres devront être déposées sous plis fermé à l'adresse : **Siège de la BCEAO, Avenue Abdoulaye FADIGA – BP 3108 DAKAR - Sénégal, Bureau 509 du 5ème étage de la Tour**, au plus tard le **mercredi 22 avril 2026 à 12 heures TU**, délai de rigueur. En ce qui concerne les offres transmises par courrier, le cachet de l'expéditeur (Poste, DHL,CHRONOPOST, EMS, etc.) indiqué sur le pli fera foi.

NB : Une copie de l'offre devra également être transmise sous clé USB en version modifiable.

Les plis fermés devront porter le titre **"AO - 054 - 2026 - SÉLECTION D'UN PRESTATAIRE POUR LA FOURNITURE ET LE DÉPLOIEMENT D'UNE PLATEFORME UNIFIÉE DE DÉTECTION, D'ANALYSE ET DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ"**.

I.24. Informations complémentaires

Pour toute demande d'informations complémentaires, les candidats pourront prendre l'attache de la Direction du Budget et des Approvisionnements, par courriel au plus tard dix (10) jours calendaires avant la date limite de dépôt des offres, à l'adresse : courrier.ZDBA-SAMA@bceao.int.

Les demandes de renseignements parvenues au-delà du délai précité ne seront pas prises en compte.

Les questions formulées ainsi que les réponses apportées seront mises en ligne sur le site Internet de la BCEAO à l'adresse www.bceao.int

A ce titre, les candidats sont invités à visiter régulièrement le site internet de la Banque.

I.25. Délai d'exécution

Le délai d'exécution devra être indiqué dans la soumission et commencera à courir à compter de la date de signature du marché.

Ce délai devra être scrupuleusement respecté sous peine d'application d'une pénalité égale à un millième (1‰) du montant de la commande, par jour calendaire de retard.

Toutefois, le montant de ces pénalités ne pourra excéder cinq pour cent (5%) du montant du marché.

I.26. Lieu d'exécution de la prestation

La prestation aura lieu dans les locaux du Siège de la BCEAO sis à l'avenue Abdoulaye FADIGA à Dakar et sur le site de l'Agence Principale de Dakar, pour assurer la haute disponibilité.

I.27. Réception

La réception interviendra en deux (2) temps, selon les modalités suivantes :

- réception provisoire après l'installation de la solution et le constat de son bon fonctionnement ;
- réception définitive, à la fin de la période de garantie, après la levée de toutes les réserves émises et la confirmation, à l'usage, du bon fonctionnement de la solution livrée.

Les réceptions provisoire et définitive feront l'objet de procès-verbaux signés par les deux Parties.

I.28. Modalités de paiement

Les Prestataires proposeront leurs meilleures conditions de paiement en fonction des éléments ci-après :

- l'échéancier devra tenir compte du planning d'exécution des différentes prestations ;
- le versement d'une avance au démarrage après la signature du contrat de marché est soumis à la fourniture d'une lettre de garantie à première demande délivrée par un établissement de crédit reconnu par la BCEAO. La mainlevée de cette garantie sera effectuée par la Banque Centrale, à la date de signature du bordereau de livraison ;
- le règlement des prestations exécutées pour chacune des phases du planning d'exécution ne peut être effectué avant le prononcé de la réception provisoire de la phase concernée ;
- une retenue de garantie égale à 5% du montant du marché est constituée. Elle est libérée à la signature du procès-verbal de réception définitive.

I.29. Propriété des documents et droits d'auteur

Les documents et les livrables du marché fournis par le Prestataire retenu dans le cadre de l'exécution de ses missions resteront la propriété de la Banque.

Les droits d'auteur pour tous les documents préparés par le Prestataire restent sa propriété. Cependant, le Prestataire autorise la Banque, sans préalable, à utiliser ces documents pour la réalisation d'autres prestations similaires ou supplémentaires, sans qu'il puisse prétendre à quelque indemnité que ce soit.

Le Prestataire retenu est censé avoir reçu l'autorisation écrite des détenteurs des procédés brevetés ou protégés, des droits de licences et autres, utilisés par lui dans le cadre du présent marché. La responsabilité de la Banque ne saurait en aucun cas être engagée à l'occasion d'un litige à ce sujet.

