تمويلكم
ⵜⴰⵎⵡⵉⵍⴽⵓⵎ
TAMWILCOM

APPEL D'OFFRES OUVERT INTERNATIONAL SUR OFFRES DE PRIX N°13/2025/SNGFE

RELATIF A

L'ACQUISITION ET RENOUVELLEMENT D'UN SIEM AINSI QUE LA MISE EN PLACE D'UN SOC AS A SERVICE POUR LE COMPTE DE LA SOCIETE NATIONALE DE GARANTIE ET DU FINANCEMENT DE L'ENTREPRISE

Règlement De Consultation

En application de l'article 8, de l'alinéa 3 paragraphe I-1 et l'alinéa a) paragraphe 3 de l'article 19 et de l'alinéa b) du paragraphe 3 de l'article 20 du Règlement des Achats de la SNGFE.

Décembre 2025

NB : Le Règlement des Achats de la Société Nationale de Garantie et du Financement de l'Entreprise est téléchargeable sur le site : www.tamwilcom.ma

SOMMAIRE

Article 1 : Objet du règlement de consultation

Le présent règlement de consultation concerne l'appel d'offres ouvert international sur offres de prix n°13/2025/SNGFE ayant pour objet l'acquisition et le renouvellement d'un SIEM ainsi que la mise en place d'un SOC as a Service pour le compte de la Société Nationale de Garantie et du Financement de l'Entreprise (SNGFE).

Il a été établi en vertu des dispositions de l'article 21 du Règlement des Achats de la SNGFE.

Les prescriptions du présent règlement de consultation ne peuvent en aucune manière déroger ou modifier les conditions et les formes prévues par le Règlement des Achats de la SNGFE. Toute disposition contraire au Règlement précité est nulle et non avenue.

Seules, sont valables les précisions et prescriptions complémentaires conformes aux dispositions de l'article 21 et des autres articles du Règlement précité.

Article 2 : Maître d'Ouvrage

Le Maître d'Ouvrage du marché qui sera passé suite au présent appel d'offres est le Directeur Général Adjoint – Ressources de la SNGFE.

Article 3 : Répartition en lots

Le présent appel d'offres concerne un marché en lot unique.

Article 4 : Contenu du dossier d'appel d'offres

Conformément aux dispositions de l'article 22 du Règlement des Achats de la SNGFE, le dossier d'appel d'offres comprend :

a. Copie de l'avis d'appel d'offres ;
b. Un exemplaire du cahier des prescriptions spéciales ;
c. Le modèle de l'acte d'engagement ;
d. Le modèle du bordereau des prix ;
e. Le modèle de la déclaration sur l'honneur ;
f. Le présent règlement de consultation.

Article 5 : Modification du contenu du dossier d'appel d'offres

Lorsque le Maître d'Ouvrage introduit des modifications dans le dossier d'appel d'offres, conformément aux dispositions du paragraphe 7 de l'article 22 du Règlement des Achats de la SNGFE, elles seront communiquées à tous les concurrents ayant retiré ou téléchargé ledit dossier et publiées sur le portail des marchés publics.

Les modifications introduites dans le dossier d'appel d'offres ne peuvent en aucun cas changer l'objet du marché.

Article 6 : Retrait du dossier d'appel d'offres

Le dossier d'appel d'offres est mis gratuitement à la disposition des concurrents dans le bureau indiqué dans l'avis d'appel d'offres dès la parution de ce dernier au premier journal et jusqu'à la date limite de remise des offres.

Le dossier d'appel d'offres peut être téléchargé sur le portail des marchés de l'Etat (www.marchespublics.gov.ma) ainsi que sur le site de la SNGFE (www.tamwilcom.ma).

Article 7 : Informations des concurrents et éclaircissements

Tout concurrent peut demander au maître d'ouvrage, par lettre transmise par tout moyen pouvant donner date certaine, de lui fournir des éclaircissements ou renseignements concernant l'appel d'offres ou les documents y afférents. Cette demande doit être adressée au :

Département Logistique et Achats
Sis à : Centre d'Affaires, bd. Ar Ryad, Hay Ryad – Rabat BP 2031 – Maroc.
Téléphone : 05 37 71 68 68
E-mail : c.doulimi@tamwilcom.ma.

Ladite demande n'est recevable que si elle parvient au maître d'ouvrage au moins **sept (7) jours** avant la date prévue pour la séance d'ouverture des plis.

Le maître d'ouvrage doit répondre, dans les mêmes formes, à toute demande d'information ou d'éclaircissement reçue, au plus tard **trois (3) jours** avant la date prévue pour la séance d'ouverture des plis.

Tout éclaircissement ou renseignement fourni par le maître d'ouvrage à un concurrent à la demande de ce dernier doit être communiqué, le même jour et dans les mêmes formes, aux autres concurrents ayant retiré ou téléchargé le dossier d'appel d'offres et aux membres de la commission d'appel d'offres.

Cet éclaircissement ou renseignement est mis à la disposition de tout concurrent potentiel dans le portail des marchés publics.

Article 8 : Conditions requises des concurrents

Conformément aux dispositions de l'article 27 du Règlement des Achats de la SNGFE :

1 - Seules peuvent participer au présent appel d'offres les personnes physiques ou morales qui :

- Justifient des capacités juridiques, techniques et financières requises ;
- Sont en situation fiscale régulière, pour avoir souscrit leurs déclarations et réglé les sommes exigibles ou, à défaut de règlement, constitué des garanties jugées suffisantes par le comptable chargé du recouvrement, et ce conformément à la législation en vigueur en matière de recouvrement des créances publiques ;
- Sont affiliées à la Caisse nationale de sécurité sociale ou à un autre régime particulier de prévoyance sociale, et souscrivent de manière régulière leurs déclarations de salaires et sont en situation régulière auprès de ces organismes ;
- Exercent l'une des activités en rapport avec l'objet du marché.

2 - Ne sont pas admis à participer au présent appel d'offres :

- Les personnes en liquidation judiciaire ;
- Les personnes en redressement judiciaire, sauf autorisation spéciale délivrée par l'autorité judiciaire compétente ;
- Les personnes ayant fait l'objet d'une décision d'exclusion temporaire ou définitive prise conformément aux dispositions de l'article 152 du présent règlement ;
- Les personnes qui représentent plus d'un concurrent dans un même marché;
- Les prestataires de services ayant contribué à la préparation du dossier de l'appel d'offres concerné ;
- Les titulaires dont les marchés ont fait l'objet de résiliation pour une faute qui leur incombe au titre des marchés d'achèvement y afférents.

Article 9 : Contenu du dossier de l'offre du concurrent

Chaque concurrent doit présenter un dossier administratif, un dossier technique, une offre technique ainsi qu'une offre financière. Chaque dossier doit être accompagné d'un état des pièces qui le constituent.

A – Un dossier administratif comprenant :

1 - Pour chaque concurrent, au moment de la présentation des offres :

a) la ou les pièces justifiant les pouvoirs conférés à la personne agissant au nom du concurrent. Ces pièces varient selon la forme juridique du concurrent :

- s'il s'agit d'un auto-entrepreneur ou d'une personne physique agissant pour son propre compte, aucune pièce n'est exigée ;

- s'il s'agit d'un représentant du concurrent, celui-ci doit présenter, selon le cas :

  - une copie certifiée conforme de la procuration légalisée, lorsqu'il agit au nom d'une personne physique ;
  - un extrait des statuts de la société et/ou copie certifiée conforme à l'original du procès-verbal de l'organe compétent lui conférant le pouvoir d'agir au nom de cette société ;
  - l'acte par lequel la personne habilitée délègue son pouvoir à une tierce personne, le cas échéant.

