ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

المكتب الوطني للمطارات
Office National Des Aéroports

DOSSIER D'APPEL D'OFFRES

Appel d'offres ouvert N° 014-24-AOO

Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

TABLE DES MATIERES

ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

AVIS D'APPEL D'OFFRES

OUVERT SUR "OFFRES DE PRIX"

N°014-24-AOO

Le **jeudi 25 janvier 2024** à **10h00**, il sera procédé, dans la salle de la Commission d'Appels d'Offres située au bâtiment de la Direction des Achats et de la Logistique (près de l'Aéroport CASABLANCA Mohammed V) à l'ouverture des plis relatifs à l'appel d'offres **sur offres de prix** concernant : **Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.**

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Le dossier d'appel d'offres peut être retiré **gratuitement**, auprès de la cellule Interface Achats au Département des Achats situé au bâtiment de la Direction des Achats et de la Logistique (près de l'Aéroport CASABLANCA Mohammed V). Il peut également être téléchargé à partir du portail des marchés publics **www.marchespublics.gov.ma** et **à titre indicatif** à partir de l'adresse électronique **www.onda.ma**.

Le cautionnement provisoire est fixé à la somme de : **328 000,00 DHS**

La constitution du cautionnement provisoire doit être effectuée **exclusivement par voie électronique via le portail des marchés publics**, dans les conditions fixées par l'arrêté n° 1692-23 du 4 hija 1444 (23 juin 2023) mentionné ci-dessous

L'estimation des coûts des prestations établie par le maitre d'ouvrage est fixée à la somme TVA comprise de :

- **Tranche ferme : 12 324 000,00 DHS.**
- **Tranche conditionnelle :**
  - **Montant minimum : 6 450 000,00 DHS**
  - **Montant maximum : 9 600 000,00 DHS.**

Le contenu, la présentation ainsi que le dépôt des dossiers des concurrents doivent être conformes aux dispositions des articles 06, 07, 08, 09, 10, 11, 12, 13 et 14 du règlement de la consultation du présent appel d'offres.

En effet, le dépôt et le retrait des plis et des offres des concurrents s'effectuent pour le présent appel d'offres, **obligatoirement**, **par voie électronique,** via le portail des marchés publics, dans les conditions fixées par l'arrêté n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatives aux marchés publics.

Les plis déposés, transmis ou reçus sur support papier ou postérieurement au jour et à l'heure fixés ci-dessus ne sont pas admis.

ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

المكتب الوطني للمطارات
Office National Des Aéroports

REGLEMENT DE CONSULTATION

Appel d'offres ouvert N° 014-24-AOO

Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

TABLE DES MATIERES

CHAPITRE 1 : DISPOSITIONS GENERALES

ARTICLE 01 : OBJET DE L'APPEL D'OFFRES

Le présent règlement concerne la consultation relative au projet : **Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.**

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

ARTICLE 02 : MAITRE D'OUVRAGE

Le maître d'ouvrage est l'Office National des Aéroports (ONDA).

ARTICLE 03 : CONDITIONS REQUISES DES CONCURRENTS

Peuvent valablement participer et être attributaires des marchés publics de l'ONDA, dans le cadre des procédures prévues par le présent règlement de consultation, les personnes physiques ou morales qui répondent aux conditions de l'article 24 du règlement des marchés de l'ONDA en vigueur.

ARTICLE 04 : CONTENU DU DOSSIER D'APPEL D'OFFRES

Le dossier d'appel d'offres comprend :

01. L'avis d'appel d'offres ;
02. Le présent règlement de consultation ;
03. Le cahier des prescriptions spéciales (CPS) ;
04. Le modèle d'acte d'engagement ;
05. Le modèle de la déclaration sur l'honneur ;
06. Le modèle du bordereau des prix-détails estimatifs ;
07. Le modèle du bordereau des prix pour approvisionnements, le cas échéant ;
08. Le modèle du sous détail des prix, le cas échéant ;
09. Les plans et documents techniques, le cas échéant.
10. Le règlement relatif aux marchés publics de l'Office National des Aéroports, approuvé le 09 juillet 2014, téléchargeable sur le site de l'ONDA à l'adresse suivante :

    http://www.onda.ma/Je-suis-Professionnel/Appels-d'offres/Règlementation-des-marchés-de-l'ONDA ;

NB : Tout concurrent est tenu de prendre connaissance et d'examiner toutes les instructions, modèles et spécifications contenues dans les documents de la consultation.

Le concurrent assumera les risques de défaut de fourniture des renseignements exigés par les documents de la consultation ou de la présentation d'une offre non conforme, au regard, des exigences des documents de la consultation. Ces carences peuvent entraîner le rejet de son offre.

ARTICLE 05 : LANGUE DE L'OFFRE

L'offre préparée par le concurrent ainsi que toute correspondance et tout document concernant l'offre échangés entre le concurrent et l'ONDA doivent être rédigés en **LANGUE FRANÇAISE**.

Tout document imprimé fourni par le candidat peut être rédigé en une autre langue dès lors qu'il est accompagné d'une traduction en langue française par une personne/autorité compétente (Les documents en arabe ne nécessite pas de traduction en français), des passages intéressants l'offre. Dans ce cas et aux fins de l'interprétation de l'offre, la traduction française fait foi.

Seules les offres techniques peuvent être fournies en langue **ARABE ou ANGLAISE**. Toutefois, en cas de besoin la Commission des Appels d'Offres peut demander, au concurrent et aux frais de ce dernier, la traduction des documents constituant l'offre technique en langue française.

ARTICLE 06 : DOSSIERS DES CONCURRENTS ET LISTE DES PIECES A FOURNIR

Conformément aux articles 25, 27, 28, 29 et 30 du règlement des marchés de l'ONDA en vigueur, chaque concurrent est tenu de présenter les pièces suivantes :

A. Le dossier administratif : Pièces exigées

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

A1. **Une déclaration sur l'honneur**, en un exemplaire unique, conformément au modèle joint au présent règlement de consultation ;

A2. Le **cautionnement provisoire**, tel que précisé au niveau de l'avis d'appel d'offres et dans les conditions fixées par l'article 7 ci-dessous.

A3. Pour les groupements, en plus des pièces citées ci-dessus, une copie légalisée de la **convention constitutive du groupement** prévue à l'article 140 du règlement des marchés de l'ONDA en vigueur.

La signature portée par chaque membre du groupement doit être originale et légalisée par une personne/autorité compétente. De ce fait, toute convention de groupement portant une signature scannée sera rejetée.

Pour les établissements publics :

A1. **Une déclaration sur l'honneur**, en un exemplaire unique, conformément au modèle joint au présent règlement de consultation.

A2. Le **cautionnement provisoire**, tel que précisé au niveau de l'avis d'appel d'offres et dans les conditions fixées par l'article 7 ci-dessous.

A3. Pour les groupements, en plus des pièces citées ci-dessus, une copie légalisée de la **convention constitutive du groupement** prévue à l'article 140 du règlement des marchés de l'ONDA en vigueur.

La signature portée par chaque membre du groupement doit être originale et légalisée par une personne/autorité compétente. De ce fait, toute convention de groupement portant une signature scannée sera rejetée.

A4. **Une copie du texte** l'habilitant à exécuter les prestations objet du marché.

B. Le complément du dossier administratif : Pièces exigées

Pour le concurrent auquel il est envisagé d'attribuer le marché, dans les conditions fixées à l'article 40 du règlement des marchés de l'ONDA en vigueur :

B1. **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'une **personne physique** agissant pour son propre compte :
  - Aucune pièce n'est exigée ;
- S'il s'agit d'un **représentant**, celui-ci doit présenter selon le cas :
  - Une copie conforme de la procuration **légalisée** lorsqu'il agit au nom d'une personne physique ;
  - Un extrait des statuts de la société et/ou le procès-verbal de l'organe compétent lui donnant pouvoir selon la forme juridique de la société, lorsqu'il agit au nom d'une personne morale ;
  - L'acte par lequel la personne habilitée délègue son pouvoir à une tierce personne, le cas échéant.

B2. **Une attestation fiscale** ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par l'Administration compétente du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties prévues à l'article 24 du **règlement des marchés de l'ONDA en vigueur**.

Cette attestation doit mentionner l'activité au titre de laquelle le concurrent est imposé.

NB : Pour les concurrents installés au Maroc, le document « Demande d'attestation de régularité fiscale » délivré par la Direction Générale des Impôts n'est pas acceptable. Seule l'attestation fiscale pour concurrents aux marchés publics délivrée par la Trésorerie Générale du Royaume est acceptable.

B3. **Une attestation** ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par la Caisse Nationale de Sécurité Sociale (**CNSS**) certifiant que le concurrent est en situation régulière envers cet organisme ou de la décision du ministre chargé de l'emploi ou sa copie certifiée conforme à l'originale, prévue par le dahir portant loi n° 1-72-184 du 15 joumada II 1392 (27 juillet 1972) relatif au régime de sécurité sociale assortie de l'attestation de l'organisme de prévoyance sociale auquel le concurrent est affilié et certifiant qu'il est en situation régulière vis-à-vis dudit organisme.

NB : La validité des pièces prévus aux B2) et B3) ci-dessus est appréciée sur la base de leur date de production par rapport de la date du dépôt du complément administratif (cf. paragraphe 5 de l'article 40 du règlement des marchés de l'ONDA).

B4. Le certificat d'immatriculation au **registre de commerce** pour les personnes assujetties à l'obligation d'immatriculation conformément à la législation en vigueur;

NB : Pour les concurrents non installés au Maroc l'équivalent des attestations visées aux paragraphes **B2**, **B3** et **B4** ci-dessus, délivrées par les administrations ou les organismes compétents de leurs pays d'origine ou de provenance.

A défaut de la délivrance de tels documents par les administrations ou les organismes compétents de leur pays d'origine ou de provenance, lesdites attestations peuvent être remplacées par une attestation délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits.

Pour les établissements publics :

B1. **Une attestation fiscale** ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par l'Administration compétente du lieu d'imposition certifiant qu'il est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties prévues à l'article 24 du règlement des marchés de l'ONDA en vigueur. Cette attestation, qui n'est exigée que pour les organismes soumis au régime de la fiscalité, doit mentionner l'activité au titre de laquelle le concurrent est imposé ;

NB : Pour les concurrents installés au Maroc, le document « Demande d'attestation de régularité fiscale » délivré par la Direction Générale des Impôts n'est pas acceptable. Seule l'attestation fiscale pour concurrents aux marchés publics délivrée par la Trésorerie Générale du Royaume est acceptable.

B2. **Une attestation** ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par la Caisse nationale de Sécurité Sociale (**CNSS**) certifiant que le concurrent est en situation régulière envers cet organisme conformément aux dispositions prévues à cet effet à l'article 24 ci-dessus ou de la décision du ministre chargé de l'emploi ou sa copie certifiée conforme à l'originale, prévue par le dahir portant loi n° 1-72-184 du 15 Joumada II 1392 (27 juillet 1972) relatif au régime de sécurité sociale assortie de l'attestation de l'organisme de prévoyance sociale auquel le concurrent est affilié et certifiant qu'il est en situation régulière vis-à-vis dudit organisme.

NB : La validité des pièces prévues aux **B1** et **B2** ci-dessus est appréciée sur la base de leur date de production par rapport de la date du dépôt du complément administratif (cf. paragraphe 5 de l'article 40 du règlement des marchés de l'ONDA).

C. Le dossier technique :

Chaque concurrent est tenu de présenter un dossier technique composé des pièces détaillées dans les dispositions particulières ci-dessous (chapitre 2 du présent règlement de consultation).

Lorsqu'il est prévu, au niveau des dispositions particulières (chapitre 2 du présent règlement de consultation), la présentation d'un certificat de qualification et de classification ou d'un certificat d'agrément. Ledit certificat tient lieu du dossier technique.

Pour les groupements, il y a lieu de se conformer aux dispositions de l'article 140 du règlement des marchés de l'ONDA en vigueur relatives au dossier technique.

D. Le dossier additif :

Il comprend toutes pièces complémentaires exigées par le présent règlement de consultation tel que détaillé dans les dispositions particulières (chapitre 2 du présent règlement de consultation).

E. Le cahier des prescriptions spéciales :

Paraphé et signé, en toutes les pages et sans réserves, par le concurrent ou la personne habilitée par lui à cet effet.

ARTICLE 07 : CAUTIONNEMENT PROVISOIRE

Chaque concurrent est tenu de produire un cautionnement provisoire ou l'attestation de la caution personnelle et solidaire en tenant lieu, tel qu'indiqué sur l'avis d'appel d'offres.