DEUXIÈME PARTIE : SPÉCIFICATIONS TECHNIQUES

II.1. Objectifs

Le présent appel d'offres a pour objet la sélection d'un prestataire spécialisé en cybersécurité en vue de la fourniture et du déploiement d'une plateforme intégrée de détection, d'analyse et de réponse aux incidents de cybersécurité de dernière génération, incluant le transfert de compétences au profit des équipes en charge des opérations de cybersécurité.

Cette plateforme vise à remplacer le SOAR et la solution SIEM existante devenue obsolète et à doter la BCEAO d'une infrastructure performante en vue de la collecte centralisée, la corrélation avancée et l'analyse intelligente des événements de sécurité, ainsi que l'orchestration et l'automatisation des réponses aux incidents de cybersécurité.

La solution attendue devra supporter *a minima* les fonctionnalités suivantes :

- SIEM (Security Information and Event Management) pour la collecte, la corrélation et l'analyse des journaux de sécurité ;
- SIEM intégrant des capacités d'analyse avancée basées sur l'intelligence artificielle (AI Analyst) pour l'assistance à l'investigation et la priorisation des alertes ;
- SOAR (Security Orchestration, Automation and Response) pour l'orchestration et l'automatisation des processus de réponse aux incidents ;
- UEBA (User and Entity Behavior Analytics) pour la détection des comportements anormaux et des menaces internes.

Dans le cadre du présent marché, le prestataire retenu devra également assurer :

- la fourniture de toutes les licences nécessaires pour un déploiement en environnement virtuel ;
- l'installation, la configuration et l'intégration de la solution avec les outils de sécurité existants ;
- l'accompagnement à la mise en production ;
- le transfert de compétences au profit des équipes en charge des opérations de cybersécurité ;
- la mise en œuvre d'un programme de formation technique et opérationnelle couvrant l'exploitation des modules SIEM, SOAR et UEBA.

Le programme de formation devra inclure :

- des formations techniques sur la plateforme déployée ;
- des formations avancées en détection et réponse aux incidents, en lien avec les domaines SIEM, analyse des journaux, réponse aux incidents, automatisation SOC et détection des menaces.

II.2. Exigences globales de la solution

La solution devra répondre aux exigences suivantes :

- Supporter **au minimum 15 000 messages par seconde (EPS/MPS)** ;
- Gérer un **nombre illimité de devices / IP / sources de logs** ;
- Ne pas limiter les fonctionnalités en cas de dépassement de licence ;
- Ne pas supprimer ni mettre en buffer les événements lorsque la limite de licence est atteinte ;.
- Fournir au minimum **100 GB de capacité de caching** ;

- Permettre la collecte, le traitement et l'indexation d'une quantité **illimitée de sources de logs** ;
- Fonctionner sans restriction sur le nombre de **collecteurs ou agents** ;
- Fournir **plus de 1000 intégrations natives** ;
- Fournir **plus de 1000 use cases prédéfinis** ;
- Proposer une **vue globale via un dashboard centralisé** ;
- Supporter le **multi-tenancy** ;
- Supporter un **RBAC granulaire** ;
- Permettre un nombre **illimité d'alertes et de recherches** ;
- Corriger automatiquement les **horodatages incorrects** ;
- Fonctionner **entièrement on-premise** sans dépendance cloud.

II.3. Architecture et modules obligatoires

La plateforme devra intégrer les capacités ci-après **nativement et sans interface avec une solution tierce** :

- SIEM
- SIEM AI Analyst
- SOAR
- UEBA
- Registry Monitoring
- Process Monitoring
- Host Forensics
- Network Forensics
- Threat Intelligence
- Network Monitoring
- Network Behavior Analytics
- Security Analytics
- Big Data Analytics Platform
- True Identity

II.4. Exigences relatives à l'architecture technique

La solution devra :

- être **100 % on-premise** ;
- fonctionner sur **serveurs virtuels** ;
- reposer sur une **architecture All-in-One intégrée** ;
- être **évolutive et extensible** ;
- chiffrer toutes les communications internes ;
- supporter **LDAP / Active Directory** ;

- journaliser toutes les actions utilisateurs ;
- permettre la **découverte automatique des hôtes Windows** ;
- continuer la collecte en cas d'interruption réseau ;
- générer des alertes si une source cesse d'envoyer des logs.