- s'il s'agit d'une coopérative ou d'une union de coopératives, la ou les pièces justifiant les pouvoirs conférés à la personne agissant au nom de la coopérative ou de l'union de coopératives.

b) la déclaration sur l'honneur ;

c) un cautionnement provisoire électronique instruit auprès de l'organisme bancaire ou de l'organisme agréé et ce, via le Portail Marocain des Marchés Publics. Ce cautionnement provisoire est fixé à **20.000,00 DHS (Vingt mille Dirhams)**

d) Pour les groupements : en plus des pièces mentionnées aux alinéas a) b) et c) ci-dessus, la convention constitutive du groupement prévue à l'article 150 du Règlement des Achats de la SNGFE ou sa copie certifiée conforme.

e) Lorsque le concurrent est un établissement public : en plus des pièces mentionnées aux alinéas a) b) et c) ci-dessus, une copie du texte l'habilitant à exercer les missions en relation avec les prestations objet du marché ;

f) Lorsque le concurrent est une coopérative ou une union de coopératives : en plus des pièces mentionnées aux alinéas a) b) et c) ci-dessus, l'attestation d'immatriculation au registre local des coopératives ;

g) Lorsque le concurrent est un auto-entrepreneur : en plus des pièces mentionnées aux alinéas a) b) et c) ci-dessus, l'attestation d'immatriculation au registre national de l'auto-entrepreneur ou sa copie certifiée conforme à l'original, délivrée depuis moins d'un an.

2 - Pour le concurrent auquel il est envisagé d'attribuer le marché :

2-1 Lorsque le concurrent est une société ou une personne physique :

a) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant que le concurrent est en situation fiscale

régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu à l'article 8 ci-dessus. Cette attestation doit mentionner l'activité au titre de laquelle le concurrent est imposé.

b) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale ou par tout autre organisme de prévoyance sociale certifiant que le concurrent est en situation régulière envers l'organisme concerné ;
c) Une copie du certificat d'immatriculation au registre de commerce (modèle 9) pour les personnes assujetties à l'obligation d'immatriculation au registre de commerce en vertu de la législation en vigueur ;
d) Des copies certifiées conformes à l'original des attestations ou autorisations requises pour l'exécution des prestations objet du marché conformément à la législation et la réglementation en vigueur, le cas échéant ;

2-2 Lorsque le concurrent est un établissement public :

a) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant qu'il est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu par l'article 8 ci-dessus. Cette attestation doit mentionner l'activité au titre de laquelle le concurrent est imposé. L'attestation précitée n'est exigée que des établissements publics soumis à l'impôt.
b) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale ou tout autre organisme de prévoyance sociale certifiant que le concurrent est en situation régulière envers l'organisme concerné.

La date de production, au maître d'ouvrage, des pièces prévues aux a) et b) ci-dessus sert de base pour l'appréciation de leur validité.

2-3 Lorsque le concurrent est une coopérative ou une union de coopératives :

a) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu à l'article 8 ci-dessus. Cette attestation doit mentionner l'activité au titre de laquelle la coopérative ou l'union de coopératives est imposée ;
b) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale certifiant que la coopérative ou l'union de coopératives est en situation régulière envers cet organisme conformément aux dispositions de l'article 8 ci-dessus.

La date de production, au maître d'ouvrage, des pièces prévues aux a) et b) ci-dessus, sert de base pour l'appréciation de leur validité.

2-4 Lorsque le concurrent est un auto-entrepreneur, il doit fournir :

Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu à l'article 8 ci-dessus. Cette attestation doit mentionner l'activité au titre de laquelle l'auto-entrepreneur est imposé.

La date de production, au maître d'ouvrage, de cette pièce sert de base pour l'appréciation de sa validité.

B – Un dossier technique comprenant :

a) Une note indiquant les moyens humains et techniques du concurrent et mentionnant, le cas échéant, le lieu, la date, la nature et l'importance des prestations qu'il a exécutées ou à l'exécution desquelles il a participé, avec précision de la qualité de sa participation ;
b) Les attestations ou leurs copies certifiées conformes à l'original délivrées par les maîtres d'ouvrage, publics ou privés, ou par les hommes de l'art sous la direction desquels le concurrent a exécuté ces prestations ou par les titulaires de marchés au titre des prestations sous-traitées. Chaque attestation précise, notamment, la nature des prestations, leur montant et l'année de réalisation, le nom et la qualité du signataire et son appréciation ;

Seuls seront admis, les concurrents qui présentent au moins trois (03) attestations de références relatives à des prestations de même nature que l'objet (SIEM/SOC) du présent appel d'offres durant les 5 (cinq) dernières années (2020-2024) pour des comptes au Maroc et dont le montant minimum annuel pour chaque attestation de références est de Neuf cent mille dirhams Toutes Taxes comprises (900.000,00 DH TTC) ;

c) Les attestations du chiffre d'affaires des deux dernières années.
d) Une attestation de certification du SOC marocain ISO 27001 ;
e) Une attestation de certification du SOC marocain ISO 9001 ;
f) Le prestataire doit être qualifié PASSI par la DGSSI ;
g) La déclaration du plan de charge du concurrent prévu à **l'annexe 4** du présent règlement de consultation ;

C – Une offre technique

Les concurrents doivent présenter une offre technique faisant ressortir leur capacité à réaliser les prestations demandées. A cet effet, ils doivent fournir les documents suivants :

1. Une note présentant la composition de l'équipe d'intervention **(Note N° 1).**
   Le candidat doit préciser l'équipe d'encadrement qui sera affectée à la réalisation des prestations ainsi que les tâches qui seront assignées à chaque membre de l'équipe.
   Cette équipe sera évaluée en fonction de la qualification de ses membres et particulièrement de leurs expériences dans la réalisation de prestations similaires.
   Le candidat doit joindre les CV, suivant le modèle en **annexe 5**, des membres de l'équipe d'encadrement susvisés dûment signés par le chef de l'entreprise et par les intéressés.
   Il devra également joindre les copies certifiées conformes des diplômes ainsi que des certificats en cours de validité avec le code de vérification clairement visible.
   L'équipe type doit comprendre au minimum : **un chef de projet, un expert en intégration SIEM, Un expert en organisation du SOC, six (6) analystes N1, deux (02) analystes N2 et un (01) analyste N3.**
2. Une note descriptive sur la solution SIEM proposée (Note **N° 2)** comprenant une fiche de présentation, basée sur le descriptif du CPS ainsi que le tableau de conformité en **annexes 6** rempli. Chaque spécification proposée doit être accompagnée par des éléments justificatifs marqués et bien indexés (Prospectus, notices, documents techniques…) ;

3. Une note présentant la démarche de conduite proposée pour assurer la réalisation du projet. Elle doit être détaillée au maximum afin de permettre d'apprécier sa qualité **(Note N° 3)**.

D - Une offre financière comprenant :

1. Un acte d'engagement établi conformément au modèle, ci-joint, en Annexe 2 ;
2. Le bordereau des prix établis conformément au modèles joint au CPS.

Le montant total de l'acte d'engagement doit être libellé en chiffres et en toutes lettres.

E- Le cahier des prescriptions spéciales et le règlement de consultation :

Paraphés et signés et portant la mention « lu et accepté » par le concurrent ou son représentant dûment habilité.

Article 10 : Présentation des dossiers des offres des concurrents

1 - Pour chaque concurrent au moment de la présentation des offres :

Le dossier présenté par chaque concurrent est mis dans une enveloppe électronique portant les mentions de l'appel d'offres.

Cette enveloppe contient trois (03) sous dossiers :

a. **Le premier sous-dossier** : outre les pièces des dossiers administratif et technique, le cahier des prescriptions spéciales et le règlement de consultation paraphés et signés et portant la mention « lu et accepté » par le concurrent ou son représentant dûment habilité. Il doit porter la mention « Dossiers administratif et technique » ;
b. **Le deuxième sous-dossier :** contient l'offre financière du soumissionnaire. Il doit porter, la mention « offre financière » ;
c. **Le troisième sous-dossier :** contient l'offre technique du soumissionnaire. Il doit porter, la mention « offre technique ».

Les concurrents doivent transmettre leurs dossiers par voie électronique eu Maître d'Ouvrage, selon les dispositions des articles 12, 13 et 14 de l'arrêté du Ministre Délégué auprès du Ministre de l'Economie et des Finances, chargé du Budget n° 1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics.

2 - Pour le concurrent auquel il est envisagé d'attribuer le marché dans les conditions fixées à l'article 43 du Règlement des Achats de la SNGFE :

Le complément de dossier et les éléments de réponse du concurrent doivent être produits dans un dossier électronique. Ce pli doit être produit conformément aux dispositions de l'article 18 de l'arrêté Ministre Délégué auprès du Ministre de l'Economie et des Finances, chargé du Budget n° 1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics

Article 11 : Dépôt des plis des concurrents

Conformément aux dispositions de l'arrêté du Ministre Délégué auprès du Ministre de l'Economie et des Finances, chargé du Budget n° 1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics, les plis doivent être déposés par voie électronique au niveau du Portail Marocain des Marchés Publics ainsi que le cautionnement provisoire dématérialisé exigé des soumissionnaires.