Le récépissé du cautionnement provisoire ou l'attestation de la caution personnelle et solidaire en tenant lieu **doivent être émis par un organisme Marocain agréé et arrêtés en Dirhams Marocains (MAD).**

NB 1 : Etant donné que la soumission par voie électronique est obligatoire, **la constitution du cautionnement provisoire s'effectue exclusivement par voie électronique, via le portail des marchés publics**, dans les conditions fixées par l'arrêté n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatives aux marchés publics et conformément aux conditions d'utilisation dudit portail.

NB 2 : Le cautionnement ne doit pas être limité dans le temps, ni comporter des conditions et/ou réserves de la part de la banque et/ou du soumissionnaire.

NB 3 : En cas de groupement, le cautionnement provisoire doit être souscrit conformément aux conditions d'utilisation du portail des marchés publics.

Aussi, **le récépissé du cautionnement provisoire** ou **l'attestation de la caution personnelle et solidaire** en tenant lieu **doivent préciser la mention suivante :**

« Le présent cautionnement est délivré dans le cadre d'un groupement et, en cas de défaillance, le montant dudit cautionnement reste acquis au maître d'ouvrage abstraction faite du membre défaillant ».

Le cautionnement provisoire reste acquis à l'ONDA dans les cas prévus par :

- L'article 15 du CCAG EMO ;
- L'article 18 du CCAG Travaux ;
- L'article 40 du règlement des marchés publics de l'ONDA.

ARTICLE 08 : OFFRES TECHNIQUES

Lorsque la présentation d'une offre technique est exigée conformément à l'article 28 du règlement des marchés de l'ONDA, les concurrents doivent fournir les pièces détaillées dans les dispositions particulières **(cf. chapitre 2 du présent règlement de la consultation)**.

ARTICLE 09 : OFFRES COMPORTANT DES VARIANTES

Les offres variantes ne sont pas prévues pour le présent appel d'offres.

ARTICLE 10 : OFFRE FINANCIERE

L'offre financière comprend :

1. **L'acte d'engagement,** conformément à **l'ANNEXE II,** en un seul exemplaire.

Cet acte d'engagement doit être dûment rempli, et comportant **le relevé d'identité bancaire (RIB)**, est signé par le concurrent ou son représentant habilité, sans qu'un même représentant puisse représenter plus d'un concurrent à la fois pour le même appel d'offres.

Lorsque l'acte d'engagement est souscrit par un groupement tel qu'il est défini à l'article 140 du règlement des marchés publics de l'ONDA, il doit être signé soit par chacun des membres du groupement ; soit seulement par le mandataire si celui-ci justifie des habilitations sous forme de **procurations légalisées** pour représenter les membres du groupement lors de la procédure de passation du marché.

Cette dernière disposition est applicable également **s'il s'agit d'un appel d'offres alloti** dont le règlement de consultation prévoit un acte d'engagement pour chaque lot ; Abstraction

faite de la répartition des lots entre les membres du groupement, qu'il soit conjoint ou solidaire.

Si le groupement est conjoint, il doit présenter un acte d'engagement unique qui indique le montant total du marché et **doit préciser** la ou les parties des prestations que chacun des membres du groupement conjoint s'engage à réaliser.

Si le groupement est solidaire, il doit présenter un acte d'engagement unique qui indique le montant total du marché et l'ensemble des prestations que les membres du groupement s'engagent solidairement à réaliser, cet acte d'engagement **peut**, le cas échéant, indiquer les prestations que chacun des membres s'engage à réaliser dans le cadre dudit marché

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

2. **Le bordereau des prix-détail estimatif**, conformément à l'**ANNEXE III**. Les concurrents **ne doivent** pas proposer plusieurs prix en monnaies différentes pour une même ligne figurant au niveau du bordereau des prix-détail estimatif.

Conformément à l'article 27 du règlement des marchés de l'ONDA en vigueur :

- Les prix unitaires du bordereau des prix, du détail estimatif et ceux du bordereau des prix-détail estimatif et les prix forfaitaires du bordereau du prix global et de la décomposition du montant global **doivent être libellés en chiffres**.
- En cas de discordance entre les prix unitaires du bordereau des prix et ceux du détail estimatif, les prix du bordereau des prix prévalent.
- En cas de discordance entre les montants totaux du bordereau du prix global et ceux de la décomposition du montant global, le montant total la décomposition du montant global prévaut.
- Les montants totaux du bordereau des prix-détail estimatif, du bordereau du prix global et de la décomposition du montant global **doivent être libellés en chiffres.**
- En cas de discordance entre le montant total de l'acte d'engagement, et de celui du détail estimatif, du bordereau des prix-détail estimatif ou du bordereau du prix global, selon le cas, le montant de ces derniers documents est tenu pour bons pour établir le montant réel de l'acte d'engagement.

3. **Le sous détail des prix**, le cas échéant.
4. **Le bordereau des prix pour approvisionnements**, lorsqu'il est prévu par le cahier de prescriptions spéciales.

ARTICLE 11 : MONNAIE DE L'OFFRE

Les offres financières **des concurrents résidents au Maroc** doivent être exprimées **exclusivement** en Dirhams Marocains (**MAD**). En cas de groupement avec des concurrents non-résidents au Maroc, les prix des prestations qui seront payées au membre résident au Maroc doivent être exprimés en Dirhams Marocains.

Lorsque le concurrent est non-résident au Maroc, son offre peut être exprimée strictement dans la(es) monnaie(s) suivante(s) :

- **MAD** : Dirhams marocains

- **EUR** : Euros
- **USD :** Dollars américains

Les offres exprimées en monnaies étrangères (**EUR/USD**) seront, pour les besoins d'évaluation et de comparaison, converties en Dirham. Cette conversion s'effectue sur la base du **cours de référence du dirham** en vigueur, du premier jour ouvrable de la semaine précédant celle du jour d'ouverture des plis, donné par Bank Al-Maghrib.

NB : Un concurrent **ne doit pas** proposer plusieurs prix en monnaies différentes pour une même ligne figurant au niveau du bordereau des prix-détail estimatif. **A défaut, son offre sera écartée.**

ARTICLE 12 : PRESENTATION DES DOSSIERS DES CONCURRENTS

Comme précisé dans l'avis d'appel d'offres, **la soumission par voie électronique est obligatoire.** De ce fait, il est demandé aux concurrents de présenter, **électroniquement**, les documents exigés, sous le **format standard A4** à l'exception des plans qui peuvent être présentés sous format A3.

Les pièces produites par chaque concurrent doivent être insérées, individuellement, dans l'enveloppe électronique les concernant.

Aussi, conformément aux conditions d'utilisation du portail des marchés publics, chaque document doit être signé, électroniquement, par le concurrent ou la personne dûment habilitée à le représenter, à l'exception des pièces dématérialisées.

Contenu des enveloppes :

1. Lorsque l'offre technique n'est pas exigée, **Deux (02) enveloppes** distinctes :
    a. **La première enveloppe** contient :
        1. Les pièces du **dossier administratif** (Article 6 § A) ;
        2. Les pièces du **dossier technique** (Article 6 § C) ;
        3. Les pièces du **dossier additif** (Article 6 § D), le cas échéant ;
        4. Le **c**ahier des **p**rescriptions **s**péciales (Article 6 § E).
    b. **La deuxième enveloppe** contient les pièces exigées de l'offre financière telles que détaillées dans l'article 10 ci-dessus ;
2. Lorsque l'offre technique est exigée, **Trois (03) enveloppes** distinctes :
    a. **La première enveloppe** contient :
        1. Les pièces du **dossier administratif** (Article 6 § A) ;
        2. Les pièces du **dossier technique** (Article 6 § C) ;
        3. Les pièces du **dossier** additif (Article 6 § D), le cas échéant.
        4. Le **c**ahier des **p**rescriptions **s**péciales (Article 6 § E).
    b. **La deuxième enveloppe** contient les pièces exigées de l'offre financière telles que détaillées dans l'article 10 ci-dessus ;
    c. **La troisième enveloppe** contient les pièces exigées de l'offre technique telles que détaillées dans l'article 8 ci-dessus.

NB : Lorsque **l'appel d'offres est alloti** :

- Le concurrent peut participer à un ou plusieurs lots ;

- Le concurrent doit présenter les offres techniques, si elles sont exigées et les offres financières **séparément** pour chaque lot.

A défaut, son offre sera écartée.

ARTICLE 13 : DEPOT DES OFFRES DES CONCURRENTS

1. Dépôt des échantillons, prospectus, notices ou autres documents techniques

Lorsque le dépôt d'échantillons et/ou la présentation de prospectus, notices ou autres documents techniques est exigé, conformément à l'article 34 du règlement des marchés de l'ONDA, les concurrents doivent déposer les échantillons/documents détaillés dans les dispositions particulières (**cf. chapitre 2 du présent règlement de la consultation**), dans les conditions fixées au niveau de l'avis d'appel d'offres.

2. Dépôt des plis par voie électronique

La soumission par voie électronique est obligatoire. Par conséquent, les plis des concurrents doivent être déposés dans les conditions fixées dans l'avis d'appel d'offres du présent dossier d'appel d'offres.

En effet et sauf stipulations différentes dans l'avis d'appel d'offres, le dépôt et le retrait des plis et des offres des concurrents s'effectuent pour le présent appel d'offres, **obligatoirement**, **par voie électronique,** via le portail des marchés publics, dans les conditions fixées par l'arrêté n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatives aux marchés publics.

Les plis déposés, transmis ou reçus sur support papier ou postérieurement au jour et à l'heure fixés ci-dessus ne sont pas admis.

Toutes les pièces exigées par le présent règlement de consultation, **doivent être insérées, individuellement, dans l'enveloppe électronique les concernant et ce, comme détaillé dans l'article 12 ci-dessus**.

Aussi, conformément aux conditions d'utilisation du portail des marchés publics, chaque document doit être signé, électroniquement, par le concurrent ou la personne dûment habilitée à le représenter, à l'exception des pièces dématérialisées et ce, avant leur insertion dans **l'enveloppe électronique** correspondante.

Cette signature s'effectue par le concurrent au moyen d'un certificat de signature électronique conformément aux dispositions des textes législatifs et réglementaires en vigueur et aux conditions d'utilisation du portail des marchés publics.

Les plis sont déposés moyennant le certificat de signature électronique susmentionné.

Le dépôt des plis fait l'objet d'un horodatage automatique au niveau du portail des marchés publics, mentionnant la date et l'heure de dépôt électronique et de l'envoi de l'accusé de réception électronique au concurrent concerné à travers ledit portail.

3. Dépôt des plis complémentaires

Le pli contenant les pièces produites, suite à la demande de la commission d'appel d'offres, par le concurrent auquel il est envisagé d'attribuer le marché, doit être, **selon le choix fixé** dans la demande de ladite commission :

- soit **déposé**, sur support papier, contre récépissé, dans le bureau du maître d'ouvrage indiqué dans la demande ;
- soit **envoyé**, sur support papier, par courrier recommandé avec accusé de réception, au bureau précité ;
- soit transmis, **par voie électronique**, via le portail des marchés publics, dans les conditions fixées par l'arrêté 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 déposés, transmis ou reçus postérieurement au délai fixé dans la demande de la commission **ne sont pas admis**.

NB :

La conclusion du marché issu de la procédure de la réponse électronique aux appels d'offres est effectuée sur la base d'un dossier sous format électronique.

Toutefois, l'adjudicataire est tenu de présenter sous format papier tout document demandé pour la conclusion du marché.

ARTICLE 14 : RETRAIT DES OFFRES DES CONCURRENTS

a. **Tout pli déposé électroniquement** peut être retiré par le concurrent antérieurement au jour et à l'heure fixés pour la séance d'ouverture des plis.

Le retrait de tout pli s'effectue au moyen du **certificat de signature électronique** ayant servi au dépôt de ce pli.

Les informations relatives au retrait des plis sont enregistrées automatiquement sur le registre de dépôts des plis.

Les concurrents ayant retiré leurs plis peuvent présenter de nouveaux plis dans les conditions prévues par le présent règlement de consultation et avant la date et heure limites d'ouverture des plis.

b. **Les échantillons, prototypes, prospectus, notices ou autres documents techniques** déposés ou reçus peuvent être retirés au plus tard le jour ouvrable précédant le jour et l'heure fixés pour l'ouverture des plis.

Le retrait des échantillons, prototypes, prospectus, notices ou autres documents techniques fait l'objet d'une demande écrite et signée par le concurrent ou son représentant dûment habilité. La date et l'heure du retrait sont enregistrées par le maître d'ouvrage dans un registre.

Les concurrents ayant retiré leurs échantillons, prototypes, prospectus, notices ou autres documents techniques peuvent présenter de nouveaux échantillons, prototypes, prospectus, notices ou autres documents techniques dans les conditions prévues dans le présent règlement de consultation.