II.5. Sécurité d'accès à la plateforme

La plateforme devra intégrer **nativement des mécanismes de sécurité d'accès avancés.** À ce titre, la solution devra :

- supporter **l'authentification forte multi-facteurs (MFA / 2FA)** pour l'accès à l'interface de la plateforme ;
- intégrer **nativement** cette fonctionnalité sans nécessiter de solution tierce ;
- supporter plusieurs méthodes d'authentification forte telles que :
    - OTP (One-Time Password)
    - applications d'authentification (TOTP)
    - token logiciel ou matériel
- permettre l'activation de la **double authentification pour tous les comptes administrateurs et analystes SOC** ;
- permettre l'application de politiques de sécurité différenciées selon les rôles ;
- journaliser toutes les tentatives d'authentification réussies ou échouées ;
- permettre l'intégration avec les mécanismes d'authentification de l'infrastructure existante (SAMBA, OpenLdap, Active Directory / LDAP).

L'authentification multi-facteurs devra être **pleinement intégrée dans la plateforme et administrable via la console centrale**.

II.6. Collecte et normalisation des logs

La solution devra :

- collecter les logs via **canaux chiffrés** ;
- supporter collecte **avec ou sans agent** ;
- supporter les interfaces :Syslog , JSON,
  API, SNMP, XML, Netflow, Jflow, Sflow,
  ODBC, FTP / SFTP, WinRM, Universal DB connection
- permettre la **normalisation des logs non supportés** ;
- permettre la **réduction des logs bruités** ;
- supporter **l'équilibrage de charge des collecteurs**.

II.7. Gestion du stockage et de la rétention

La solution devra :

- stocker **logs bruts et métadonnées** ;
- supporter une rétention minimale :
    - 6 mois online
    - 12 mois archive

- compresser les logs archivés ;
- supporter sauvegarde **NAS / SAN / NFS** ;
- permettre restauration des logs archivés ;
- garantir l'intégrité des logs.

II.8. Corrélation et détection des menaces

La solution devra :

- fournir **1000 règles de corrélation natives minimum** ;
- intégrer **MITRE ATT&CK** ;
- corréler les événements :
    - openLdap
    - SAMBA
    - Active Directory
    - VPN
    - DHCP
    - Firewall
    - Endpoints
- détecter automatiquement les anomalies comportementales ;
- minimiser les faux positifs.

II.9. Module SOAR natif

Le SOAR devra permettre :

- création de **playbooks personnalisés** ;
- automatisation des workflows ;
- gestion des incidents ;
- intégration avec outils **ITSM** ;
- traçabilité complète.

Actions automatisées :

- blocage IP firewall
- désactivation compte AD
- quarantaine machine
- suppression fichier malveillant
- extraction PCAP
- memory dump.

II.10. Module UEBA et Intelligence Artificielle

La solution devra intégrer **un moteur d'IA natif capable de :**

- détecter comportements anormaux ;
- générer scores de risque dynamiques ;

- identifier menaces inconnues ;
- apprendre automatiquement les comportements historiques.

L'UEBA devra :

- être **natif** ;
- supporter **nombre illimité d'utilisateurs**.

II.11. Module SIEM-AI Analyst

La plateforme devra intégrer nativement un module d'analyse assistée par Intelligence Artificielle (SIEM-AI Analyst) destiné à assister les analystes du SOC dans l'analyse et l'investigation des incidents de cybersécurité.

Ce module devra être entièrement intégré à la plateforme SIEM et fonctionner sans dépendance à un service cloud externe.

Le SIEM-AI Analyst devra permettre :

- l'analyse automatisée des alertes générées par le SIEM ;
- la corrélation et la contextualisation des événements liés à un même incident ;
- la reconstruction de la chronologie d'une attaque ;
- l'identification des entités impliquées (utilisateurs, hôtes, processus, adresses IP) ;
- l'attribution d'un score de risque dynamique aux incidents ;
- la priorisation automatique des alertes ;
- la réduction des faux positifs.