NB : Chacune des pièces constituant la réponse du concurrent, est insérée, individuellement, dans l'enveloppe électronique la concernant.

Conformément aux conditions d'utilisation du portail des marchés publics, chaque pièce est signée, électroniquement, par le concurrent ou la personne dûment habilitée à le représenter, à l'exception des pièces dématérialisées.

Toute offre ne respectant pas la procédure de soumission électronique sera rejetée.

Article 12 : Retrait des plis

Le retrait des plis s'effectue également par voie électronique conformément aux dispositions de l'arrêté du Ministre Délégué auprès du Ministre de l'Economie et des Finances, chargé du Budget n° 1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics.

Les concurrents ayant retirés leurs plis peuvent présenter de nouveaux plis dans les conditions prévues par l'article 14 de l'arrêté du Ministre Délégué auprès du Ministre de l'Economie et des Finances, chargé du Budget n° 1692-23 du 4 hija 1444 (23 juin 2023) précité et avant la date limite de remise des plis.

Article 13 : Ouverture et examen des offres des concurrents

La séance d'ouverture des plis se tiendra aux bureaux du siège de la Société Nationale de Garantie et du Financement de l'Entreprise sis au : **Centre d'Affaires, Boulevard Ar-Ryad, Hay Ryad – Rabat le jeudi 08 janvier 2026 à 10 heures.**

L'ouverture et l'examen des offres s'effectuent conformément aux dispositions prévues aux articles 39, 41, 42 et 43 du Règlement des Achats de la SNGFE.

Article 14 : Critères d'appréciation des capacités techniques et financières des concurrents

Au vu des éléments contenus dans les dossiers administratif et technique, la commission d'appel d'offres apprécie les capacités financières et techniques de chaque concurrent, en rapport avec la nature et l'importance des prestations objet du présent appel d'offres.

Ne feront l'objet d'une évaluation de leur offre technique que les candidats admis à l'issue de l'examen des pièces du dossier administratif et du dossier technique conformément à l'article 9 du présent Règlement de Consultation.

La note technique minimale d'admissibilité de chaque concurrent prendra en considération les éléments composant son offre technique.

L'ensemble des critères retenus sur la base desdits éléments sont mentionnés au tableau ci-dessous :

1. Composition de l'équipe proposée (50 points).
2. Conformité de la solution SIEM proposée (40 points) ;
3. Démarche de réalisation du projet (10 points) ;

Critères d'appréciation	Indicateurs de mesure	Note d'évaluation	Justificatifs
1 - Evaluation de l'équipe projet	**Le chef de projet** **=> Formation** - **2 points** si le chef de projet a une formation supérieure de bac+5 en management ou ingénierie des systèmes d'information (SI) ou équivalent au moins ; - **0 point** s'il a une formation < Bac + 5. **=> Expérience dans le domaine de la sécurité des SI** - **3 points** s'il a plus que 8 ans d'expérience dans le domaine ; - **1 point** s'il a entre 5 et 8 ans d'expérience dans le domaine ; - **0 point** s'il a moins de 5 ans d'expérience dans le domaine. **=> Certification** - **1 point** s'il dispose d'une certification valide PMP ou PRINCE2 ; - **1 point** s'il dispose d'une certification valide ISO 27001 LI ; - **0 point** s'il ne dispose d'aucune certification. **Expert en intégration SIEM** **=> Formation** - **1 point** si l'expert a une formation supérieure de bac+5 en sécurité SI ou équivalent au moins ; - **0 point** s'il a une formation < Bac + 5. **=> Expérience dans le domaine** - **2 points** s'il a plus que 5 ans d'expérience dans le domaine ou équivalent ; - **0 point** s'il a moins de 5 ans d'expérience dans le domaine ou équivalent. **=> Certification** - **1 point** s'il dispose d'une certification valide relative à la solution SIEM proposée ; - **1 point** s'il dispose d'une certification valide ISO 27001 LI ; - **0 point** s'il ne dispose d'aucune certification. **Expert en organisation du SOC** **=> Formation** - **1 point** si l'expert a une formation supérieure de bac+5 en sécurité et réseau SI ou équivalent au moins ; - **0 points** s'il a une formation < Bac + 5. **=> Expérience dans le domaine** - **2 points** s'il a plus que 5 ans d'expérience dans le domaine ; - **0 point** s'il a moins de 5 ans d'expérience dans le domaine. **=> Certification** - **1 point** s'il dispose d'une certification valide CISSP ou CISM ; - **1 point** s'il dispose d'une certification valide ISO 27001 LA; - **0 point** s'il ne dispose d'aucune certification. **Architecte en Cybersécurité** **=> Formation** - **1 point** si l'expert a une formation supérieure de bac+5 en sécurité et réseau SI ou équivalent au moins ; - **0 points** s'il a une formation < Bac + 5. **=> Expérience dans le domaine** - **2 points** s'il a plus que 5 ans d'expérience dans le domaine ; - **0 point** s'il a moins de 5 ans d'expérience dans le domaine. **=> Certification** - **2 point** s'il dispose d'une certification valide CISSP; - **0 point** s'il ne dispose d'aucune certification. **Pour chaque analyste N1 avec un plafond de 06 profils** **=> Formation** **- 1 point** s'il a une formation supérieure de bac+3 en ingénierie ou équivalent au moins ; **- 0 point** s'il a une formation en ingénierie ou équivalent inférieure à bac+3 ; **=> Expérience** **- 1 point** s'il a une expérience en sécurité supérieure ou égale à 1 an ; **- 0 point** s'il a une expérience en sécurité inférieure strictement à 1 an. **=> Certification** - **1 point** s'il dispose d'une certification valide CEH ; - **0 point** s'il ne dispose d'aucune certification. **Pour chaque analyste N2 avec un plafond de 02 profils** **=> Formation** **- 1 point** s'il a une formation supérieure de bac+3 en ingénierie ou équivalent au moins ; **- 0 point** s'il a une formation en ingénierie ou équivalent inférieure à bac+3 ; **=> Expérience** **- 1 point** s'il a une expérience en sécurité supérieure ou égale à 2 ans ; **- 0 point** s'il a une expérience en sécurité inférieure strictement à 2 ans. **=> Certification** - 1 **point** s'il dispose d'une certification valide ECIH ; - **0 point** s'il ne dispose d'aucune certification. **Pour l'analyste N3** **=> Formation** **- 1 point** s'il a une formation supérieure de bac+5 en ingénierie ou équivalent au moins ; **- 0 point** s'il a une formation en ingénierie ou équivalent inférieure à bac+5 ; **=> Expérience** **- 1 point** s'il a une expérience en sécurité supérieure ou égale à 5 ans ; **- 0 point** s'il a une expérience en sécurité inférieure strictement à 5 ans. **=> Certification** - 1 **point** s'il dispose d'une certification valide GCFA ; - 1 **point** s'il dispose d'une certification valide GMON ; - **0 point** s'il ne dispose d'aucune certification.	/7 /5 /5 /5 /18 /6 /4	Note N° 1 + CVs de l'équipe (annexe 5)

		/50	
2- Conformité aux spécifications techniques de la solution SIEM proposée	La fiche technique de la solution SIEM basée sur le descriptif du CPS	**/40**	Note N°2 (Annexe 6)
3 – Démarche de réalisation du projet	**Pertinence des approches proposées pour la réalisation des prestations** **- 10 points** : Excellente ; **- 5 points** : Bonne ; **- 0 points** : Insuffisante. (Excellente : niveau de détail, pertinence, cohérence et conformité au CPS / Bonne : cohérence et conformité au CPS / Insuffisante : Omission d'éléments qui touchent à la substance de la mission exigée par le CPS).	/10 **/10**	Note N° 3
	Total (Note Technique)	**/100**	

Les concurrents ayant obtenu au moins une **note technique minimale** d'admissibilité égale à **soixante-dix (70)** sont admis.