ARTICLE 15 : OUVERTURE DES PLIS ET EXAMEN ET EVALUATION DES OFFRES

La séance d'ouverture des plis des concurrents **est publique.** Elle se tient au lieu, au jour et à l'heure prévus par le dossier d'appel d'offres ; si ce jour est **déclaré férié ou chômé**, la

réunion se tient le jour ouvrable suivant à la même heure, et ce conformément à l'article 36 paragraphe 1 du règlement des marchés de l'ONDA en vigueur.

Conformément aux conditions d'utilisation du portail des marchés publics, il est procédé à l'ouverture des plis et à l'examen des offres des concurrents déposés **par voie électronique** dans les conditions fixées, notamment, dans articles **36, 37, 38, 39, 40, 41 et 42** du règlement des marchés de l'ONDA en vigueur jusqu'à l'achèvement des travaux de la commission de la consultation.

Les résultats de l'évaluation des offres des concurrents déposées **par voie électronique** sont portés à la connaissance de ces derniers au fur et à mesure du déroulement des travaux de la commission de consultation.

Lorsqu'il s'agit d'un appel d'offres alloti, la commission procède pour l'attribution des lots à l'ouverture, l'examen des offres de chaque lot et l'attribution des lots, lot par lot, dans l'ordre de leur énumération dans le dossier d'appel d'offres.

L'adjudication d'un lot n'est pas conditionnée par l'adjudication de l'un ou des autres lots quelle que soit leur énumération dans le dossier d'appel d'offres, sauf stipulations contraires dans les dispositions particulières du présent règlement de consultation. Par conséquent, l'ouverture des plis d'un lot peut être effectuée par la commission même si le lot précédent dans l'appel d'offres n'est pas encore adjugé.

ARTICLE 16 : CRITERES D'ADMISSIBILITE DES CONCURRENTS ET D'ATTRIBUTION DU MARCHE

Les critères d'admissibilité des concurrents sont détaillés dans les dispositions particulières (chapitre 2 du présent règlement de la consultation).

ARTICLE 17 : RESULTATS DEFINITIFS DE L'APPEL D'OFFRES

Le maître d'ouvrage informe le concurrent attributaire du marché de l'acceptation de son offre **via le portail des marchés publics** ou **par lettre recommandée avec accusé de réception** ou **par tout autre moyen de communication donnant date certaine**. Cette lettre est adressée dans un délai de **cinq (05) jours ouvrables** au maximum à compter du lendemain de la date d'achèvement des travaux de la commission.

Dans le même délai, il avise également les concurrents éliminés du rejet de leurs offres, en leur indiquant les motifs de leur éviction **via le portail des marchés publics** ou par **lettre recommandée avec accusé de réception** ou par **tout autre moyen de communication donnant date certaine**.

Les échantillons ou prototypes, le cas échéant, sont restitués, après achèvement du délai de réclamation auprès du maître d'ouvrage, aux concurrents éliminés contre décharge.

ARTICLE 18 : DELAI DE VALIDITE DES OFFRES ET DELAI DE NOTIFICATION DE L'APPROBATION

Les concurrents restent engagés par leurs offres pendant un délai de **soixante-quinze (75)** jours, à compter de la date de la séance d'ouverture des plis.

Ce délai peut être prorogé dans les conditions prévues aux articles 33 et 136 du règlement des marchés de l'ONDA en vigueur.

Toutefois, la signature du marché par l'attributaire vaut le maintien de son offre.

ARTICLE 19 : ANNULATION D'UN APPEL D'OFFRES

L'autorité compétente (ONDA) peut, sans de ce fait encourir aucune responsabilité à l'égard des concurrents et quel que soit le stade de la procédure pour la conclusion du marché, annuler l'appel d'offres. Cette annulation intervient dans les cas suivants :

1. Lorsque les données économiques ou techniques des prestations objet de l'appel d'offres ont été fondamentalement modifiées ;
2. Lorsque des circonstances exceptionnelles ne permettent pas d'assurer l'exécution normale du marché ;
3. Lorsque les offres reçues dépassent les crédits budgétaires alloués au marché ;
4. Lorsqu'un vice de procédure a été décelé ;
5. En cas de réclamation fondée d'un concurrent **sous réserve** des dispositions de l'article 152 du règlement des marchés de l'ONDA en vigueur;

En cas d'annulation d'un appel d'offres dans les conditions prévues ci-dessus, les concurrents ou l'attributaire du marché ne peuvent prétendre à indemnité.

ARTICLE 20 : INFORMATION, DEMANDE D'ECLAIRCISSEMENT ET RECLAMATIONS

Tout concurrent peut demander au maître d'ouvrage, **par courrier** porté avec accusé de réception, **par lettre recommandée** avec accusé de réception ou par **voie électronique** de lui fournir des éclaircissements ou renseignements concernant l'appel d'offres ou les documents y afférents, **exclusivement**, aux coordonnées suivantes :

Adresse	**Département des Achats** Office National des Aéroports Aéroport Casablanca Mohammed V – Nouasseur
Boite postale	BP 52, Aéroport Casablanca Mohammed V – Nouasseur
E-mail	achats@onda.ma
Portail des marchés publics	https://www.marchespublics.gov.ma

NB : Cette 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.

Les réclamations des concurrents doivent être formulées dans les conditions fixées par l'article 152 du règlement des marchés publics de l'ONDA.

En effet, les réclamations des concurrents doivent être introduites **à partir de la date de la publication** de l'avis d'appel à la concurrence et **au plus tard cinq (05) jours** après l'affichage du résultat du présent appel d'offres.

Toutefois, la réclamation du concurrent pour contester les motifs d'éviction, doit intervenir à compter de la date de réception de la lettre d'éviction et au plus tard dans les cinq (05) jours suivants.

Important : Toute correspondance émanant d'un concurrent, sur support papier ou par voie électronique, doit être signée, datée et établie sur papier en-tête précisant notamment, la

dénomination/la raison sociale du concurrent ainsi que le nom, le prénom et la qualité de la personne habilitée ayant émis et signé ladite correspondance. A défaut, l'ONDA se réserve le droit de ne pas donner une suite à ladite correspondance.

CHAPITRE 2 : DISPOSITIONS PARTICULIERES

Article 1 : Objet de l'appel d'offres

Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Article 06 § C : Liste des pièces exigées pour le dossier technique

C1. Une note indiquant **les moyens humains et techniques** du concurrent et mentionnant éventuellement,

- La date,
- Le lieu,
- La nature et l'importance des prestations à l'exécution desquelles le concurrent a participé et la qualité de sa participation.

C2. Les attestations de référence, originales 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 des prestations d'importance et de complexité similaires à l'objet du présent appel d'offres, **dont au moins trois (3) attestations de référence** :

- **Une (1) relative à des prestations dans le domaine de la sécurité SI de complexité similaire de plus de 7 millions DHS HTVA ;**
- **Une (1) relative au déploiement ou infogérance d'une solution SIEM ou de supervision SOC de plus de 5 600 000 millions DHS HTVA ;**
- **Une (1) relative au déploiement ou infogérance/supervisions des solutions EDR ou NDR de plus de 800 000,00 DHS HTVA.**

Chaque attestation précise notamment :

- La nature des prestations ;
- Leur montant ;
- Le nom et la qualité du signataire et son appréciation ;
- L'année de réalisation (**entre 2017 et 2023**).

Article 06 § D : Liste des pièces exigées pour le dossier additif

- **Attestation de qualification PASSI Classe A et B en cours de validité, délivrée par la DGSSI au concurrent.**

Article 08 : Liste des pièces exigées pour l'offre technique

a. La méthodologie de gestion du projet proposée ;

b. Le planning envisagé pour la réalisation du projet et décrivant l'ordonnancement des tâches ;

c. Un tableau récapitulatif des spécifications techniques des solutions proposées en précisant les caractéristiques proposées (Cf. Annexe IV) ;

d. Les certifications en cours de validité ISO 27001 du SOC du concurrent ;

e. Les CV nominatifs de tous les intervenants en précisant les diplômes, les qualités et les anciennetés dans le domaine objet de l'appel d'offres, les membres du projet doivent comprendre au moins :

a. Pour la mise en place

Chef de projet : Bac+5 en management des SI, Ingénierie des SI ou équivalent ayant les compétences suivantes :

b. Ayant au **moins huit (8) ans** d'expériences dans la gestion de projets de sécurité complexes et de grandes envergures.

c. Disposant obligatoirement des certifications suivantes : PMP, CISM et CISSP.

Expert en intégration SIEM : Bac +5 en Sécurité SI ou équivalent ayant **5 ans** d'expériences et les certificats suivants :

d. Certifié obligatoirement sur la solution SIEM proposée et CEH.

Expert en organisation du SOC : Bac +5 en Sécurité et réseau ou équivalent et disposant de **cinq (5) ans** d'expériences et obligatoirement les certifications suivantes : CISSP et ISO 27001 LI .

Architecte (qualifié PASSI par la DGSSI dans les domaines audit des architectures et audit des systémes industriels) ayant une formation Bac +5 en sécurité ou équivalent et **dix (10) ans** d'expériences et obligatoirement les certifications suivantes : CISSP et OSCE.

Expert Aéroportuaire ayant une expérience de plus de 5 ans dans le domaine de la cybersécurité au sein des aéroports.

a. Pour la supervision :

Au moins six (6) analystes N1 : Bac +2 ou plus en informatique ou équivalent ayant **un (1) an** ou plus d'expérience en sécurité et dont au moins 2 certifiés CEH.

Au moins deux (2) analystes N2 : Bac +3 ou plus en informatique ou équivalent ayant **deux (2) ans** ou plus d'expérience en sécurité et certifiés obligatoirement OSCP.

Au moins deux (2) analystes N3 : Bac +5 ou plus en informatique ou équivalent ayant **cinq (5) ans** ou plus d'expérience en sécurité et certifiés obligatoirement CHFI et CEH.

Article 16 : Critères d'admissibilité des concurrents et d'attribution du marché

Le seul critère d'attribution, après admission, est l'**offre la moins-disante** sur la base **du prix global combinant le prix de la tranche ferme et le prix de la tranche conditionnelle pour les cinq années.**

ANNEXE I : MODELE DE DECLARATION SUR L'HONNEUR

Déclaration sur l'honneur

- Référence de l'appel d'offres : **014-24-AOO**
- Mode de passation : **Appel d'offres Ouvert**
- Objet du marché : **Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence**
    - **Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.**
    - **Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.**

A – Si le concurrent est une personne physique

Je, soussigné : .....(prénom, nom et qualité)
Numéro de tél……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° : ..... (1)
-Inscrit au registre du commerce de.....(localité) sous le n° ..... (1)
-N° de patente..... (1)
-N° du compte courant postal/bancaire ou à la TGR……(RIB)

B - Si le concurrent est une personne morale

Je, soussigné .....(prénom, nom et qualité au sein de l'entreprise)
numéro de tél…….numéro du fax……adresse électronique……..…

-Agissant au nom et pour le compte de..... (raison sociale **(**)** et forme juridique de la société) au capital de : .....
-Adresse du siège social de la société : .....
-Adresse du domicile élu.....
-Affiliée à la CNSS sous le n°.....(1)
-Inscrite au registre du commerce.....localité) sous le n°.....(1)
-N° de patente.....(1)
-N° du compte courant postal-bancaire ou à la TGR……..(RIB)

En vertu des pouvoirs qui me sont conférés déclare sur l'honneur :

1) M'engager à couvrir, dans les limites fixées dans le cahier des charges, par une police d'assurance, les risques découlant de mon activité professionnelle ;

2) Que je remplie les conditions prévues à l'article 24 du règlement des marchés publics de l'ONDA ;

3) Étant en redressement judiciaire j'atteste que je suis autorisé par l'autorité judiciaire compétente à poursuivre l'exercice de mon activité (2) ;

4) M'engager, si j'envisage de recourir à la sous-traitance :

a) A m'assurer que les sous-traitants remplissent également les conditions prévues par l'article 24 du règlement des marchés publics de l'ONDA ;

b) Que celle-ci ne peut dépasser 50 % du montant du marché, ni porter sur les prestations constituant le lot ou le corps d'état principal prévues dans le cahier des

prescriptions spéciales, ni sur celles que le maître d'ouvrage a prévu dans ledit cahier ;

5) M'engager à ne pas recourir par moi-même ou par personne interposée à des pratiques de fraude ou de corruption de personnes qui interviennent à quelque titre que ce soit dans les différentes procédures de passation, de gestion et d'exécution du présent marché.

6) M'engager à ne pas faire, par moi-même ou par personnes interposées, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion du présent marché.

7) Attester que je ne suis pas en situation de conflit d'intérêt tel que prévu à l'article 151 du règlement des marchés publics de l'ONDA.

8) Certifier l'exactitude des renseignements contenus dans la présente déclaration sur l'honneur et dans les pièces fournies dans mon dossier de candidature.