Le module devra également :

- fournir des explications et recommandations d'investigation pour les analystes SOC ;
- s'appuyer sur les données issues des modules SIEM, UEBA, Threat Intelligence et Forensics ;
- permettre la visualisation des relations entre événements et entités.

La solution devra être capable d'améliorer progressivement la précision de ses analyses grâce à l'apprentissage des comportements et aux retours des analystes SOC.

II.12. Interface et visualisation

La solution devra offrir :

- dashboards temps réel HTML5 ;
- visualisation graphique des relations entre événements ;
- timeline d'attaque ;
- export PDF / CSV ;
- interface unique.

II.13. Exigences relatives à la formation

Le soumissionnaire devra assurer :

- formation administrateur plateforme
- formation analyste SOC

- formation investigation SIEM
- formation création playbooks SOAR
- formation exploitation UEBA

Le programme devra inclure des formations certifiantes reconnues internationalement (SANS/GIAC ou équivalent).

II.14. Clauses techniques spécifiques

- **Clause anti-faux SIEM**

La solution devra être une **plateforme SIEM native développée par un éditeur reconnu** et ne devra pas être constituée d'un assemblage d'outils hétérogènes ou open source.

La plateforme devra fonctionner avec **une console unique et un moteur de corrélation unique**.

- **Clause anti-SIEM basé sur ELK / Open Source**

Ne seront pas acceptées les solutions reposant principalement sur :

  - ELK
  - OpenSearch
  - assemblages open source nécessitant développement spécifique.

La plateforme devra disposer d'un **moteur natif Big Data et corrélation intégré**.

- **Clause relative à l'Intelligence Artificielle**

La plateforme devra intégrer un **véritable moteur d'apprentissage automatique (Machine Learning)**.

Les solutions reposant uniquement sur des règles statiques, des corrélations définies pra défaut et des outils basiques d'analyse statistique ne seront pas retenues.

II.15. Exigences relatives au soumissionnaire

Le soumissionnaire devra :

- être éditeur ou partenaire certifié ;
- mettre à disposition des consultants certifiés ;
- proposer un Project Manager dédié ;
- justifier projets similaires ;
- assurer support éditeur minimum 36 mois.

II.16. Livrables attendus

Le prestataire devra fournir :

- architecture détaillée
- plan de déploiement
- plan de migration SIEM
- documentation d'administration
- documentation d'exploitation
- playbooks SOAR

- catalogue use cases SOC
- rapport de formation
- rapport de transfert de compétences.

II.17. Support et maintenance

Le prestataire devra assurer :

- support technique 24/7
- maintenance corrective
- maintenance évolutive
- mises à jour sécurité
- assistance technique.

Durée minimale : **36 mois**

II.18. Intégration avec les solutions de sécurité existantes et mise en œuvre opérationnelle du SOC

Le prestataire devra réaliser l'intégration complète de la plateforme avec l'écosystème de sécurité existant de la Banque, ainsi que la configuration des mécanismes nécessaires au fonctionnement opérationnel du SOC.

Intégration avec les solutions existantes

La solution devra être intégrée avec les outils de sécurité déjà déployés au sein de l'infrastructure de la Banque, notamment :

- solutions **XDR / NDR ;**
- scanners de vulnérabilités ;
- solutions **PAM (Privileged Access Management) ;**
- pare-feux et systèmes IDS / IPS ;
- solutions de sécurité des endpoints;
- systèmes d'authentification et annuaires (SAMBA, Active Directory / LDAP) ;
- solutions de messagerie ;
- systèmes ITSM ;
- plateformes Cyber Range ;
- solution FIM existante.

Le prestataire devra :

- configurer les **connecteurs nécessaires** ;
- assurer la **collecte des journaux de ces solutions** ;
- normaliser les événements collectés.

Mise en œuvre des cas d'usage SOC

Le prestataire devra :

- adapter les **règles de corrélation natives** à l'environnement de la Banque ;
- configurer les **cas d'usage SOC** ;
- aligner les cas d'usage avec la matrice **MITRE ATT&CK**.