Pendant l'examen des offres techniques et avant de se prononcer, la commission d'appel d'offres peut demander par écrit à l'un ou à plusieurs concurrents des éclaircissements sur leurs offres techniques. La commission lui fixe, à cet effet, un délai de réponse de **trois (03) jours** à compter de la date de réception de la lettre de demande d'éclaircissement. Les éléments de réponse du concurrent sont donnés par écrit.

Article 15 : Examen des offres financières

Conformément aux dispositions des articles 42, 43 et 44 du Règlement des Achats de la SNGFE, l'examen des offres financières concerne les seuls candidats admis à l'issue de l'examen de leurs offres techniques.

Le marché sera attribué au concurrent dont l'offre est **économiquement la plus avantageuse** conformément à l'article 43 du Règlement des Achats de la SNGFE, qui est celle la mieux disante par rapport aux prix de référence.

NB :

Le prix de référence est :

$$P = \frac{\left[\text{Estimation du Maître d'Ouvrage} + \left(\frac{\text{Somme des offres financières}}{\text{Nombre des offres financières}}\right)\right]}{2}$$

L'offre mieux disante est :

- L'offre la plus proche du prix de référence **par défaut** ;
- L'offre la plus proche **par excès** si aucune offre n'est inférieure à ce prix.

Article 16 : Délai de validité des offres

Les soumissionnaires qui n'ont pas retiré définitivement leurs plis dans les conditions prévus à l'article 12 ci-dessus, resteront engagés par leurs offres pendant un délai de **soixante jours (60 jours)**, à compter de la date d'ouverture des plis.

Si dans ce délai, le choix de l'attributaire ne peut être arrêté, le Maître d'Ouvrage pourra proposer, par lettre recommandée avec accusé de réception, de prolonger le délai de validité de leurs offres. Seuls les concurrents qui auront donné leur accord par lettre recommandée avec accusé de réception adressée au maître d'ouvrage resteront engagés pendant ce nouveau délai.

Article 17 : Monnaie de formulation des offres

Les prix des offres doivent être formulés et exprimés en Dirham marocain.

Lorsque le concurrent n'est pas installé au Maroc, son offre doit être exprimée en monnaie étrangère convertible. Dans ce cas, pour être évalués et comparés, les prix des offres exprimées en monnaie étrangère doivent être convertis en dirham. Cette conversion doit s'effectuer sur la base du cours vendeur du dirham en vigueur le premier jour ouvrable de la semaine précédant celle du jour d'ouverture des plis donné par Bank Al-Maghreb.

Article 18 : Langue d'établissement des pièces des offres

Les pièces contenues dans les dossiers et les offres présentées par les concurrents doivent être établies en langue française.

Article 19 : Préférence nationale

Conformément aux dispositions de l'article 147 du Règlement des Achats de la SNGFE, une préférence est accordée, lors de l'évaluation des offres financières, aux offres présentées par les concurrents installés au Maroc.

A cet effet, le montant de l'offre financière présentée par le concurrent non installé au Maroc est :

- Minoré d'un pourcentage fixé à quinze pour cent (15%), lorsque le montant de cette offre est le plus proche par défaut du prix de référence et qu'il existe des offres présentées par des concurrents installés au Maroc inférieures à ce prix de référence ;
- Majoré d'un pourcentage fixé à quinze pour cent (15%), lorsque le montant de cette offre est le plus proche par excès du prix de référence, en cas d'absence d'offres inférieures à ce prix de référence ;
- Majoré d'un pourcentage fixé à quinze pour cent (15%), lorsque le montant de cette offre est le plus proche par défaut du prix de référence, dans le cas où les offres présentées par les concurrents installés au Maroc sont supérieures à ce prix de référence.

Les dispositions du présent article ne s'appliquent pas au groupement, lorsqu'un ou plusieurs de ses membres sont installés au Maroc, à condition que la part qu'il détient ou qu'ils détiennent dans le groupement, telle qu'indiquée sur l'acte d'engagement, est égale ou supérieure à trente (30%) pour cent.

Article 20 : Résultat définitif de l'appel d'offres

Pour les résultats définitifs de l'appel d'offres, il sera appliqué les dispositions de l'article 47 du Règlement des Achats de la SNGFE.

Maitre d'Ouvrage	
Préparé par	**Signé par**
Chef du Département Logistique et Achats Signé : Charaf DOULIMI	Directeur Général Adjoint Ressources Signé : Abdelkhalek GLILLAH
Le concurrent Lu et accepté (mention manuscrite)	

Annexe 1 : Avis d'appel d'offres ouvert international

SOCIETE NATIONALE DE GARANTIE ET DU FINANCEMENT DE L'ENTREPRISE

Appel d'offres ouvert international n°13/2025/SNGFE

L'ACQUISITION ET LE RENOUVELLEMENT D'UN SIEM AINSI QUE LA MISE EN PLACE D'UN SOC AS A SERVICE POUR LE COMPTE DE LA SOCIETE NATIONALE DE GARANTIE ET DU FINANCEMENT DE L'ENTREPRISE (SNGFE)

Le jeudi 08 janvier 2026 à 10 heures, il sera procédé, dans les bureaux du siège de la Société Nationale de Garantie et du Financement de l'Entreprise, sise à Centre d'affaires Bd Ar Ryad, Rabat, à l'ouverture des plis relatifs à l'appel d'offres ouvert international sur offres de prix n° 13/2025/SNGFE, ayant pour objet l'acquisition et le renouvellement d'un SIEM ainsi que la mise en place d'un SOC as a Service pour le compte de la Société Nationale de Garantie et du Financement de l'Entreprise (SNGFE).

Le dossier d'appel d'offres doit être téléchargé à partir du portail des marchés publics : www.marchespublics.gov.ma. Il est également téléchargeable à partir du site de la Société Nationale de Garantie et du Financement de l'Entreprise : www.tamwilcom.ma

Le montant du cautionnement provisoire est fixé à **20.000,00 DHS (vingt mille dirhams).**

L'estimation annuelle des coûts des prestations établie par le Maître d'Ouvrage est de **1.500.000,00 DHS TTC (Un million cinq cent mille dirhams Toutes Taxes Comprises).**

Le contenu, la présentation ainsi que le dépôt des dossiers des concurrents doivent être conformes aux dispositions des articles 30 à 34 du Règlement des Achats de la SNGFE.

Les concurrents doivent déposer leurs dossiers par voie électronique dans le portail des marchés publics accessible à l'adresse www.marchespublics.gov.ma.

Les pièces justificatives à fournir sont celles prévues par l'article 9 du règlement de consultation.

NB : Le Règlement des Achats de la Société Nationale de Garantie et du Financement de l'Entreprise est téléchargeable sur le site : www.tamwilcom.ma

Annexe 2 : Modèle d'acte d'engagement

A - Partie réservée à la Société Nationale de Garantie et du Financement de l'Entreprise

Appel d'offres ouvert international sur offres de prix n° : **13/2025/SNGFE** du **08/01/2026 à 10 heures.**
Objet du marché : " L'acquisition et le renouvellement d'un SIEM ainsi que la mise en place d'un SOC as a Service pour le compte de la Société Nationale de Garantie et du Financement de l'Entreprise (SNGFE) " passé en application de l'alinéa 3 paragraphe i-1 et l'alinéa a) paragraphe 3 de l'article 19 et de l'alinéa b) du paragraphe 3 de l'article 20 du Règlement des Achats de la SNGFE.

B - Partie réservée au concurrent

a) Pour les personnes physiques

Je (1), soussigné : ..... (prénom, nom et qualité) agissant en mon nom personnel et pour mon propre compte, adresse du domicile élu ..... affilié à la CNSS sous le ..... inscrit au registre du commerce de ..... (localité) sous le n°.....n° de patente ..... , n° de l'ICE… ;

b) Pour les personnes morales

Je (1), soussigné .... (prénom, nom et qualité au sein de l'entreprise, de la coopérative ou de l'union des coopératives) agissant au nom et pour le compte de .....(raison sociale et forme juridique de la société ou raison sociale de la coopérative ou de l'union des coopératives) au capital de :.....adresse du siège social de la société, de la coopérative ou de l'union des coopérative .....adresse du domicile élu .....affiliée à la CNSS sous le n°..... et (2)inscrite au registre du commerce..... (localité) sous le n°..... et (2) Inscrit au registre local des coopératives ……(localité) sous le n° …… n° de patente ..... et (2), n° de l'ICE… et (2).