9) Reconnaitre avoir pris connaissance des sanctions prévues par l'article 142 du règlement des marchés publics de l'ONDA, relatives à l'inexactitude de la déclaration sur l'honneur.

Fait à.....le.....

Signature et cachet du concurrent

(1) pour les concurrents non installés au Maroc, préciser la référence aux documents équivalents lorsque ces documents ne sont pas délivrés par leur pays d'origine ou de provenance.

(2) à supprimer le cas échéant.

(**) La raison sociale doit être identique à celle figurant sur les statuts de la société

NB : Pour les groupements, chaque membre du groupement doit présenter sa propre déclaration sur l'honneur.

ANNEXE II : MODELE D'ACTE D'ENGAGEMENT

Acte d'engagement

Appel d'offres ouvert sur offres de prix n° **014-24-AOO** du **jeudi 25 janvier 2024**

A - Partie réservée à l'ONDA

Objet du marché : **Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence**

- **Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.**
- **Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.**

Passé en application des dispositions de l'alinéa 2, paragraphe 1 de l'article 16 et de l'alinéa 3, paragraphe 3 de l'article 17 du règlement relatif aux marchés publics de l'Office National des Aéroports en vigueur.

B - Partie réservée au concurrent

a) Si le concurrent est une personne physique

Je, soussigné : .....(prénom, nom et qualité)
Numéro de tél……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° : ..... (2)
- Inscrit au registre du commerce de.....(localité) sous le n° ..... (2)
- N° de patente..... (2)

b) Si le concurrent est une personne morale

Je, soussigné .....(prénom, nom et qualité au sein de l'entreprise)
numéro de tél…….numéro du fax……adresse électronique……..…

- Agissant au nom et pour le compte de..... (raison sociale **(**)** et forme juridique de la société) au capital de : .....
- Adresse du siège social de la société : .....
- Adresse du domicile élu.....
- Affiliée à la CNSS sous le n°.....(2)
- Inscrite au registre du commerce.....localité) sous le n°.....(2)
- N° de patente.....(2)(3)

En vertu des pouvoirs qui me sont conférés :

Après avoir pris connaissance du dossier de consultation concernant les prestations précisées en objet de la partie A ci-dessus ;

Après avoir apprécié à mon point de vue et sous ma responsabilité la nature et les difficultés que comportent ces prestations :

- Remets, revêtu (s) de ma signature un bordereau de prix, un détail estimatif et/ou la décomposition du montant global) établi (s) conformément aux modèles figurant au dossier de consultation ;

- M'engage à exécuter lesdites prestations conformément au cahier des prescriptions spéciales et moyennant les prix que j'ai établis moi-même, lesquels font ressortir :

Tranche ferme :

- Montant hors T.V.A. Y COMPRIS DROITS DE DOUANES : ..... (en chiffres et en lettres) ;
- Taux de la T.V.A. : **20**% ;
- Montant de la T.V.A. : ..... (en chiffres et en lettres) ;
- Montant T.V.A. comprise : ..... (en chiffres et en lettres).

Tranche conditionnelle :

- **Montant minimum :**
  - Montant annuel hors T.V.A. : ..... (en chiffres et en lettres) ;
  - Taux de la T.V.A. : **20**% ;
  - Montant de la T.V.A. : ..... (en chiffres et en lettres) ;
  - Montant annuel T.V.A. comprise : ..... (en chiffres et en lettres).

- **Montant maximum :**
  - Montant annuel hors T.V.A. : ..... (en chiffres et en lettres) ;
  - Taux de la T.V.A. : **20**% ;
  - Montant de la T.V.A. : ..... (en chiffres et en lettres) ;
  - Montant annuel T.V.A. comprise : ..... (en chiffres et en lettres).

L'Office National des Aéroports se libérera des sommes dues par lui en faisant donner crédit au compte ..... (à la trésorerie générale, bancaire, ou postal) 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 (optionnel).
2) Pour les concurrents non installés au Maroc, préciser la référence des documents équivalents et lorsque ces documents ne sont pas délivrés par leur pays d'origine, la référence à la déclaration délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits.
3) Ces mentions ne concernent que les personnes assujetties à cette obligation.

(**) La raison sociale doit être identique à celle figurant sur les statuts de la société

ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE)-TF

AO N° : 014-24-AOO

Objet : Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

item	Description	UDM	Quantité	PU HORS TVA en chiffres (*)	PT HORS TVA en chiffres
1	Audit, risk assessement et cadrage du périmètre	Forfait	1		
2	Fourniture de la solution SIEM (U=EPS)	U	5000		
3	Fourniture de la solution EDR (U=Endpoints)	U	1600		
4	Fourniture de la solution NDR (U=IP)	U	2000		
5	Mise en place de Threat intelligence	Forfait	1		
6	Installation, Configuration, Formation et Mise en service du SOC	Forfait	1		
TOTAL HORS TVA Y COMPRIS DROITS DE DOUANES (A)					
DONT MONTANT DROITS DE DOUANE					
TVA 20% (B)					
TOTAL TVA COMPRISE (A+B)					

(*) Le concurrent doit préciser le libellé de la monnaie conformément au règlement de la consultation.

ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE)-TC

AO N° : 014-24-AOO

Objet : Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Item	Désignation des prestations	Unité de mesure ou de compte	Quantité Min	Quantité Max	PU HORS TVA en chiffres (*)	Prix total Min HORS TVA Annuel en chiffres	Prix total Max HORS TVA Annuel en chiffres
1	Infogérance des services de supervision SOC (U=EPS)	U	**5 000**	**10 000**			
2	Infogérance des services de supervision EDR (U=Endpoint)	U	**1600**	**2000**			
3	Infogérance des services de supervision NDR (U=IP)	U	**2000**	**2500**			
4	Dark web monitoring	Forfait	**1**	**1**			
5	Incidense response via SOAR	Forfait	**1**	**1**			
6	Veille de vulnérabilité	Ensemble	**1**	**1**			
7	Services annexes SOC	J/H	**75**	**150**			
TOTAL ANNUEL HORS TVA							
TVA (20%)							
TOTAL ANNUEL TVA COMPRISE							

(*) Le concurrent doit préciser le libellé de la monnaie conformément au règlement de la consultation.

ANNEXE IV : TABLEAU RECAPITULATIF DES SPECIFICATIONS TECHNIQUES DES SOLUTIONS PROPOSEES

AO N° : 014-24-AOO

Objet : Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

- **Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.**

Spécification minimale demandée	Réponse du concurrent	Commentaire
Exigence globale de la Solution SIEM		
La solution ainsi que tous ces composants doivent supporter, au minimum, une moyenne soutenue de **5000 Events per Seconde** extensible à **10.000 EPS** sans changement des Serveurs/Appliance et **sans ajout de frais supplémentaires**		
La solution ne doit supprimer, ni mettre dans un cash ni dans un buffer les évènements dans le cas du dépassement de la licence 5000 EPS.		
La solution ne doit pas limiter les fonctionnalités du SIEM dans le cas du dépassement de la licence		
La solution doit pouvoir gérer **jusqu'à 10,000 EPS sans ajout de licence** supplémentaire **ni de frais supplémentaires**		
La possibilité de prédire les attaques via du machine Learning et IA		
La plateforme NextGen SIEM doit inclure ces modules de manière native et out-of-the box **sans « 3rd party » ou licence supplémentaire :**		
• SIEM		
• Host Forensics		
• Network Forensics Module		
• Files and Registry Integrity Monitoring		

• Security Analytics		
• True Big Data Indexing and Analytics Platform		
• Advanced Correlation within the same platform		
• Threat Intelligence		
Tous les modules doivent être fournis nativement à partir d'une seule solution SIEM sans recours aux solutions tierces. (Veuillez inclure des détails et des liens de documentation pour chaque module proposé)		
Démontrer la valeur out of the box de la plateforme proposée. La solution doit prendre en charge un minimum de + de 250 intégrations de vendors/technologies prêtes « sans customisation des parseurs et sans frais»). – Veuillez fournir une liste complète des 250+ intégrations disponibles		
La solution doit gérer un nombre de 200 de device et se baser sur le nombre de MPS (Message par seconde) mentionné dans l'AO		
La solution proposée ne devra pas être limitée par le nombre des collecteurs		
La licence proposée ne doit imposer aucune pénalité (blocage, suppression), ne doit réduire aucune fonctionnalité ou imposer une période de grâce si le système dépasse la licence EPS fournie et pourra continuer à fonctionner jusqu'à la capacité maximale des ressources hardware allouées. (Ne doit pas mettre en mémoire tampon, mettre en cache, réduire la visibilité ou désactiver toute fonction ou imposer une période de grâce)		
La solution proposée doit supporter la haute disponibilité entre leurs composantes		
Le concurrent doit prévoir des collecteurs pour couvrir tout le périmètre et les SI de notre organisme		
Dashboard doit avoir une seule vue globale sur l'ensemble des données collectées à travers l'ensemble des plateformes		
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 800 use cases prédéfinis (règles d'analyse) : Fournir la liste complète.		
+ de 2000 rapports prédéfinis		
La solution doit prendre en charge la multi-tenant complète et la séparation complète des données		
La solution doit prendre en charge un niveau très granulaire d'accès basé sur les rôles :		
o Autoriser différentes équipes à accéder au même appareil physique et à afficher la data liée à leur permission uniquement		
Les alarmes et recherches de la solution doivent être illimités et ne subir aucune limitation en termes de licences ou de performances hardware par exemple, limitations en nombre de CPUs.		
Hardware proposé		
Le prestataire doit proposer la plateforme hardware nécessaire à la prise en charge des exigences du CPS et qui peut etre une extension de la plateforme nutanix de l'ONDA		
Architecture		
Toutes les fonctionnalités de la solution proposée doivent être on-permise (sur site)		
L'architecture à proposer doit être All in one .		
La solution doit prendre en charge les modes de déploiement ci-dessous :		
• Standalone		
• Disaster recovery entre 2 sites		
• Haute disponibilité (avec failover automatique sans intervention de l'administrateur)		
• Une combinaison HA et Disaster Recovery		
Veuillez joindre chaque document de configuration de déploiement		
Le concurrent doit détailler l'architecture de la solution à mettre en place et les protocoles utilisés pour la collecte des logs		

L'ajout de nouveaux collecteurs ou la mise en place de nouveau agent ne doit pas engendrer de frais supplémentaires et doit être gratuite		
L'architecture proposée doit être extensible et évolutive.		
Le concurrent doit offrir une solution qui stocke toutes les données localement (sur les plateformes de notre organisme).		
Toute communication entre les composants de la solution doit être chiffrée.		
Chaque équipement Collector SIEM de la solution doit être installé sur des machines virtuelles sécurisés		
La solution proposée doit offrir la possibilité d'utiliser des sources externes pour l'authentification sécurisée des utilisateurs de la solution (ex : Active Directory…).		
La solution proposée doit tracer toutes les activités effectuées par les utilisateurs de la solution.		
La solution doit s'intégrer avec les outils de test de vulnérabilité tiers. À détailler		
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		
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.		
La solution proposée doit permettre la collecte continue des logs en cas d'interruption temporaire de la communication avec la plateforme back-end.		
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.		
La solution backend Big-Data proposée doit stocker les logs bruts et aussi les données meta-data		
La solution proposée doit fournir un stockage pour la visualisation et l'analyse des tendances à long terme		
La solution proposée doit effectuer des contrôles d'intégrité sur les journaux stockés pour une conservation à long terme.		