Les cas d’usage devront couvrir notamment :

- compromission de comptes
- mouvements latéraux
- attaques sur SAMBA, OpenLdap, Active Directory
- exécution de malware
- exfiltration de données
- abus de privilèges
- activités anormales sur les endpoints
- anomalies réseau.

Mise en œuvre des playbooks SOAR

Le prestataire devra configurer les **playbooks SOAR nécessaires à l’automatisation de la réponse aux incidents**.

Ces playbooks devront permettre notamment :

- blocage automatique d’adresses IP malveillantes ;
- désactivation de comptes compromis ;
- mise en quarantaine de machines ;
- extraction d’artefacts d’investigation ;
- ouverture automatique d’incidents dans l’outil ITSM ;
- escalade vers les analystes SOC.

Les playbooks devront être **documentés et personnalisables par les équipes du SOC**.

Mise en place des tableaux de bord SOC

Le prestataire devra configurer les **tableaux de bord (Dashboards) nécessaires à la supervision opérationnelle de la cybersécurité**.

Ces tableaux de bord devront être adaptés aux différents niveaux d’utilisation, notamment :

Tableaux de bord SOC opérationnels

- incidents de sécurité actifs
- alertes critiques
- événements de sécurité par type
- activités suspectes utilisateurs
- activités suspectes réseau
- menaces détectées.

Tableaux de bord d’investigation

- chronologie des attaques
- entités impliquées (utilisateurs, machines, IP)
- corrélation des événements.

Tableaux de bord de pilotage

- nombre d’alertes détectées
- incidents traités
- MTTD (Mean Time To Detect)
- MTTR (Mean Time To Respond)
- taux de faux positifs.

Les tableaux de bord devront être :

- **personnalisables** ;
- accessibles via l’interface centrale de la plateforme ;
- exportables sous forme de **rapports sous format PDF , Microsoft office (ou équivalent)**.

Mise en production opérationnelle

Le prestataire devra assurer :

- la mise en service complète de la plateforme ;
- la validation des cas d’usage SOC ;
- la validation des playbooks SOAR ;
- la validation des tableaux de bord ;
- la réalisation de tests de détection et de réponse aux incidents.

TROISIÈME PARTIE : ANNEXES

Annexe 1 : Lettre de soumission (à reprendre sur papier en-tête du soumissionnaire)

(indiquer le lieu et la date)

A l' attention de :

MONSIEUR LE DIRECTEUR DU BUDGET ET DES APPROVISIONNEMENTS

BP 3108 DAKAR - BCEAO/SIEGE

Objet : Sélection d'un prestataire pour la fourniture et le déploiement d'une plateforme unifiée de détection, d'analyse et de réponse aux incidents de cybersécurité

Nous, soussignés..., soumettons par la présente, une offre de prix pour *[Indiquer l'objet de l'appel d'offres]*, pour un montant de……...........FCFA HT/HD ou................. euros.

La durée de validité de notre soumission est de cent vingt (120) jours au moins pour compter du *[indiquer la date limite de dépôt des offres].*

Nous déclarons, par la présente, que toutes les informations et affirmations faites ci-dessous dans le cadre de cet appel offres sont authentiques et acceptons que toute déclaration erronée puisse conduire à notre disqualification :

1. Nous avons lu et compris les dispositions du présent dossier d'appel d'offres, et nous acceptons d'être liés par celles-ci.
2. Nous proposons de réaliser l'objet de cet appel d'offres dans les taux et prix indiqués dans l'offre financière incluse dans notre soumission.
3. Comme le prévoit le dossier d'appel d'offres, les prix mentionnés resteront fermes pendant la durée du contrat.
4. Nous n'avons aucun conflit d'intérêts pouvant remettre en cause notre participation au processus d'acquisition et à l'attribution du contrat.
5. Nous n'avons pas été déclarées inéligibles par la Banque Centrale.

Nous prenons l'engagement de respecter scrupuleusement les lois en vigueur dans notre pays d'enregistrement et le pays dans lequel le contrat est exécuté.