En vertu des pouvoirs qui me sont conférés :

après avoir pris connaissance du dossier d'appel d'offres, concernant les prestations précisées en objet de la partie A ci-dessus ;
après avoir apprécié de mon point de vue et sous ma responsabilité la nature et les difficultés que comportent ces prestations :

1) remets, revêtu de ma signature un bordereau des prix établi conformément au modèle figurant au dossier d'appel d'offres.
2) m'engage à exécuter lesdites prestations conformément au cahier des prescriptions spéciales et moyennant les prix que j'ai établi moi-même, lesquels font ressortir :

Montant annuel hors T.V.A ..... (en lettres et en chiffres) ;
Taux de la T.V.A ……(en lettres et en chiffres)
Montant de la T.V.A. ..... (en lettres et en chiffres) ;
Montant annuel T.V.A comprise..... (en lettres et en chiffres)

La Société se libérera des sommes dues par elle en faisant donner crédit au compte ouvert à mon nom (ou au nom de la société) à .....(localité), sous relevé d'identification bancaire (RIB) numéro .....

Fait à.....le.....

(Signature et cachet du concurrent)

(1) Lorsqu'il s'agit d'un groupement, ses membres doivent :
a) mettre « Nous, soussignés ……. nous obligeons conjointement ou solidairement » (choisir la mention adéquate et ajouter au reste de l'acte d'engagement les rectifications grammaticales correspondantes) ;
b) ajouter l'alinéa suivant : « désignons, (prénoms, noms et qualité) en tant que mandataire du groupement » ;
c) préciser la ou les parties des prestations que chacun des membres du groupement s'engage à réaliser pour le groupement conjoint et éventuellement pour le groupement solidaire.
(2) Ces mentions ne concernent que les sociétés assujetties à cette obligation.

Annexe 3 : Modèle de la déclaration sur l'honneur (*)

Mode de passation : Appel d'offres ouvert international n° **13/2025/SNGFE du 08/01/2026 à 10 heures.**
Objet du marché : " L'acquisition et le renouvellement d'un SIEM ainsi que la mise en place d'un SOC as a Service pour le compte de la Société Nationale de Garantie et du Financement de l'Entreprise (SNGFE) ".

A – Pour les personnes physiques

Je soussigné : ..... (Prénom, nom et qualité) ;
Numéro de téléphone ..... Numéro du fax ..... ;
Adresse électronique ..... ;
Agissant en mon nom personnel et pour mon propre compte, Adresse du domicile élu : .....;
Affilié à la CNSS sous le n° ..... ;
Inscrit au registre du commerce de .....(localité) sous le n° ..... ;
N° de patente..... ;
N° de l'identifiant commun de l'entreprise (ICE)..... ;
N° d'inscription au registre national de l'Auto-entrepreneur ..... ; (1)
N° de compte (RIB).....

B – Pour les personnes morales

Je soussigné : ..... (prénom, nom et qualité au sein de l'entreprise, de la coopérative ou de l'union des coopératives) ;
Numéro de téléphone ..... Numéro du fax ..... ;
Adresse électronique ..... ;
Agissant au nom et pour le compte de ..... (raison sociale et forme juridique de la société ou raison sociale de la coopérative ou l'union des coopératives), au capital de : ..... ;
Adresse du siège social de la société, de la coopérative ou de l'union des coopératives ..... ;
Adresse du domicile élu : ..... ;
Affilié à la CNSS sous le n° ..... ;
Inscrit au registre du commerce de .....(localité) sous le n° ..... ;
Inscrit au registre local des coopératives.....(localité) sous le n° ..... ;
N° de patente..... ;
N° de l'identifiant commun de l'entreprise (ICE)..... ;
N° de compte (RIB)....., en vertu des pouvoirs qui me sont conférés :

Déclare sur l'honneur :

1. que je remplie les conditions prévues à l'article 27 du Règlement des Achats de la SNGFE ;
2. m'engage à couvrir, dans les conditions fixées aux cahiers des charges, par une police d'assurance, les risques découlant de mon activité professionnelle ;
3. m'engage, si je recours à la sous-traitance, à veiller à ce que celle-ci ne dépasse pas cinquante pour cent (50%) du montant du marché et qu'elle ne porte pas sur le lot ou le corps d'état principal du marché, et à de m'assurer que les sous-traitants auxquels je recours remplissent les conditions prévues à l'article 27 du Règlement des Achats de la SNGFE ;
4. atteste que je dispose des autorisations requises pour l'exécution des prestations telles que prévues par la législation et la réglementation en vigueur ;
5. atteste que je ne suis pas en liquidation judiciaire ou en redressement judiciaire, et que si je suis en redressement judiciaire, que je suis autorisé par l'autorité judiciaire compétente à participer aux appels d'offres ; (2)
6. m'engage à ne pas recourir par lui-même ou par personne interposée à des pratiques de fraude ou de corruption des personnes qui interviennent, à quelque titre que ce soit, dans les procédures de passation, de gestion et d'exécution du marché ;
7. m'engage à ne pas faire, par moi-même ou par personne interposée, de promesses, de dons ou de présents, en vue d'influer sur la procédure de conclusion du marché et de son exécution ;
8. atteste que je ne suis pas en situation de conflit d'intérêts ;
9. atteste que je n'ai pas participé à la préparation du dossier de l'appel d'offres considéré ;
10. certifie l'exactitude des renseignements contenus dans la déclaration sur l'honneur et dans les pièces fournies dans mon dossier de candidature, sous peine de l'application des mesures coercitives prévues à l'article 152 du Règlement des Achats de la SNGFE.

Fait à ……,le……

(Signature et cachet du concurrent)

(1) A supprimer le cas échéant.
(*) En cas de groupement, chacun des membres doit présenter sa propre déclaration sur l'honneur.

Annexe 4 : Déclaration du plan de charges

Mode de passation : Appel d'offres ouvert international n° **13/2025/SNGFE du 08/01/2026 à 10 heures.**
Objet du marché : " L'acquisition et le renouvellement d'un SIEM ainsi que la mise en place d'un SOC as a Service pour le compte de la Société Nationale de Garantie et du Financement de l'Entreprise (SNGFE) "

Je soussigné : ..... (Prénom, nom et qualité) ; agissant en mon nom personnel et pour mon propre compte ou pour le compte de ..... (raison sociale et forme juridique) ;

En vertu des pouvoirs qui me sont conférés ;

Je déclare sur l'honneur mon plan de charge relatif au marchés publics en cours d'exécution à la date du .....[1] en vue de participer à la procédure d'appel d'offres n° 13/2025/SNGFE du 08/01/2026 relatif à l'acquisition et le renouvellement d'un SIEM ainsi que la mise en place d'un SOC as a Service pour le compte de la Société Nationale de Garantie et du Financement de l'Entreprise (SNGFE).

N°	Références[2]	Maître d'Ouvrage	Qualité (Titulaire ou sous-traitant)	Montant[3]	Taux d'exécution (en %)	Reste à exécuter (en %)
1						
2						
…						

Fait à ……,le……

Signature et cachet du concurrent
(signature électronique)

[1] Indiquer la date de remise de l'offre.
[2] Indiquer la référence du marché en question.
[3] Indiquer le montant en toutes taxes comprises y compris les augmentations ou diminution.

Annexe 5 : Modèle des Cvs

Nom	
Prénom	
Date de naissance	
Tél	
E-mail	
Profil	
Emploi Actuel	
Ancienneté dans le présent emploi	
Fonction au sein de l'équipe proposée	

Expérience professionnelle

Date du recrutement	Entreprise	Secteur d'activité	Poste

Formations

Intitulé du Diplôme	Durée de la formation	Etablissement	Année d'obtention

Certifications

Intitulé de la certification	Domaine de la certification	Etablissement	Année d'obtention

Projets professionnels (similaires à la prestation)

Client	Domaine d'activité	Intitulé du projet	Description du projet	Date de début du projet	Date de fin du projet	Fonction dans le projet

Annexe 6 : Tableau de conformité

Pour la solution SIEM :

*** Les spécifications n° : 1-2-3-4-5-6-7-8-9-10-11-12-13,15-16-17-20-21-22-23-24-27-28-29,32,33,36-37-38-39-41-44-45-47-48-49-51-55-56-57-58-59-60-61-63-64-66-69-72-74-75-76-7 7-78-80-82-87-88-89-90-92-95-96-97-99-100-101-102-103-104-106-107-108-110-114-115-117-118-119-121-124 sont obligatoires.**

Les détails de chaque spécification ainsi que les liens vers la documentation, doivent être présentés dans le tableau.