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		
La solution proposée doit effectuer une résolution de géolocalisation native au trafic d'adresses IP		
La solution proposée doit contextualiser les informations de l'utilisateur avec des 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.		
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		
Collecte/Regroupement/Normalisation		
La solution doit permettre de faire la collecte des données sur les événements par une voie de communication protégée		
La solution doit permettre la normalisation ou le formatage des logs en provenance des équipements non supportés		
La technologie de collecte doit prendre en charge la collecte depuis « Netflow - Jflow – Sflow-IPfix » nativement et gratuitement sans licence de flux spécifique ni licence supplémentaire ni ajout d'un boitier collecteur de flux		
La solution doit prendre en charge la synchronisation automatisée par horodatage au moyen du protocole de synchronisation réseau (NTP)		
Les collecteurs doivent avoir un espace de stockage local d'au moins 500Go en local avec protection des données (Raid)		
En cas de défaillance du collecteur assigné, les équipements/application devraient être en mesure d'envoyer les logs à un autre collecteur (si disponible) sans perte de données. Dans le cas où la connectivité avec le système de gestion SIEM est perdu, le collecteur devrait être en mesure de stocker les données dans son propre référentiel.		
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 …)		

La solution doit permettre la collecte en mode agent ou sans agent pour les différents systèmes d'exploitation (Windows, Unix…)		
La collecte d'événements doit supporter une variété de méthodes de collecte de logs, incluant : (CEF ou équivalent, OPSEC, SDEE, XML, ODBC-JDBC). À détailler		
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.		
Le collecteur de solution proposé doit prendre en charge l'équilibrage et le partage de charge automatiques		
La solution proposée doit collecter les journaux via un Agent et aussi supporter la collecte en méthode sans agent		
La solution proposée pour l'intégrité des fichiers « FIM » , doit inclure la prise en charge des plates-formes Windows et *Nix. Svp Fournissez une liste complète de tous ceux qui sont pris en charge.		
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.		
La solution proposée doit supporter la planification de l'envoie des logs, la compression et/ou le chiffrement des logs collectés en remote.		
Le collecteur de la solution proposée doit supporter un load balacing/sharing automatique.		
La solution doit être capable de dropper les « noisy logs » au niveau de la couche de collecte.		
Archive/Retention		
La solution doit prendre en charge une période de rétention de 12 mois (3 mois en ligne et 9 mois hors ligne)		
La solution proposée doit compresser les logs d'archivage		
La solution proposée doit fournir un assistant simple pour accéder aux données d'archives.		
La solution proposée doit compresser les logs d'archivage		

La solution doit permettre la sauvegarde automatique des logs archives et rapport par une solution de sauvegarde externe (DAS, NAS, SAN). À détailler		
Mise en corrélation		
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		
La solution doit être en mesure de suivre l'activité des utilisateurs et lier un individu à une action		
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		
La solution doit disposer de base de règles de corrélation prédéfinies pour les différents types d'équipements (Top Attacks, Activity by specific username, etc)		
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		
La solution doit supporter au minimum 1000 règles de corrélation out-of-the-box (fournir la liste complète des règles)		
Le prestataire est tenu de donner une liste des solutions de sécurité qui sont supporté par le SIEM (Vulnerability Management, IPS/IDS…)		
La solution proposée doit avoir la capacité de créer automatiquement des listes blanches de comportements observés (c'est-à-dire sans intervention manuelle).		
La solution proposée doit déterminer automatiquement les menaces en fonction de schémas de comportement suspects.		
La solution proposée doit avoir la capacité d'apprendre automatiquement des références comportementales ou statistiques.		
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.		

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]		
La solution doit fournir du UEBA nativement et moyennant des agents pour les utilisateurs		
La solution proposée doit pouvoir minimiser les faux positifs		
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]		
Analyse		
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		
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).		
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…		
La solution doit permettre l'évaluation du risque selon la cible		
La solution doit générer des notifications en réponse à une attaque de sécurité : Alerte sur Dashboard E-mail SYSLOG, SNMP, etc		
La solution doit être capable de détecter les menaces sur la base de la réputation		
Gestion des Incident [case Management]		
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 prevues 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.		

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.		
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.		
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.		
La solution proposée doit offrir des playbook intégrés à la plateforme sans coût additionnel.		
La solution proposée doit permettre de s'interfacer avec un système tiers de gestion de la réponse aux incidents (Remedy, etc.)		
Sauvegarde et récupération		
Le solution SIEM doit fournir une méthode simple pour sauvegarder et restaurer les données de configuration du système automatiquement et manuellement		
Traitements des logs		
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		
La solution doit garantir l'interrogation des logs normalisés en ligne avec une durée de rétention au moins de 12 mois (3 mois en ligne et 9 mois hors ligne).		
La solution doit prévoir un mécanisme de reprise des logs en cas de rupture de connexion avec un collecteur		
La solution doit être capable de garder les logs collectés avec une taille de cache de 50 Go au minimum en cas de perte de connectivité		
Une fois reçu par le collecteur, les logs bruts doivent subir les traitements minimums ci-dessous :		
o La normalisation		
o L'enrichissement		
o L'agrégation		

o Filtrage		
o Cryptage		
o Compression et 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		
La solution de bout-en-bout doit collecter, traiter, et enregistrer des informations d'une manière qui est conforme aux meilleures pratiques de gestion de journal.		
La solution doit permettre aux administrateurs d'extraire les journaux dans son format brut pour une période définit.		
Les journaux doivent être stockés dans un format chiffré afin d'assurer la sécurité des journaux de toute modification non autorisée.		
Intégration du système		
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		
- …		

La solution proposée doit prendre en charge la collecte des journaux Netflow sans appliances supplémentaires ni licence supplémentaire.		
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]		
Performance de traitement		
Le Taux de compression doit aller jusqu'à 8fois		
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		
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.		
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.		
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.		
Le concurrent doit proposer des solutions avec le hardware (serveur/matériel) nécessaire et assurer une capacité de rétention des logs minima de 12 mois (9 mois hors ligne et 3 mois en ligne). Le prestataire peut envisager la plateforme hardware sous forme d'extension de la plateforme nutanix de l'ONDA.		
Administration		
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)		
Administration centralisée depuis un point unique		
Rapport et conformité		
La solution doit fournir plus de 2000 rapports out of the box, (Fournir la liste des rapports)		

Le module de reporting doit inclure nativement les packages de conformité ci-dessous :		
o GLBA Compliance Module		
o FISMA Compliance Module		
o GPG-13 Compliance Module		
o PCI-DSS Compliance Module		
o BSI IT-Grundschutz Module		
o 201 CMR 17 Module		
o HIPAA Module		
o ISO 27001		
o NERC-CIP Module		
o ASD Module		
o SOX Module		
o HiTech Module		
o Dodi 8500.2 Module		
o NRC Module		
o NEI Module		
o CCF Module		
o GDPR Compliance Module		
o ISO Compliance Module		
Source de réputation (Threat Intelligence)		
La solution doit être fournie avec une licence basée sur la réputation (IP des botnet, adresse email de phishing, url suspect, …etc)		
La solution proposée doit intégrer les données de plusieurs flux de renseignements sur les menaces -sources gratuits- dans ses analyses avancées.		
SOAR		
La solution proposée doit automatiser la réponse aux menaces		

La solution proposée doit permettre d'ajouter des custom actions automatisée. Décrivez en détail le processus d'ajout d'une correction automatisée personnalisée.		
Le moteur SOAR proposé doit être intégré dans la plate-forme prête à l'emploi		
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.		
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		
System Dashboard et Interface		
• 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)		
• Le dashboard doit afficher les logs et alertes en temps réel		
• La solution doit donner la possibilité de créer des vues pour chaque utilisateur		
• Les différents rapports devront être consolidés et accessibles sur le Dashboard		
• La solution doit supporter le téléchargement des rapports sous plusieurs formats (PDF, CSV…)		
• La solution doit donner la possibilité de créer tout les dashboard sur la base de n'importe quel champ des logs		
Exigence globale de la Solution NDR		
La solution proposée doit utiliser plusieurs algorithmes d'intelligence artificielle ainsi que plusieurs techniques de machine learning, contenant au minimum : le deep learning, le machine learning supervisé et le machine learning non supervisé		
Utilisation de l'apprentissage automatique non supervisé de manière prédominante : La capacité du logiciel d'utiliser plusieurs techniques d'IA supervisées, non supervisées et de deep learning dans un cadre bayésien, ce qui permet de créer une protection sur mesure pour l'organisation		

Corrélation directe entre toutes les sources de données : réseau, nuage, point final, courrier électronique, SaaS, IoT : Le potentiel de protection totale des actifs numériques de l'organisation, sans intégration nécessaire avec une autre technologie de sécurité.		
Le système doit avoir la capacité de déployer des capteurs légers sur les points de terminaison pour étendre la visibilité lorsque les appareils sont déconnectés du réseau de l'entreprise sans compter sur les intégrations		
Le fournisseur doit fournir des exemples authentiques et réels d'attaques APT zero-day détectées par le système		
Le système doit disposer d'une fonction d'analyste IA capable de mener des enquêtes autonomes automatisées		
Le système doit disposer d'une fonctionnalité d'analyse de l'IA capable de mener des enquêtes à la demande		
Le système doit être en mesure de partager les rapports d'incident d'IA avec les systèmes SIEM, SOAR et SOC à l'aide d'une API externe		
Il doit s'agir d'une plateforme d'auto-apprentissage et avec une approche adaptative, qui utilise une intelligence artificielle éprouvée pour en savoir plus sur l'environnement dans lequel elle se trouve, et détecter et répondre aux écarts par rapport à l'activité normale ;		
le modèle du réseau appris par la solution doit être suffisamment dynamique pour s'adapter à tout changement de comportement de l'environnement		
Modification/création de modèles : Capacité de la solution à modifier/créer des règles comportementales sur des scénarios spécifiques - les critères d'alerting combinent des mesures de 'metric' inhabituelles (Machine Learning) et des conditions classiques: protocoles, évènement, identité...		
La solution devrait fonctionner entièrement à base d'apprentissage comportemental quand les technologies basées sur des règles et/ou des signatures ne s'appliquent pas		

La solution doit permettre une analyse continue des chemins d'attaque les plus critiques. La solution analyse le risque cyber au niveau du SI (Système d'information) plutôt qu'au niveau de l'IP ou de device (niveau d'analyse inférieur de la concurrence).		
La solution doit être capable de regrouper automatiquement les périphériques en groupes et clusters en fonction de leur similitude de comportement		
La solution doit représenter visuellement toutes les activités du réseau et les connexions entre toutes les machines et les utilisateurs (en interne et en externe). Interface 3D pour la visualisation et la lecture en temps réel, avec possibilité de revisionner les évènements passés.		
La solution doit fournir des rapports de flux de données en temps réel et des vues de tableau de bord		
La solution proposée ne doit pas partager des données internes avec le cloud de l'éditeur.		
Stockage des données : Toutes les données sont stockées on-premise sur le site du client, sans qu'il soit nécessaire de recourir à un cloud pour l'apprentissage, l'analyse ou la réponse.		
La solution doit avoir une fonctionnalité capable de permettre une analyse rétrospective des journaux de l'incident, en retournant sur l'axe temps les données de connexion à quelques secondes, minutes, heures ou jours avant qu'une certaine anomalie ait été identifiée		
La solution doit permettre la personnalisation et l'adaptation de l'apprentissage automatique aux conditions et caractéristiques spécifiques du réseau		
La solution proposée doit consommer et analyser des données/flux bruts (paquets bruts) via la mise en miroir de ports (SPAN) ou via l'utilisation d'un TAP		
La solution proposée doit être une technologie sans agent sans aucun besoin de configuration ou d'installation sur les terminaux		

La solution proposée doit prendre en charge une architecture complète et évolutive grâce à l'ajout simple de licences de composants supplémentaires nécessaires pour s'intégrer aux différents environnements numériques, y compris sur site, cloud et hybrides, prenant en charge au moins :		
a. Amazon AWS SaaS, EC2, IAM, S3, VPC et LAMBDA		
b. Microsoft Azure		
d. Bureau 365		
d. Composants virtuels (machines virtuelles)		
e. Scripts pour l'analyse des serveurs locaux (capteurs pour les systèmes d'exploitation)		
La solution proposée doit permettre la création automatique de rapports exécutifs couvrant au moins un aperçu de :		
a. le résumé complet du déploiement indiquant le nombre total d'appareils, le nombre total de sous-réseaux et la bande passante multimédia traitée		
b. un récapitulatif des failles par phase d'attaque		
c. un récapitulatif des violations d'appareils		
d. un résumé des appareils TOP violant les conditions de haute priorité		
e. un résumé des violations les plus fréquentes des principaux éléments de conformité tels que l'utilisation abusive de : USB, google drive, RDP sortant, SQL externe, entre autres		
f. un résumé TOP des appareils qui enfreignent le plus les conditions de conformité générant un risque pour l'organisation		
La technologie doit avoir sa propre application mobile disponible à la fois sur GooglePlay et AppleStore afin de permettre la gestion à distance des incidents		
La solution doit avoir la capacité d'effectuer des notifications push pour les alertes		
La solution proposée doit identifier les logiciels malveillants dans l'environnement de l'entreprise qui ont contourné les contrôles de sécurité au niveau des défenses du périmètre		