Nous comprenons que vous n'êtes nullement tenus à l'obligation d'accepter la proposition la moins disante, ni l'une quelconque des propositions que vous recevez.

Notre proposition engage notre responsabilité et, sous réserve des modifications résultant d'éventuelles négociations du marché, nous nous engageons, si elle est retenue, à commencer la prestation au plus tard à la date convenue lors des négociations.

Nous confirmons que le soussigné est autorisé à engager le(s) soumissionnaire(s) à respecter les obligations contenues dans le dossier d'appel d'offres et le contrat.

Signature du représentant habilité :

Nom et titre du signataire :

Nom de l'entreprise ou du groupement :

<u>ANNEXE 2</u> : Fiche d'Information du Soumissionnaire *(à reprendre sur en-tête du soumissionnaire dans le dossier de présentation)*

<table>
<tr><th>Description</th><th colspan="3">Détail</th></tr>
<tr><td>Nom légal du soumissionnaire</td><td colspan="3">En cas de groupement , préciser toutes les sociétés</td></tr>
<tr><td>Forme juridique</td><td colspan="3"></td></tr>
<tr><td>Année de création / début exercice</td><td colspan="3"></td></tr>
<tr><td>Nature d'activités</td><td colspan="3"></td></tr>
<tr><td>Adresse juridique, Ville, Pays</td><td colspan="3"></td></tr>
<tr><td>Informations Bancaires (RIB)</td><td colspan="3"></td></tr>
<tr><td colspan="4">Données Administratives</td></tr>
<tr><td>Noms</td><td>Numéro</td><td>Date de délivrance / validité</td><td>L'Autorité Signataire</td></tr>
<tr><td>Régistre de commerce</td><td></td><td></td><td></td></tr>
<tr><td>Capital social</td><td></td><td></td><td></td></tr>
<tr><td>Quitus Fiscal</td><td></td><td></td><td></td></tr>
<tr><td>Attestation de régularité sociale</td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Données Financières des trois dernières années</td></tr>
<tr><td></td><td>Année N-1</td><td>Année N-2</td><td>Année N-3</td></tr>
<tr><td>Bilan</td><td></td><td></td><td></td></tr>
<tr><td>Capitaux propres</td><td></td><td></td><td></td></tr>
<tr><td>Chiffre d'affaires</td><td></td><td></td><td></td></tr>
<tr><td>Résultats nets</td><td></td><td></td><td></td></tr>
<tr><td>Capacité d'autofinancement</td><td></td><td></td><td></td></tr>
</table>

Références similaires				
Objet du marché	**Références client**	**Valeur contrat**	**Période**	**Détail du marché**

Signature du représentant habilité : __

Nom et titre du signataire : ___

Nom de l'entreprise ou du groupement : _____

<u>ANNEXE 3 :</u> TABLEAU D'ÉVALUATION DES OFFRES TECHNIQUES

Ce tableau est à renseigner par le soumissionnaire.

N°	Exigences	Conformité	Justificatifs et commentaires
Exigences relatives au soumissionnaire			
1	Etre éditeur ou partenaire certifié ;		
2	Mettre à disposition des consultants certifiés ;		
3	Proposer un Project Manager dédié ;		
4	Justifier projets similaires ;		
5	Assurer support éditeur minimum 36 mois.		
Exigences d'ordre général de la solution			
6	Supporter au minimum 15 000 messages par seconde (EPS/MPS)		
7	Gérer un nombre illimité de devices / IP / sources de logs		
8	Ne pas limiter les fonctionnalités en cas de dépassement de licence		
9	Ne pas supprimer ni mettre en buffer les événements lorsque la limite de licence est atteinte		
10	Fournir au minimum 100 GB de capacité de caching		
11	Permettre la collecte, le traitement et l'indexation d'une quantité illimitée de sources de logs		
12	Fonctionner sans restriction sur le nombre de collecteurs ou agents		
13	Fournir plus de 1000 intégrations natives		
14	Fournir plus de 1000 use cases prédéfinis		
15	Proposer une vue globale via un dashboard centralisé		
16	Supporter le multi-tenancy		
17	Supporter un RBAC granulaire		
18	Permettre un nombre illimité d'alertes et de recherches		
19	Corriger automatiquement les horodatages incorrects		
20	Fonctionner entièrement on-premise sans dépendance cloud		
Architecture et modules obligatoires			
21	SIEM		
22	SIEM AI Analyst		