N°	Spécifications demandées	Note	Oui / Non	Référence par rapport aux documents techniques
	Exigence globale de la solution SIEM			
1*	La solution ainsi que tous ces composants doivent supporter, au minimum, une moyenne soutenue de **300 Event per Seconde** extensible à **1000** sans frais supplémentaires.	**N/A**		
2*	La solution proposée doit être d'un éditeur SIEM connu dans le marché, qui a au moins 20 ans d'existence et affichée dans le Magic Quadrant SIEM de Gartner	**N/A**		
3*	La solution devra être fournie avec un bundle UEBA, SOAR et FIM.	**N/A**		
4*	La solution ne doit supprimer, ni mettre dans un cash ni dans un buffer les évènements dans le cas du dépassement de la licence de 300 EPS.	**N/A**		
5*	La solution doit gérer un nombre illimité de device/adresse IP sans aucune restriction liée à la licence.	**N/A**		
6*	La solution doit être capable de collecter, traiter et indexer une quantité illimitée de sources de journaux sans aucune restriction sur les [actifs-périphériques IP ..etc] à surveiller.	**N/A**		
7*	La solution ne doit pas limiter les fonctionnalités du SIEM dans le cas du dépassement de la licence	**N/A**		
8*	La solution doit pouvoir gérer jusqu'à 1,000 EPS sans ajout de licence supplémentaire ni de frais supplémentaires	**N/A**		
9*	La solution doit gérer un nombre illimité d'équipement (log source) depuis le jour 1 de la mise en place	**N/A**		
10*	La possibilité de prédire les attaques « threat intelligence » sur la même plateforme	**N/A**		
11*	La solution doit inclure un SOAR managé depuis la même interface du SIEM	**N/A**		
12*	La solution doit inclure une fonctionnalité de « True identity » nativement, qui a la possibilité de collecter les identifiants des utilisateurs, tel que « le login et l'adresse e-mail,» qui constituent une identité unique afin d'enrichir tous les logs pour offrir à l'analyste une réelle visibilité sur les utilisateurs. (Fournir le lien et le détail de cette fonctionnalité)	**N/A**		
13*	La solution proposée ne devra pas être limitée par le nombre des collecteurs ou agents.	**N/A**		
14	Dashboard doit avoir une seule vue globale sur l'ensemble des données collectées à travers l'ensemble des plateformes	**1**		
15*	Le SIEM doit inclure nativement et sans ajout de licence, un module e-mail anti-phishing (Le SIEM doit avoir la capacité de tracker, d'analyser « en utilisant sa propre sandbox » et de répondre aux mails de Phishing). Le module antiphishing intégré, évalue en permanence les messages tracking logs à la recherche de contenu malveillant et répond de manière dynamique lorsque des menaces sont identifiées ou que des e-mails sont signalés (Veuillez inclure des détails et des liens de documentation pour chaque module proposé)	**N/A**		
16*	La plateforme NextGen SIEM doit inclure ces modules de manière native et out-of-the box sans « 3rd party » et sans licence ou frais supplémentaire : - SIEM - SOAR (Including Case Management and Incident Response) - Built in Email Anti-Phishing Module (SIEM Capability to Track, analyze "Using its own standalone Sandbox" and Respond to Phishing Mails) - UEBA Scénario based - Host Forensics - Network Forensics Module - Files Integrity Monitoring - Registry Integrity Monitoring - Process Monitoring - Security Analytics - True Big Data Indexing and Analytics Platform - Correlation avancée depuis une platform unique - Threat Intelligence - True identity Tous les modules doivent être fournis nativement à partir d'une seule solution SIEM sans recours aux solutions tierces et doivent être fonctionnels depuis le 1er jour de la mise en place. (Veuillez inclure des détails et des liens de documentation pour chaque module proposé)	**N/A**		
17*	Démontrer la valeur out of the box de la plateforme proposée.	**N/A**		

	La solution doit prendre en charge un minimum de + de 1000 intégrations de vendors/technologies prêtes « sans customisation des parseurs et sans frais»). – Veuillez fournir une liste complète des 1000+ intégrations disponibles La solution doit gérer un nombre illimité de device et se baser sur le nombre de EPS mentionné dans l'AO			
18	Pour offrir la meilleure expérience « out of the box », « depuis le jour 1 », la solution doit proposer au minimum le nombre de package ci-dessous : - + de 1000 use cases prédéfinis (règles d'analyse) : Fournir la liste complète. - + de 1250 rapports prédéfinis - 3 types de Classifications - 30 sous-classifications - +30.000 Common Events (Sub Classification) - +700.000+ Message Processing Engine Rules (Parsing Rules)	**1**		
19	La solution doit prendre en charge la multi-tenancy complète et la séparation complète des données	**1**		
20*	La solution doit prendre en charge un niveau très granulaire d'accès basé sur les rôles : - Autoriser différentes équipes à accéder au même appareil physique et à afficher la data liée à leur permission uniquement	**N/A**		
21*	La solution proposée doit corriger automatiquement l'heure de l'événement pour les journaux des systèmes avec des horodatages incorrects.	**N/A**		
	Architecture			
22*	Toutes les fonctionnalités de la solution proposée doivent être on-permise (sur site)	**N/A**		
23*	L'architecture à proposer doit être All in one .	**N/A**		
24*	La solution doit prendre en charge les modes de déploiement ci-dessous : - Standalone - Disaster recovery entre 2 sites - Une combinaison HA et Disaster Recovery - Haute disponibilité (avec failover automatique sans intervention de l'administrateur)	**N/A**		
25	Le soumissionnaire doit détailler l'architecture de la solution à mettre en place et les protocoles utilisés pour la collecte des logs	**1**		
26	Le soumissionnaire doit fournir les prérequis (RAM, CPU, Stockage, etc…) pour la création des VM.	**1**		
27*	S'engager que l'ajout de nouveaux collecteurs ou la mise en place de nouveau agent ne doit pas engendrer de frais supplémentaires et doit être gratuite.	**N/A**		
28*	L'architecture proposée doit être extensible et évolutive.	**N/A**		
29*	Le soumissionnaire doit offrir une solution qui stocke toutes les données localement (sur les plateformes de notre organisme).	**N/A**		
30	Toute communication entre les composants de la solution doit être chiffrée.	**1**		
31	La solution proposée doit offrir la possibilité d'utiliser des sources externes pour l'authentification sécurisée des utilisateurs de la solution (ex : Active Directory…).	**1**		
32*	La solution proposée doit tracer toutes les activités effectuées par les utilisateurs de la solution.	**N/A**		
33*	La solution doit offrir un outil « Node link graph » qui permet de visualiser les relations entre les serveurs , les patterns et les anomalies présentent au niveau des logs. L'outil doit permettre une visualisation graphique du traffic réseau entre les hôtes sources et destinations ainsi que les informations d'authentification entre un utilisateurs et un serveur ou application. Cet outil doit être fourni sous format graphique pour faciliter le threat hunting. (fournir une capture du graph)	**N/A**		
34	La solution doit s'intégrer avec les outils de test de vulnérabilité tiers. À détailler	**1**		
35	la solution doit permettre de chiffrer toute donnée au niveau de la collecte de journaux pour la surveillance des données confidentielles dans les journaux. À détailler	**1**		
36*	La solution proposée doit prendre en charge la capacité d'analyser un domaine Windows pour automatiser la découverte et la collecte d'événements à partir d'hôtes Windows.	**N/A**		
37*	La solution proposée doit permettre la collecte continue des logs en cas d'interruption temporaire de la communication avec la plateforme back-end.	**N/A**		
38*	La solution proposée doit inclure des alertes qui peuvent être facilement configurées si une source arrête d'envoyer des données de journal ou si la source de journal devient silencieuse.	**N/A**		
39*	La solution backend Big-Data proposée doit stocker les logs bruts et aussi les données meta-data	**N/A**		
40	La solution proposée doit fournir un stockage pour la visualisation et l'analyse des tendances à long terme	**1**		
41*	La solution proposée doit effectuer des contrôles d'intégrité sur les journaux stockés pour une conservation à long terme.	**N/A**		
42	Les capacités de recherche de la solution proposée doivent fournir des capacités d'exploration, de pivotement et de filtrage pour faciliter et accélérer les enquêtes	**1**		
43	La solution proposée doit effectuer une résolution de géolocalisation native au trafic d'adresses IP	**1**		
44*	La solution proposée doit contextualiser les informations de l'utilisateur avec des	**N/A**		