La solution proposée doit identifier l'installation de portes dérobées permettant aux utilisateurs malveillants d'accéder aux ressources du réseau interne		
La solution proposée doit pouvoir revenir sur des anomalies de comportement apparemment sans rapport pour ajouter un contexte à une violation ou à une tentative d'attaque		
La solution proposée doit détecter les problèmes de performances sur le réseau		
La solution proposée doit identifier une attaque de ransomware et doit permettre une intervention avant que les lecteurs/partages réseau mappés ne soient impactés		
La solution proposée doit détecter les sessions actives pendant une période de temps plus longue que celle acceptée, par exemple une session FTP active pendant plus de 15 heures		
La solution proposée doit identifier les attaquants utilisant des informations d'identification légitimes volées pour accéder au réseau		
La solution proposée doit pouvoir prendre des mesures autonomes pour contenir les menaces en cours, ce qui donne à l'équipe de sécurité le temps d'enquêter et de remédier au besoin. La réponse autonome doit :		
a. S'appuyer sur une compréhension de l'activité normale (comportementale) et être capable d'interrompre chirurgicalement l'activité inhabituelle uniquement		
b. Utiliser l'IA et l'apprentissage automatique comme base de réponse et non sur la base de règles et de signatures prédéfinies.		
c. Prendre des mesures proportionnées en temps réel - des interruptions spécifiques à la connexion jusqu'à la mise en quarantaine complète des appareils, soit directement, soit via des intégrations avec des pare-feu et/ou des contrôles d'accès au réseau.		
e. La réponse autonome doit pouvoir être affinée en fonction du type de comportement observé et de la gravité de l'incident.		
F. La réponse autonome doit avoir à la fois un mode humain et un mode actif, selon le niveau de visibilité que l'équipe de sécurité exige de la réponse automatique.		

g. Le système doit être capable de répondre de manière autonome à l'aide de contrôles natifs et de ne pas s'appuyer sur des intégrations. La technologie sélectionnée doit être capable de réaliser une réponse de manière totalement autonome, sans aucune intégration nécessaire avec une technologie extérieure (pare-feu, EDR, etc.). Cette réponse doit être effectuée par TCP-Reset et être suffisamment précise afin de pouvoir de réaliser en blocage indépendant en quelques secondes, et uniquement du flux (et non pas tout le poste).		
Intégrations avec l'ensemble des produits de l'editeur et hors editeur. La capacité de fournir une sécurité de bout en bout grâce à un système interconnecté de moteurs d'IA qui se répercutent dans un cycle vertueux.		
MITRE Attack : 139 techniques d'attaque couvertes pour le client utilisant toute la suite de technologie que propose l'éditeur		
Analyse Forensic : Index Advanced Search (basé sur Elastic Search) et entrepôt de fichiers PCAPS. Ces artefacts d'analyse sont générés en continu et sont disponibles indépendamment d'une détection par la solution.		
La solution doit être proposée avec le matériel nécessaire, l'extension de la plateforme nutanix peut être envisagée par le prestataire		
Le titulaire doit prendre en charge totalement le déploiement des agents sur les endpoints et autres composants du réseau		
Spécifications techniques de la solution EDR		
• La console centrale permet d'être mise en place en mode sur site (FULL On-Premise). L'interface d'administration et les données doivent être On-premise.		
• Les binaires d'installations peuvent être récupérés et intégrés dans un outil de déploiement tiers pour une installation également de manière pleinement silencieuse		
• L'installation des agents doit être réalisée et finalisée sans obligation de redémarrage des postes de travail et des serveurs		

• Un utilisateur ou administrateur du poste de travail ou du serveur ne doit pas avoir le droit de désinstaller les agents. L'administrateur de la solution EDR doit être l'unique profil habilité à désinstaller les agents		
• La solution EDR doit proposer un mode « Apprentissage » permettant d'absorber tous les usages internes et créer des règles de sécurité Zero-Trust / durcissement d'une manière automatique adaptés au contexte interne.		
• Outre les règles de sécurité Zero-Trust créées automatiquement par le mode apprentissage, la solution EDR doit intégrer par défaut des règles de durcissement permettant de (liste non exhaustive):		
• Interdire l'utilisation des outils d'administration (PSexec, PowerShel, WMI, etc) par les malwares		
• Interdire l'accès d'un processus non authentifié à la mémoire d'un autre processus		
• Protection des DLL		
• Protection des processus sensibles (lsaas, VSS, etc)		
• La solution doit proposer la possibilité de configurer des règles Zero-Trust permettant de bloquer les TTPs de la matrice MITRE.		
• La solution doit proposer des règles Zero-Trust permettant de bloquer les TTPs de la matrice MITRE ciblant les Endpoints.		
• La durée de rétention des données doit être paramétrable au niveau de la console centrale.		
• La consommation des ressources mémoires et CPU du terminal doit être faible (1% de CPU en utilisation normale, 100Mo de RAM, 100Mo de disque)		
• La consommation de la bande passante doit être faible		
• Pour un client n'ayant pas de connexion avec la console centrale, le mode offline doit assurer le même niveau de sécurité		

• L'EDR doit être capable de pleinement remplacer un antivirus classique :		
• Smart Scan		
• Analyse de binaire		
• Gestion des supports amovible		
• L'EDR doit être capable d'être désactivé sur sa fonctionnalité d'AV et travailler en binôme avec une solution antivirale conventionnelle basée sur des signatures uniquement.		
• Capacités de mise à jour transparentes des clients dans un LAN qui n'a aucun accès à internet		
• Possibilité de mettre à jour l'agent depuis la console centrale sans intervention locale ou à distance sur l'endpoint.		
• L'EDR doit alerter à minima par mail les administrateurs suite à l'identification d'un évènement malveillant.		
• L'EDR doit proposer une ségrégation par entité. La ségrégation doit être totale en termes de données ainsi qu'en terme d'administration.		
• L'EDR doit proposer une configuration permettant la délégation de l'administration par entité ou ensemble d'entités.		
• Administration / Exploitation de la console		
• Un Système de MultiFactor Authentication comme le OneTime Passwords doit être intégré dans l'EDR		
• Historique des données remontées des agents (rétention de logs) dans la console centrale sont paramétrables		
• Dans le cadre d'alertes sur de multiples agents, la console regroupe ces alertes et les agrège pour un "hunting" plus efficace		
• La solution doit proposer des API afin de permettre l'échange d'information avec d'autres solution de sécurité		

• Depuis une alerte de sécurité ou un simple événement, la solution EDR doit permettre de créer automatiquement un schéma sous forme d'arbre d'exécution incluant tous les éléments d'une attaque afin de faciliter l'investigation.		
• La console permet un soutien spécifique aux administrateurs pour faciliter la gestion des faux positifs		
• La console permet de bloquer ou autoriser certains programmes (scripts, exécutables, etc.) propres au clients		
• La solution doit permettre aux administrateurs d'appliquer des règles de sécurité dédiée aux utilisateurs nomade :		
• Limitation domaine / IP		
• Limitation sur les périphériques USB		
• Limitation de l'exécution de binaire		
• Limitation d'utilisation des support amovibles		
• La solution doit permettre d'appliquer des stratégies de sécurité différentes en fonction des machines (serveurs, users, IT, dev, prod …). Et par conséquent fournir de niveau de sécurité différents pour les applications en fonction de la stratégie.		
• L'EDR doit être capable de collecter les actions de chaque programme en temps réel (exécution, lecture, écriture, renommage, suppression, accès mémoire, accès réseau) sur la console d'administration de manière détaillée.		
• L'EDR doit permettre de mettre en place des blocages spécifiques sur des actions faites par les programmes pour limiter la surface d'attaque. (Exécution, lecture, écriture, renommage, suppression, accès mémoire, accès réseau) Exemple : empêcher l'accès réseau pour les programmes sur les clés USB.		
• L'EDR doit détecter les comportement des programmes et limiter l'utilisation des outils nécessaire aux attaques non basé sur des malware.		

• L'EDR doit permettre de récupérer toutes les informations en live sur un système :		
• User connectés		
• Hardware de chaque composants interne ou périphérique de la machine		
• Processus / service / driver en cours d'exécution		
• Observateur d'évènements / logs		
• Rapports d'erreur système		
• Programme au démarrage		
• Variables d'environnement		
• L'EDR doit permettre de récupérer la mémoire des programmes à distance afin de faire des investigation forensic		
• L'EDR doit permettre de faire du versionning des fichiers sur les disques dur, pour pouvoir les restaurer en cas de compromission, d'altération, ou suppression malveillante.		
• L'EDR doit proposer un mécanisme innovant basé sur l'intelligence artificielle (Machine learning ou Deep Learning) afin d'analyser les binaires.		
• L'EDR doit proposer une API permettant l'utilisation directe des capacités de détection de l'intelligence artificielle dans d'autres produits.		

• L'EDR doit proposer un système de monitoring des capacités Mémoire et CPU du parc afin d'identifier les malwares de type crypto-miner par exemple.		
• La solution doit permettre une gestion de vulnérabilités automatique sans lancement ou planification de scan. La gestion de vulnérabilité doit inclure les vulnérabilités applicatives et les correctifs de sécurité système (ex. KB Microsoft)		
• La solution doit permettre de lister les logiciels installés sur chaque poste.		
• La solution doit permettre de lister tous les binaires connus sur le parc protégé cet sur chaque poste.		
• L'EDR doit proposer une vue dédiée aux activités de HUNT. Cette vue doit regrouper tous les évènements (accès à la donnée, accès à la mémoire, accès réseau, etc.) générés sur le parc.		
• L'EDR doit proposer des fonctionnalités de durcissement des applicatifs installé :		
• IP ou domaines autorisés		
• Type de données autorisés		
• La solution EDR doit permettre à l'administrateur d'analyser des binaires sans les exécuter.		
• La solution EDR doit permettre à l'administrateur de créer des politiques de sécurité différentes et d'y affecter des postes de travail et/ou des serveurs.		
• La solution doit permettre la réalisation d'actions de remédiation et de « Rollback ».		
• La remédiation doit permettre le nettoyage d'un système de tous les éléments malveillants suite à une attaque.		
• Le « Rollback » doit permettre la récupération de donnée supprimées, altérées ou chiffrées suite à une attaque.		

• La solution doit proposer un panel d'actions d'investigation qui peuvent être exécutées à distance sur un ou plusieurs postes (liste non exhaustive) :		
• Dump de mémoire d'un processus		
• Récupération d'une clé de registre		
• Récupération de la liste des processus en exécution		
• Isolation de la machine		
• Eteindre la machine		
• La solution EDR doit disposer d'un outil d'aide à l'amélioration de la sécurité qui propose à l'administrateur des actions à réaliser afin d'améliorer le niveau de sécurité du parc.		
• La solution doit permettre d'avoir une visibilité sur les fichiers système et programmes afin de vérifier leur intégrité		
• La solution doit proposer une Live Map réseau permettant de visualiser les communications réseau en temps réel à l'échelle mondiale.		
• L'éditeur doit disposer d'une équipe de support technique locale (Maroc).		
• L'éditeur doit disposer d'une offre Cloud souverain basée sur des serveurs localisés sur le territoire national marocain, les logs et les données ONDA doivent etre traités au niveau de ce cloud souverain et ne doivent en aucun cas être traités ou hébergés au niveau d'un cloud extraterritorial.		
• L'éditeur doit proposer le service MDR opéré par des équipes locales au Maroc.		
• L'éditeur doit proposer des rapports périodiques contextualisé au parc de client avec des recommandations personnalisées afin de guider les équipes internes dans l'amélioration du niveau de sécurité du périmètre		
• La plateforme hardware est à la charge du prestataire et peut etre une extension de la plateforme nutanix de l'ONDA		

• Le titulaire doit prendre en charge totalement le déploiement des agents sur les endpoints (postes de travail et serveurs)		
Livrables		
Le titulaire doit produire toutes les politiques et procédures exigées dans la DNSSI et la norme ISO27001 qui sont liés aux processus de gestion des incidents de sécurité SI		
Le titulaire doit assister les équipes ONDA durant les périodes de garantie pour la mise à jour des politiques et procédures liés aux processus de gestion des incidents de sécurité SI		
Le titulaire doit produire à minima les livrables suivants :		
o Document d'exploitation		
o Document d'architecture		
o Document d'installation		
o Rapports d'activité trimestriels		
o Comptes rendu de réunion projet : Comité de suivi et comité de pilotage		
Il est demandé au titulaire de documenter tous les processus du SOC, EDR, NDR, SOAR. Cette documentation devra inclure à minima, des procédures, les modes opératoires associés, description des interactions entre ces processus et les activités SI existantes ainsi que les indicateurs de performances à surveiller. En résumé, il s'agit de produire une carte d'identité de chaque processus.		
Les différentes prestations devront être décrites, en détaillant les inputs, outputs, acteurs et étapes des traitements ainsi que les éventuels prérequis.		
Pour le processus de traitement des incidents, ce processus doit faire apparaitre, au minima, les acteurs et les actions, voire les outils.		
Deux processus sont particulièrement à documenter : le traitement d'incident détecté et remonté par la DGSSI (macert), le traitement d'incident détecté et remonté par le SOC ONDA (incident majeur ou normal).		
Licences		

Toutes les licences utilisées pour la mise en place du projet doivent être au nom de l'ONDA. L'équipe technique de l'ONDA doit être en mesure d'accéder aux plateformes éditeur pour la création de ticket support, consultation des licences, téléchargement des patchs, toute autre action nécessaire durant le cycle de vie des licences		
Le titulaire doit justifier la pérennité des solutions proposées sur une durée minimale de six (06) ans, moyennant un document livré par les éditeurs.		

ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

المكتب الوطني للمطارات
Office National Des Aéroports

CAHIER DES PRESCRIPTIONS SPECIALES

Appel d'offres ouvert N° 014-24-AOO

Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Table des matières

ENTRE :

L'OFFICE NATIONAL DES AEROPORTS, désigné ci-après, par le sigle « O.N.D.A », représenté par sa Directrice Générale, faisant élection de domicile à l'Aéroport CASABLANCA Mohammed V - Nouasseur.

d'u ne part

ET :
(Titulaire)
Faisant élection de domicile à
Inscrite au Registre de Commerce de sous le n°
Affiliée à la CNSS sous le n°
Représentée par _____ en vertu des pouvoirs qui lui sont conférés,

D'autre part,

CAHIER DES PRESCRIPTIONS SPECIALES

CHAPITRE 1 : CLAUSES ADMINISTRATIVES

ARTICLE 01 : OBJET DU MARCHE

Le présent marché a pour objet : **Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence :**

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tel que décrits dans les Chapitre 2 et 3 (clauses techniques) du présent Cahier des Prescriptions Spéciales.

ARTICLE 02 : MODE DE PASSATION DU MARCHE

Le présent marché est passé en application des dispositions de **l'alinéa 2, paragraphe 1 de l'article 16 et de l'alinéa 3, paragraphe 3 de l'article 17** du règlement relatif aux marchés publics de l'Office National des Aéroports en vigueur.

ARTICLE 03 : TYPE DU MARCHE

Le présent marché est un marché à tranche conditionnelle pour lequel il est prévu une tranche ferme couverte par un crédit budgétaire disponible et que le prestataire est certain de réaliser, et une tranche conditionnelle dont l'exécution est subordonnée par la disponibilité du crédit budgétaire et à la notification de l'ordre de service prescrivant le commencement, dans les délais prévus par le présent marché.

ARTICLE 04 : DECOMPOSITION EN TRANCHES

Le présent marché comporte une tranche ferme et une tranche conditionnelle.

Les prestations de la tranche ferme concernent l' **« Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Treath intelligence ».**

Les prestations de la tranche conditionnelle concernent l' **« Infogérance des solution de cybersécurité SIEM, EDR, NDR et Treath intelligence. ».**

ARTICLE 05 : INDEMNITES

5.1 Indemnité de dédit : en cas de renonciation par le maître d'ouvrage à réaliser la tranche conditionnelle, il ne sera pas versé d'indemnité de dédit au prestataire.
5.2 Indemnité d'attente : Lorsque l'ordre de service afférent à la tranche conditionnelle n'a pu être donné dans les délais prescrit dans le présent marché, aucune indemnité d'attente ne sera versée au titulaire. Néanmoins, le titulaire a le droit de demander la résiliation de la tranche conditionnelle au cas où la notification de l'ordre de service de commencement dépassera **trois (3) mois** suivant la date prévue de commencement.

ARTICLE 06 : PIECES CONSTITUTIVES DU MARCHE

Les pièces constitutives du présent marché sont :

1) L'acte d'engagement ;
2) Le présent cahier des prescriptions spéciales (CPS) ;

3) Le Bordereau Des Prix – Détail Estimatif : (BDP-DE) ;
4) Les pièces constitutives de l'offre technique ;
5) Le CCAG-T pour **la tranche ferme** ;
6) Le CCAG-EMO pour la **tranche conditionnelle**.

ARTICLE 07 : CONNAISSANCE DU DOSSIER

Les spécifications et les prescriptions techniques relatives aux prestations à réaliser sont contenues dans le présent marché, l'entrepreneur déclare :

- Avoir pris pleine connaissance de l'ensemble des prestations ;
- Avoir fait préciser tous points susceptibles de contestations ;
- Avoir fait tous calculs et sous détails ;
- N'avoir rien laissé au hasard pour déterminer le prix de chaque nature de prestations présentées par elle et pouvant donner lieu à discussion.
- Avoir apprécié toutes les difficultés qui pourraient se présenter lors de l'exécution des prestations objet du présent marché et pour lesquelles aucune réclamation ne sera prise en considération.

ARTICLE 08 : REFERENCES AUX TEXTES GENERAUX

Le présent marché est soumis aux prescriptions relatives aux marchés publics notamment celles définies par :

- Le règlement relatif aux marchés publics de l'Office National des Aéroports approuvé le 09 Juillet 2014 et la décision de son amendement réf 01/RM/2015 du 02 avril 2015 ;
- Le décret N° 2-14-394 du 6 Chaabane 1437 (13 Mai 2016) approuvant le cahier des clauses administratives générales, applicables aux marchés de travaux exécutés pour le compte de l'Etat, pour les prestations à réaliser dans le cadre de **la tranche ferme** du présent marché ;
- Le décret N° 2-01-2332 du 22 Rabii I 1423 (04 juin 2002) approuvant le cahier des clauses administratives générales, applicables aux marchés d'études et de maîtrises d'œuvres (CCAG EMO) exécutés pour le compte de l'Etat, pour les prestations à réaliser dans le cadre de **la tranche conditionnelle** du présent marché ;
- Tous les textes législatifs et règlementaires concernant l'emploi et les salaires de la main d'œuvre ;
- Les lois et règlements en vigueur au Maroc à la date de la signature du présent marché.

Bien que non jointes au présent CPS, le titulaire est réputé connaître tous textes ou documents techniques applicables au présent marché. Le titulaire ne peut se prévaloir dans l'exercice de sa mission d'une quelconque ignorance de ces textes et, d'une manière générale, de toute la réglementation intéressant les prestations en question.

ARTICLE 09 : RESILIATION

Dans le cas où le titulaire aurait une activité insuffisante ou en cas de la non-exécution des clauses du présent marché, l'Office National Des Aéroports le mettrait en demeure de satisfaire à ses obligations, si la cause qui a provoqué la mise en demeure subsiste, le marché pourra être résilié sans aucune indemnité sous peine d'appliquer les mesures coercitives

prévues par les articles 79 et 80 du CCAG-T et/ou par l'article 52 du CCAG-EMO selon la tranche concernée du présent marché.

L'ONDA se réserve le droit de résilier le marché dans le cas de modifications importantes ne pouvant être prises en charge dans le cadre du présent marché conformément à la réglementation en vigueur.

ARTICLE 10 : DOMICILE DU PRESTATAIRE

L'entrepreneur est tenu d'élire domicile au Maroc qu'il doit indiquer dans l'acte d'engagement ou le faire connaître au maître d'ouvrage dans le délai de quinze (15) jours à partir de la notification, qui lui est faite, de l'approbation de son marché en application des dispositions de l'article 136 du règlement relatif aux marchés publics de l'Office National des Aéroports en vigueur.

Faute par lui d'avoir satisfait à cette obligation, toutes les notifications qui se rapportent au marché sont valables lorsqu'elles ont été faites au siège de l'entreprise dont l'adresse est indiquée dans le présent marché.

En cas de changement de domicile, l'entrepreneur est tenu d'en aviser le maître d'ouvrage, par lettre recommandée avec accusé de réception, dans les quinze (15) jours suivant la date d'intervention de ce changement.

ARTICLE 11 : REGLEMENT DES DIFFERENDS

Tout litige entre l'Office National Des Aéroports et le prestataire sera soumis aux tribunaux compétents de Casablanca « MAROC ».

ARTICLE 12 : CAS DE FORCE MAJEURE

En cas de survenance d'un événement de force majeure, les dispositions applicables sont celles définies par l'article 47 du C.C.A.G.T pour les prestations à réaliser dans le cadre de **la tranche ferme** du présent marché et l'article 32 du CCAG-EMO pour les prestations à réaliser dans le cadre de **la tranche conditionnelle** dudit marché.

ARTICLE 13 : ENTREE EN VIGUEUR ET APPROBATION

L'entrée en vigueur du présent marché interviendra après son approbation par l'autorité compétente, le visa du Contrôleur d'Etat si le visa est requis et la notification au titulaire.

ARTICLE 14 : NANTISSEMENT

En cas de nantissement, les dispositions applicables sont celles prévues par la loi n° 112-13 relative au nantissement des marchés publics promulguée par le Dahir n°1-15-05 du 29 rabii II 1436 (19 février 2015).

En vue de l'établissement de l'acte de nantissement, le maître d'ouvrage remet au titulaire du marché, sur demande et sans frais, une copie du marché portant la mention « EXEMPLAIRE UNIQUE » dûment signée et indiquant que ladite copie est délivrée en unique exemplaire destiné à former titre pour le nantissement du marché, et ce conformément aux dispositions de l'article 4 de la loi n°112-13 susmentionnée.

Le responsable habilité à fournir au titulaire du marché ainsi qu'au bénéficiaire du nantissement ou de subrogation les renseignements et les états prévus à l'article 8 de la loi n° 112-13 est le Directeur ou la Directrice Général(e) de l'ONDA.

Le Directeur ou la Directrice Général(e) de l'ONDA et le Trésorier Payeur de l'ONDA sont seuls habilités à effectuer les paiements au nom de l'ONDA entre les mains du bénéficiaire du nantissement ou de la subrogation, conformément à la législation et à la réglementation en vigueur.

ARTICLE 15 : FORMALITE D'ENREGISTREMENT

Le titulaire s'engage à présenter le présent marché à la formalité d'enregistrement dans un délai de **30 jours** à compter de la date de la notification de son approbation conformément à la réglementation en vigueur. L'original du marché enregistré sera conservé par l'Office National Des Aéroports.

ARTICLE 16 : DROIT APPLICABLE

Le marché sera interprété conformément au droit Marocain

ARTICLE 17 : DROITS ET TAXES

Les prix du présent marché s'entendent Toutes Taxes Comprises Delivered Duty Paid (TTC DDP).

Le prestataire (Entrepreneur, fournisseur ou prestataire de service) est réputé avoir parfaitement pris connaissance de la législation fiscale en vigueur au Maroc. Par conséquent, il supportera, par défaut, tous les impôts et taxes dont il est redevable au Maroc, y compris la TVA, tous droits de douane, de port ou autres.

Les **prestations de service** réalisées pour le compte de l'ONDA par une entreprise non résidente sont soumises à l'impôt sur les sociétés au taux de **10%** de ces prestations. Cet impôt est prélevé du montant desdites prestations sous forme de retenue à la source. **Une copie de l'attestation du versement** de cet impôt sera remise au prestataire, à sa demande.

Pour les entreprises originaires de pays ayant signé avec le Maroc une convention destinée à éviter les doubles impositions, la retenue à la source est déductible des impôts dus dans leur pays d'origine.

Pour les prestations à réaliser dans le cadre de la tranche ferme, l'ONDA prendra en charge le paiement des impôts et taxes à l'importation y compris les droits et accessoires de douane et la TVA à l'importation **figurant sur la fiche de liquidation émise par les services de la douane**, **hors** les frais de la logistique (Transitaire, emmagasinage et surestaries le cas échéant) qui restent à la charge du prestataire y compris la gestion de la logistique d'importation.

Dans le cas où le Cahier des Prescriptions Spéciales prévoit le paiement par lettre de crédit et le prestataire opterait pour ce mode de paiement, le montant des droits et taxes en question sera déduit du montant du CREDOC.

Si l'ONDA paierait des frais supplémentaires, pour quelle que raison que ce soit, à cause d'un motif imputable au fournisseur, l'ONDA déduira d'office lesdits frais des sommes dues au fournisseur.

Aussi, en cas de déclaration douanière faisant ressortir des montants supérieurs à ceux indiqués au présent Marché, le supplément de droits et taxes de douane résultant de cette différence de déclaration sera à la charge du Fournisseur.

En cas d'augmentation des sommes à valoir pour la couverture des droits de douane et taxes à l'importation, l'ONDA prendra les engagements complémentaires nécessaires pour couvrir lesdites sommes, conformément à la réglementation en vigueur.