23	SOAR		
24	UEBA		
25	Registry Monitoring		
26	Process Monitoring		
27	Host Forensics		
28	Network Forensics		
29	Threat Intelligence		
30	Network Monitoring		
31	Network Behavior Analytics		
32	Security Analytics		
33	Big Data Analytics Platform		
34	True Identity		
Exigences relatives à l'architecture technique			
35	Etre 100 % on-premise		
36	Fonctionner sur serveurs virtuels		
37	Reposer sur une architecture All-in-One intégrée		
38	Etre évolutive et extensible		
39	Chiffrer toutes les communications internes		
40	Supporter LDAP / Active Directory		
41	Journaliser toutes les actions utilisateurs		
42	Permettre la découverte automatique des hôtes Windows		
43	Continuer la collecte en cas d'interruption réseau		
44	Générer des alertes si une source cesse d'envoyer des logs		
Sécurité d'accès à la plateforme			
45	Supporter l'authentification forte multi-facteurs (MFA / 2FA) pour l'accès à l'interface de la plateforme		
46	Intégrer nativement cette fonctionnalité sans nécessiter de solution tierce		
47	Supporter plusieurs méthodes d'authentification forte telles que : - OTP (One-Time Password), - applications d'authentification (TOTP), - token logiciel ou matériel ;		
48	Permettre l'activation de la double authentification pour tous les comptes administrateurs et analystes SOC		

49	Permettre l'application de politiques de sécurité différenciées selon les rôles		
50	Journaliser toutes les tentatives d'authentification réussies ou échouées		
51	Permettre l'intégration avec les mécanismes d'authentification de l'infrastructure existante (SAMBA, OpenLdap, Active Directory / LDAP)		
52	Intégrer l'authentification multi-facteurs administrable via la console centrale.		
Collecte et normalisation des logs			
53	Collecter les logs via canaux chiffrés ;		
54	Supporter collecte avec ou sans agent ;		
55	Supporter les interfaces : Syslog , JSON, API, SNMP, XML, Netflow, Jflow, Sflow, ODBC, FTP / SFTP, WinRM, Universal DB connection		
56	Permettre la normalisation des logs non supportés ;		
57	Permettre la réduction des logs bruités ;		
58	Supporter l'équilibrage de charge des collecteurs.		
Gestion du stockage et de la rétention			
59	Stocker logs bruts et métadonnées ;		
60	Supporter une rétention minimale : - 6 mois online - 12 mois archive		
61	Compresser les logs archivés ;		
62	Supporter sauvegarde NAS / SAN / NFS ;		
63	Permettre restauration des logs archivés ;		
64	Garantir l'intégrité des logs.		
Corrélation et détection des menaces			
65	Fournir 1000 règles de corrélation natives minimum		
66	Intégrer MITRE ATT&CK		
67	Corréler les événements : - openLdap - SAMBA - Active Directory - VPN - Firewall - Endpoints		
68	Détecter automatiquement les anomalies comportementales ;		

69	Minimiser les faux positifs.		
Module SOAR natif			
70	Création de playbooks personnalisés ;		
71	Automatisation des workflows ;		
72	Gestion des incidents ;		
73	Intégration avec outils ITSM ;		
74	Traçabilité complète.		
75	Blocage IP firewall		
76	Désactivation compte AD		
77	Quarantaine machine		
78	Suppression fichier malveillant		
79	Extraction PCAP		
80	Memory dump.		
Module UEBA et Intelligence Artificielle			
	un moteur d'IA natif capable de :		
81	Détecter comportements anormaux ;		
82	Générer scores de risque dynamiques ;		
83	Identifier menaces inconnues ;		
84	Apprendre automatiquement les comportements historiques.		
	L'UEBA devra		
85	Etre natif ;		
86	Supporter nombre illimité d'utilisateurs.		
Module SIEM-AI Analyst			
87	Analyse automatisée des alertes générées par le SIEM ;		
88	Corrélation et la contextualisation des événements liés à un même incident ;		
89	Reconstruction de la chronologie d'une attaque ;		
90	Identification des entités impliquées (utilisateurs, hôtes, processus, adresses IP) ;		
91	Attribution d'un score de risque dynamique aux incidents ;		
92	Priorisation automatique des alertes ;		
93	Réduction des faux positifs.		
94	Fournir des explications et recommandations d'investigation pour les analystes SOC ;		