	informations détaillées sur les attributs de l'utilisateur du domaine tels que le nom d'utilisateur, le titre, le département, la dernière fois qu'il s'est connecté, la dernière fois qu'il a échoué dans le mot de passe, l'adresse e-mail...etc.			
45*	La solution proposée doit avoir un moteur de priorité basé sur les risques qui peut attribuer une valeur de risque pour tous les journaux, événements et alarmes nativement sans frais supplémentaires	**N/A**		
	Collecte/Regroupement/Normalisation			
46	La solution doit permettre de faire la collecte des données sur les événements par une voie de communication protégée	**1**		
47*	La solution doit permettre la normalisation ou le formatage des logs en provenance des équipements non supportés	**N/A**		
48*	La technologie de collecte doit prendre en charge la collecte depuis « Netflow - Jflow – Sflow » nativement et gratuitement sans licence de flux spécifique ni licence supplémentaire ni ajout d'un boitier collecteur de flux	**N/A**		
49*	La solution doit prendre en charge la synchronisation automatisée par horodatage au moyen du protocole de synchronisation réseau (NTP)	**N/A**		
50	Les collecteurs doivent avoir un espace de stockage local d'au moins 500Go en local avec protection des données (Raid)	**1**		
51*	La collecte des logs devra être faite d'une manière chiffrée en cas de mise en place d'agent local de collecte sur tout système (Windows, Unix …)	**N/A**		
52	La solution doit permettre la collecte en mode agent ou sans agent pour les différents systèmes d'exploitation (Windows, Unix…)	**1**		
53	Le collecteur ne doit pas être limitée par les interfaces des logs sources et doit prendre en charge toutes les interfaces de collecte connues, notamment "Json, API, FlatFile, Syslog, ODBC, etc."	**1**		
54	Le mécanisme de collecte distribuée doit fournir des options inline pour réduire les données d'événements à la source en filtrant les données d'événements inutiles. (Supprimer les « noisy logs » au niveau de la couche de collecte.)	**1**		
55*	Le collecteur de solution proposé doit prendre en charge l'équilibrage et le partage de charge automatiques	**N/A**		
56*	La solution proposée pour l'intégrité des fichiers « FIM » , doit inclure la prise en charge des plates-formes Windows et Linux. (Fournissez une liste complète de tous ceux qui sont pris en charge).	**N/A**		
57*	Le FIM intégré à la solution proposée doit surveiller de manière sélective les vues de fichiers, les modifications et les suppressions, ainsi que les changements de groupe, de propriétaire et d'autorisations.	**N/A**		
58*	La solution proposée doit supporter la planification de l'envoie des logs, la compression et/ou le chiffrement des logs collectés en remote.	**N/A**		
	Archive/Retention			
59*	La solution doit prendre en charge une période de rétention de 2 mois en ligne et 12 mois hors ligne d'archivage	**N/A**		
60*	La solution proposée doit compresser les logs d'archivage	**N/A**		
61*	La solution proposée doit fournir un assistant simple pour accéder aux données d'archives.	**N/A**		
62	La solution doit permettre la sauvegarde automatique des logs archives et rapport par une solution de sauvegarde externe (DAS, NAS, SAN). À détailler	**1**		
	Mise en corrélation			
63*	La solution doit fournir la capacité de corréler DHCP-VPN et des événements Active Directory pour fournir le suivi de session pour chaque utilisateur dans l'entreprise	**N/A**		
64*	La solution doit être en mesure de suivre l'activité des utilisateurs et lier un individu à une action	**N/A**		
65	La solution doit fournir la capacité de surveiller le réseau utilisateur et ses activités d'applications pour créer des lignes de base et ensuite utiliser ces lignes de base pour identifier le comportement anormal des utilisateurs	**1**		
66*	La solution doit disposer de base de règles de corrélation prédéfinies pour les différents types d'équipements (Top Attacks, Activity by specific username, etc)	**N/A**		
67	La solution doit être capable de restaurer les logs archivés pour analyse, corrélation et rapport. La solution doit permettre la corrélation des logs online et offline	**1**		
68	La solution doit supporter au minimum 1000 règles de corrélation out-of-the-box (fournir la liste complète des règles)	**1**		
69*	Les uses case doivent inclure dès le 1er jour, au minimum : - Le module de corrélation MITRE - Network Threat Detection and Correlation - User Threat Correlation - Emerging Active Threats and UEBA (User and Entity Behavior Analystics).	**N/A**		
70	Le prestataire est tenu de donner une liste des solutions de sécurité qui sont supporté par le SIEM (Vulnerability Management, IPS/IDS…)	**1**		
71	La solution proposée doit avoir la capacité de créer automatiquement des listes blanches de comportements observés (c'est-à-dire sans intervention manuelle).	**1**		
72*	La solution proposée doit déterminer automatiquement les menaces en fonction de schémas de comportement suspects.	**N/A**		

73	La solution proposée doit avoir la capacité d'apprendre automatiquement des références comportementales ou statistiques.	**1**		
74*	Les capacités d'analyse du comportement des utilisateurs et des entités (UEBA) de la solution proposée doivent être prêtes à l'emploi sans fonctionnalité/module/application/composant complémentaire.	**N/A**		
75*	La solution proposée doit avoir la capacité de tirer parti des événements corrélés ou d'anomalies dans d'autres règles de corrélation ou d'analyse avancée. [Chained Attacks]	**N/A**		
76*	La solution doit fournir du UEBA scénario based, nativement out of the box sans coût additionnel. L'UEBA doit supporter un nombre illimité d'utilisateurs.	**N/A**		
77*	La solution proposée doit pouvoir minimiser les faux positifs	**N/A**		
78*	La solution doit prendre en charge de nombreux types différents de méthodes de corrélation et d'analyse : [Observation – Non/Observation- Statistic-Behavior-Valeur Unique - Facteur limitant]	**N/A**		
79	La solution doit horodater tous les événements avec une précision à la seconde.	**1**		
	Analyse			
80*	La solution proposée doit contextualiser les informations utilisateurs avec des détails relatifs aux attributs des users depuis le domaine comme par exemple le username, titre, département, temps de la dernière authentification, le dernier failed login, l'adresse email afin d'enrichir les logs avec l'identité réelle derrière les informations de login	**N/A**		
81	La solution SIEM devra initier automatiquement un workflow qui sera capable d'ouvrir et d'attribuer des tickets localement ou sur une solution externe tout en conservant une piste d'audit complète pour le processus de traitement de l'incident	**1**		
82*	La solution doit permettre l'analyse des requêtes DNS pour détecter les malwares et les noms de domaine malveillants tel que DGA (Domain generation algorithm).	**N/A**		
83	La solution doit permettre la génération des alertes sur la base des événements selon plusieurs critères comme le type d'événement, les attaques, la localisation géographique, etc…	**1**		
84	La solution doit permettre l'évaluation du risque selon la cible	**1**		
85	La solution doit générer des notifications en réponse à une attaque de sécurité : Alerte sur Dashboard E-mail SYSLOG, SNMP, etc	**1**		
86	La solution doit être capable de détecter les menaces sur la base de la réputation	**1**		
	Anti Phishing Email Intelligence			
87*	La solution proposée doit être dotée d'une intelligence « Phishing Email » intégrée dans le SIEM (sans licence ni frais supplémentaire) afin de réduire l'exposition des actifs et des ressources internes aux risques. (Fournir le lien et le détail de cette fonctionnalité).	**N/A**		
88*	Le Phishing Email Intelligence proposé doit envoyer les e-mails suspects, y compris leurs pièces jointes, à une Sandbox (inclut dans le SIEM) pour des analyses et une vérification de la réputation	**N/A**		
89*	L'intelligence Emails phishing doit être en mesure d'envoyer une réponse au serveur de messagerie sur site ou dans le cloud (Exchange ou office365) pour empêcher l'e-mail de se propager au reste des employés.	**N/A**		
	Gestion des Incident [case Management]			
90*	La solution de gestion de cas intégrée proposée doit permettre de partager n'importe quel cas avec d'autres collaborateurs, qui peuvent également ajouter des preuves et des annotations pour accélérer la détection des menaces et la réponse. Toutes les activités doivent être suivies dans le cadre de l'historique du cas, fournissant un statut en temps réel et une piste d'audit inviolable.	**N/A**		
91	La solution doit inclure le suivi des incidents via une plate-forme de réponse aux incidents de sécurité entièrement intégrée capable de concevoir des flux de travail et des actions exécutives en réponse aux menaces et aux incidents déclenchés par la solution.	**1**		
92*	Le Playbook doit permettre à l'analyste de créer sa propre procédure/playbook de réponse aux incidents et de le suivre via l'interface utilisateur Web.	**N/A**		
93	La solution doit calculer les valeurs MTTD (Mean Time To Detect) et MTTR (Mean Time To respond) et les présenter au niveau du tableau de bord des analystes.	**0,5**		
94	La solution proposée doit offrir des playbook intégrés à la plateforme sans coût additionnel.	**0,5**		
95*	La solution proposée doit permettre de s'interfacer avec un système tiers de gestion de la réponse aux incidents (Remedy, etc.)	**N/A**		
	Sauvegarde et récupération			
96*	La solution SIEM doit fournir une méthode simple pour sauvegarder et restaurer les données de configuration du système automatiquement et manuellement	**N/A**		
	Traitements des logs			
97*	La solution doit supporter la rétention des logs en leur état brut pour une durée d'un an avec la possibilité de « replay » en cas de besoin	**N/A**		
98	La solution doit prévoir un mécanisme de reprise des logs en cas de rupture de connexion avec un collecteur	**0,5**		
99*	La solution doit être capable de garder les logs collectés avec une taille de cache de 100 Go au minimum en cas de perte de connectivité	**N/A**		
100*	Une fois reçu par le collecteur, les logs bruts doivent subir les traitements minimums suivants :	**N/A**		