95	S'appuyer sur les données issues des modules SIEM, UEBA, Threat Intelligence et Forensics ;		
96	Permettre la visualisation des relations entre événements et entités.		
Interface et visualisation			
97	Dashboards temps réel HTML5 ;		
98	Visualisation graphique des relations entre événements ;		
99	Timeline d'attaque ;		
100	Export PDF / CSV ;		
101	Interface unique.		
Exigences relatives à la formation			
102	Formation administrateur plateforme		
103	Formation analyste SOC		
104	Formation investigation SIEM		
105	Formation création playbooks SOAR		
106	Formation exploitation UEBA		
107	Programme devra inclure des formations certifiantes reconnues internationalement (SANS/GIAC ou équivalent).		
Clauses techniques spécifiques			
108	Clause anti-faux SIEM		
109	Clause anti-SIEM basé sur ELK / Open Source		
110	Clause relative à l'Intelligence Artificielle		
Livrables attendus			
111	Architecture détaillée		
112	Plan de déploiement		
113	Plan de migration SIEM		
114	Documentation d'administration		
115	Documentation d'exploitation		
116	Playbooks SOAR		
117	Catalogue use cases SOC		
118	Rapport de formation		
119	Rapport de transfert de compétences.		
Support et maintenance			
120	Support technique 24/7		

121	Maintenance corrective		
122	Maintenance évolutive		
123	Mises à jour sécurité		
124	Assistance technique.		
Intégration avec les solutions de sécurité existantes et mise en œuvre opérationnelle du SOC			
	Intégration avec les solutions existantes		
125	Solutions XDR / NDR ;		
126	Scanners de vulnérabilités ;		
127	Solutions PAM (Privileged Access Management) ;		
128	Pare-feux et systèmes IDS / IPS ;		
129	Solutions de sécurité des endpoints;		
130	Systèmes d'authentification et annuaires (SAMBA, Active Directory / LDAP) ;		
131	Solutions de messagerie ;		
132	Systèmes ITSM ;		
133	Plateformes Cyber Range ;		
134	Solution FIM existante.		
	Mise en œuvre des cas d'usage SOC		
135	Adapter les règles de corrélation natives à l'environnement de la Banque ;		
136	Configurer les cas d'usage SOC ;		
137	Aligner les cas d'usage avec la matrice MITRE ATT&CK.		
	Mise en œuvre des playbooks SOAR		
138	Blocage automatique d'adresses IP malveillantes ;		
139	Désactivation de comptes compromis ;		
140	Mise en quarantaine de machines ;		
141	Extraction d'artefacts d'investigation ;		
142	Ouverture automatique d'incidents dans l'outil ITSM ;		
143	Escalade vers les analystes SOC.		
Mise en place des tableaux de bord SOC			
	Tableaux de bord SOC opérationnels		
144	Incidents de sécurité actifs		
145	Alertes critiques		

146	Evénements de sécurité par type		
147	Activités suspectes utilisateurs		
148	Activités suspectes réseau		
149	Menaces détectées.		
	Tableaux de bord d’investigation		
150	Chronologie des attaques		
151	Entités impliquées (utilisateurs, machines, IP)		
152	Corrélation des événements.		
	Tableaux de bord de pilotage		
153	Nombre d’alertes détectées		
154	Incidents traités		
155	MTTD (Mean Time To Detect)		
156	MTTR (Mean Time To Respond)		
157	Taux de faux positifs		
Mise en production opérationnelle			
158	Mise en service complète de la plateforme		
159	Validation des cas d’usage SOC		
160	Validation des playbooks SOAR		
161	Validation des tableaux de bord		
162	Réalisation de tests de détection et de réponse aux incidents		