	- La normalisation - L'enrichissement - L'agrégation - Le filtrage - Le cryptage - La Compression et l'archivage Le système doit être capable de supporter les méthodes de livraison de journaux communes. Celles-ci comprennent par exemple Syslog, événements Windows Collection (WinRM), FTP, S/FTP, SNMP, CP-LEA, SDEE, OPSEC, fichiers de texte brut, ODBC/JDBC et les fichiers XML. A détailler			
101*	La solution doit permettre aux administrateurs d'extraire les journaux dans son format brut pour une période définit.	**N/A**		
102*	Les journaux doivent être stockés dans un format haché afin d'assurer la sécurité des journaux de toute modification non autorisée.	**N/A**		
	Intégration du système			
103*	Le SIEM proposé doit supporter les technologies existantes. Le prestataire doit fournir la liste exhaustive des technologies avec les versions supportées. - Firewall - Proxy Web - Relais Mail - Endpoint Detection and Response - Network Detection and Response - Sandbox - IPS/IDS - Antivirus - Equipements réseaux - Serveurs	**N/A**		
104*	La solution proposée doit prendre en charge la collecte des journaux Netflow gratuitement sans appliances supplémentaires ni licence supplémentaire.	**N/A**		
105	Le collecteur de données/l'agent doit être en mesure de collecter les journaux par différentes méthodes, y compris, mais sans s'y limiter : [API-Flatfile-Syslog-SNMP-Universal Database Connection-WinRPC-AS/400-Netlfow-Jflow-Sflow-Compressed Flatfile]	**1**		
	Performance de traitement			
106*	Le Taux de compression doit aller jusqu'à 10 fois dans la couche de collecte.	**N/A**		
107*	La solution doit se baser sur une plateforme BigData nativement (sans ajout d'une BDD externe) pour l'indexation des logs sans compression pour garantir une rapidité de recherche, de génération des rapports et de threat hunting	**N/A**		
108*	La base de données de la solution doit inclure nativement une plateforme d'indexation Big Data (sans ajout d'une BDD externe) utilisée en tant que base de données principale et doit stocker 100 % des logs traités (pour vérifier la véracité des données). Veuillez mentionner quelle base de données des deux est utilisée.	**N/A**		
109	La plateforme d'indexation Bigdata doit avoir la capacité de prendre en charge le clustering jusqu'à 10 nœuds dans un seul cluster ainsi que la hiérarchisation des index stockés (Hot, Warm) pour prendre en charge une période de rétention EN LIGNE plus longue.	**0,5**		
110*	La solution proposée doit supporter un cluster actif/actif qui peut aller jusqu'à 10 appliances avec la capacité de construire une multitude de clusters et les manager depuis une seule console centralisée.	**N/A**		
	Administration			
111	La gestion de la solution devra être assurée depuis une console web sécurisée (HTTPS) et/ou console utilisateur (au minimum 3 utilisateurs à la fois)	**0,5**		
112	Administration centralisée depuis un point unique	**0,5**		
	Rapport et conformité			
113	La solution doit fournir depuis le 1er jour plus de 1250 rapports out of the box, (Fournir la liste des rapports)	**0,5**		
114*	Le module de reporting doit inclure nativement les packages de conformité ci-dessous : - GLBA Compliance Module - FISMA Compliance Module - GPG-13 Compliance Module - PCI-DSS Compliance Module - BSI IT-Grundschutz Module - 201 CMR 17 Module - HIPAA Module - ISO 27001 - NERC-CIP Module - ASD Module - SOX Module - HiTech Module - Dodi 8500.2 Module - NRC Module - NEI Module - CCF Module	**N/A**		

	- GDPR Compliance Module - ISO Compliance Module			
	Source de réputation (Threat Intelligence)			
115*	La solution doit être fournie avec une licence basée sur la réputation (IP des botnet, adresse email de phishing, url suspect, …etc)	**N/A**		
116	La solution proposée doit intégrer les données de plusieurs flux de renseignements sur les menaces -sources gratuits (OSINT)- dans des analyses avancées.	**0,5**		
	SOAR			
117*	La solution proposée doit automatiser la réponse aux menaces (Fournir le lien et le détail de cette fonctionnalité)	**N/A**		
118*	La solution proposée doit permettre d'ajouter des custom actions automatisée. Décrivez en détail le processus d'ajout d'une correction automatisée personnalisée.	**N/A**		
119*	Le moteur SOAR proposé doit être intégré dans la plate-forme prête à l'emploi	**N/A**		
120	La correction automatisée de la solution proposée doit fournir un flux de travail d'approbation hiérarchique intégré, afin que les actions puissent être prises automatiquement ou via une chaîne d'approbation.	**0,5**		
121*	La solution proposée doit prendre les mesures ci-dessous (sans s'y limiter) : - Désactiver le compte utilisateur AD - Mettre en quarantaine une machine infectée - Ajouter une adresse IP à la liste de blocage du pare-feu - Appliquer le service pour démarrer - Forcer le service à s'arrêter - Forcer la désactivation du service - Ajouter un élément à une liste de surveillance - Supprimer l'élément de la liste de surveillance - Désactiver le compte d'utilisateur local - Obliger l'utilisateur à se déconnecter d'une machine - Extraire le fichier pcap et ouvrir la pièce jointe divulguée - Exécuter la commande à distance - Supprimer le fichier - Effectuer un vidage de la mémoire	**N/A**		
	System Dashboard et Interface			
122	Le dashboard de la solution proposée doit être basé sur HTML5 affichant des données en temps réel et doit prendre en charge la fonction de timeline. (La fonctionnalité de timeline décompose les événements d'attaque par ordre chronologique)	**0,5**		
123	Le dashboard doit afficher les logs et alertes en temps réel	**0,5**		
124*	La solution doit donner la possibilité de créer des vues pour chaque utilisateur	**N/A**		
125	Les différents rapports devront être consolidés et accessibles sur le Dashboard	**0,5**		
126	La solution doit supporter le téléchargement des rapports sous plusieurs formats (PDF, CSV…)	**0,5**		
127	La solution doit donner la possibilité de créer tous les dashboard sur la base de n'importe quel champ des logs	**0,5**		
	Certification			
128	Accréditation Forensic Investigators du SOC marocain	**0,5**		
129	Le Soc marocain proposé est membre du CERT international First au Maroc	**0,5**		