CHAPITRE 2 : CLAUSES TECHNIQUES – Tranche ferme

ARTICLE 01 : MAITRE D'OEUVRE

Le maitre d'œuvre de la tranche ferme du présent marché est la **Direction Des Systèmes D'information.**

ARTICLE 02 : GARANTIE PARTICULIERE

Le Prestataire garantit que toutes les fournitures livrées en exécution du marché sont neuves, n'ont jamais été utilisées, sont du modèle le plus récent en service et incluent toutes les dernières améliorations en matière de conception et de matériaux, sauf si le marché en a disposé autrement. Le fournisseur garantit en outre que les fournitures livrées en exécution du marché n'auront aucune défectuosité due à leur conception, aux matériaux utilisés ou à leur mise en œuvre (sauf dans la mesure où la conception ou le matériau est requis par les spécifications du Maître d'Ouvrage) ou à tout acte ou omission du fournisseur, survenant pendant l'utilisation normale des fournitures livrées dans les conditions prévalant dans le pays de destination finale.
Le Maître d'ouvrage notifiera au prestataire par écrit toute réclamation faisant jouer cette garantie.
A la réception d'une telle notification, le prestataire, dans un délai de trois (03) semaines, remplacera les fournitures non conformes sans frais pour le maître d'ouvrage.
Si le prestataire, après notification, manque à se conformer à la notification du maître d'ouvrage, dans un délai de deux (02) semaines, ce dernier applique les mesures coercitives nécessaires, aux risques et frais du fournisseur et sans préjudice de tout autre recours de l'acquéreur contre le fournisseur en application des clauses du marché.

ARTICLE 03 : CONTROLE ET VERIFICATION

L'ONDA aura le droit de contrôler et/ou d'essayer les fournitures pour s'assurer qu'elles sont bien conformes au marché. L'ONDA notifiera par écrit au fournisseur l'identité de ses représentants à ces fins.

Si l'une quelconque des fournitures contrôlées ou essayées se révèle non conforme aux spécifications, l'ONDA la refuse ; le titulaire devra alors remplacer les fournitures refusées sans aucun frais supplémentaire pour l'ONDA.

Le droit de l'ONDA de vérifier, d'essayer et, lorsque cela est nécessaire, de refuser les fournitures ne sera en aucun cas limité, et l'ONDA n'y renoncera aucunement du fait que lui-même ou son représentant les aura antérieurement inspectées, essayées et acceptées.

Rien de ce qui est stipulé dans cet article ne libère le titulaire de toute obligation de garantie ou autre, à laquelle il est tenu au titre du présent marché.

ARTICLE 04 : DELAI D'EXECUTION

La présente tranche ferme du marché est valable pour une durée globale de **Huit (08) mois** à compter de la date de l'ordre de service prescrivant le commencement des prestations.

ARTICLE 05 : PENALITES POUR RETARD

A défaut par l'Entrepreneur d'avoir exécuté à temps la tranche ferme du marché ou d'avoir respecté tout planning ou délai prévu par la présente tranche ferme du marché, il lui sera appliqué sans préjudice de l'application des mesures prévues par les articles 79 et 80 du

CCAGT, une pénalité de **cinq pour mille** (**5 ‰)** du montant initial de la présente tranche ferme marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux, par jour de retard.

1- **En cas de retard dans l'exécution des travaux :** Par application de l'article 65 du CCAGT la pénalité est plafonnée à huit pour Cent (8 %) du montant de la tranche ferme du marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux ; au-delà de ce plafond, l'O.N.D.A. se réserve le droit de procéder à la résiliation du marché sans préjudice des mesures coercitives prévues par les articles 79 et 80 C.C.A.G.T.

2- **En cas de retard dans la remise des documents ou rapports ou pour défaut de réalisation de certaines de ses obligations :** Par application de l'article 66 du CCAGT la pénalité est plafonnée à deux pour Cent (2 %) du montant de la tranche ferme du marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux.

Les sommes concernant les pénalités seront déduites des décomptes de l'entreprise sans qu'il ne soit nécessaire d'une mise en demeure préalable.

ARTICLE 06 : CAUTIONNEMENT DEFINITIF - RETENUE DE GARANTIE

a) **Cautionnement** : Le cautionnement définitif est fixé à Trois pour cent (3%) du montant initial de la tranche ferme du marché arrondi au dirham supérieur conformément aux dispositions de l'article 15 du C.C.A.G.T

b) **Retenue de garantie** : Les Dispositions relatives à la retenue de garantie telles que définies aux articles 16 et 64 du C.C.A.G.T sont seules applicables.

Toutes les cautions présentées sous forme de cautions personnelles et solidaires doivent contenir la mention « à première demande de l'ONDA » et être émises par un organisme marocain agréé.

ARTICLE 07 : DELAI ET NATURE DE GARANTIE

I. DELAI DE LA GARANTIE

Le délai de garantie est fixé à **trente-six (36) mois** à compter de la date de la réception provisoire globale de la tranche ferme du marché. Durant la période de garantie, le Prestataire est soumis aux dispositions arrêtées par l'article 75 du CCAGT. **Cette garantie couvre aussi bien le support logiciel, l'assistance, l'intervention sur site, les pièces de rechanges que la main d'œuvre**.

II. NATURE DE LA GARANTIE

Pendant le délai de garantie, le prestataire sera tenu, de procéder aux rectifications qui lui seraient demandées en cas de mauvaise qualité, anomalies ou défectuosités constatées, sans pour autant que ces prestations supplémentaires puissent donner lieu à des frais supplémentaires.

La garantie consentie s'applique à toute défectuosité ou déficience qui se révèle pendant l'utilisation normale du matériel/logiciel livré, dans les conditions et l'environnement prévalant lors de son exploitation et qui n'est pas imputable à une fausse manœuvre, à une faute de conduite ou à un manque de surveillance et d'entretien du matériel et logiciel.

Au titre de cette garantie, le Titulaire s'engage durant la période de garantie à :

- Maintenir gratuitement en bon état de fonctionnement le matériel/logiciel livré ;
- Introduire à ses frais les modifications, réglages et mises au point nécessaires pour que le matériel/logiciel soit conforme aux normes de performance et de productivité prévues dans le présent marché et procéder aux essais de contrôle y afférents ;
- Remplacer à titre gratuit, par un matériel identique à celui reconnu défectueux lorsque sa remise en état nécessite un délai de réparation dépassant une semaine, à compter de la date de son identification, ou si celle-ci n'est tout simplement pas possible.

La garantie technique est totale. Elle couvre tous les frais nécessaires à la réparation et au remplacement des pièces de rechange ou du matériel défectueux et les mises à jour logicielles. Elle englobe en outre les frais de main d'œuvre et de déplacement du personnel d'entretien ainsi que le frais de démontage/remontage, emballage et transport du matériel, nécessités par leur remise en état, qu'il soit procédé à ces opérations sur le lieu d'utilisation du matériel ou que le titulaire ait obtenu qu'il soit renvoyé dans ses locaux.

ARTICLE 08 : RECEPTION PROVISOIRE

La réception provisoire sera prononcée après l'achèvement des livraisons et tests nécessaires de tous les Items comme détaillé dans le bordereau des prix.

Le prestataire est tenu de procéder à ses frais à tous les travaux nécessaires pour remédier aux essais non concluants et ce, dans les limites du délai d'exécution contractuel.

Un Procès-verbal de réception provisoire globale sera établi par les personnes habilitées de l'ONDA dès que toutes les vérifications et tests auront été déclarés satisfaisants et après achèvement des travaux de réalisation du dernier aéroport conformément aux dispositions définies par l'article 73 du CCAGT.

ARTICLE 09 : RECEPTION DEFINITIVE

La réception définitive de la tranche ferme du marché sera prononcée dans un délai de **trente-six (36) mois** à compter de la date de réception provisoire globale conformément aux dispositions définies par l'article 76 du CCAGT.

ARTICLE 10 : MODALITES DE PAIEMENT

L'ONDA se libérera des sommes dues en exécution du présent marché en faisant donner crédit au compte ouvert au nom du prestataire indiqué sur l'acte d'engagement.
Les réceptions et paiements partiels sont autorisés.

Les paiements seront effectués par virement bancaire ou par une lettre de crédit irrévocable et confirmée par la banque du fournisseur.

Si le prestataire opte pour le paiement par lettre de crédit, tous les frais et accessoires relatifs à l'ouverture de la lettre de crédit sont à la charge du fournisseur.

Lorsque le règlement n'est pas prévu par lettre de crédit, le paiement des sommes dues est effectué dans un délai maximum de quatre-vingt-dix jours (90) à compter de la date de réception des prestations demandées sur présentation de factures en cinq exemplaires.

ARTICLE 11 : BREVETS

Le prestataire garantira le maître d'ouvrage contre toute réclamation de la tierce relative à la contrefaçon ou à l'exploitation non autorisée d'une marque commerciale ou de droit de création industrielle résultant de l'emploi des fournitures ou d'un de leurs éléments.

ARTICLE 12 : NORMES

Les fournitures livrées en exécution du présent marché doivent être conformes aux normes Marocaines ou autres normes applicables au Maroc en vertu d'accords internationaux fixées aux prescriptions et spécifications techniques du présent marché ou à des normes internationales en cas d'absence desdites normes.

ARTICLE 13 : NATURE DES PRESTATIONS ET REVISION DES PRIX

Le présent marché est un marché de **fourniture** dont les prix applicables sont fermes et non révisables.

ARTICLE 14 : DESCRIPTION DU PROJET

1. INTRODUCTION

Dans le cadre de son plan de renforcement de la plateforme de sécurité SI, l'office national des aéroports (ONDA) lance la deuxième brique de la mise à niveau de sa plateforme de sécurité centrale.

Elle concerne la refonte et mise à niveau du SOC.

L'ONDA en tant qu'infrastructure d'importance vitale (IIV), applique en priorité la directive nationale de sécurité des systèmes d'information (DNSSI V2) et est régi par un ensemble de règles qui définissent et précisent les objectifs de sécurité à atteindre et qui se déclinent en organisations et moyens techniques. Parmi ces règles, on distingue :

- Les contraintes réglementaires liées au domaine aéroportuaire.
- Les contraintes des réglementations internationales et nationales.
- L'obligation de localisation des données
- L'obligation de notification d'incidents.
- La conformité à la loi 05/20 relative à la cyber sécurité

Pour cela, la mise en place d'un SOC est un élément important de plateforme de sécurité SI, il consiste à surveiller, détecter, analyser et qualifier les évènements de sécurité.

Les missions de la mise en place du SOC se déclinent en 3 activités majeures pouvant être gérées indépendamment :

1. Supervision/Qualification/Alerting ;
2. Pilotage des incidents de bout en bout ;

3. Traitement standardisé d'un incident.

En complément de ces missions principales, le SOC a la charge de conserver les journaux d'activité (ou logs) qui lui sont remontés pour la durée qui a été définie. Cette mission est essentielle pour permettre des analyses forensic à postériori ainsi que la production de rapports et statistiques à valeur ajoutée.

Description du projet :

Le présent appel d'offre concerne la refonte et la mise en place d'un SOC de nouvelle génération avec toutes les fonctionnalités nécessaires de sécurisation de la plateforme ONDA et a pour objectifs :

- La mise en place des solutions SIEM, NDR et EDR
- L'amélioration de la qualité et la quantité de collecte
- L'amélioration de la durée de rétention
- La définition des uses cases
- La réponse à de nouveaux besoins réels (Use Cases) via des rapports spécifiques et règles de corrélation avancées
- La fourniture des vues en termes de conformité par rapport aux normes et standard en vigueur
- L'accompagnement de l'ONDA dans l'élaboration des procédures et processus SOC

1. PARTIE 1 : MISE EN PLACE DES SOLUTIONS SIEM, NDR ET EDR

1.1. **Caractéristiques des produits SIEM, NDR et EDR :**

Spécification minimale demandée
Exigence globale de la Solution SIEM
La solution ainsi que tous ces composants doivent supporter, au minimum, une moyenne soutenue de **5000 Events per Seconde** extensible à **10.000 EPS** sans changement des Serveurs/Appliance et **sans ajout de frais supplémentaires**
La solution ne doit supprimer, ni mettre dans un cash ni dans un buffer les évènements dans le cas du dépassement de la licence 5000 EPS.
La solution ne doit pas limiter les fonctionnalités du SIEM dans le cas du dépassement de la licence
La solution doit pouvoir gérer **jusqu'à 10,000 EPS sans ajout de licence** supplémentaire **ni de frais supplémentaires**
La possibilité de prédire les attaques via du machine Learning et IA
La plateforme NextGen SIEM doit inclure ces modules de manière native et out-of-the box **sans « 3rd party » ou licence supplémentaire :** • SIEM • Host Forensics

• Network Forensics Module • Files and Registry Integrity Monitoring • Security Analytics • True Big Data Indexing and Analytics Platform • Advanced Correlation within the same platform • Threat Intelligence Tous les modules doivent être fournis nativement à partir d'une seule solution SIEM sans recours aux solutions tierces. (Veuillez inclure des détails et des liens de documentation pour chaque module proposé)
Démontrer la valeur out of the box de la plateforme proposée. La solution doit prendre en charge un minimum de + de 250 intégrations de vendors/technologies prêtes « sans customisation des parseurs et sans frais»). – Veuillez fournir une liste complète des 250+ intégrations disponibles La solution doit gérer un nombre de 200 de device et se baser sur le nombre de MPS (Message par seconde) mentionné dans l'AO
La solution proposée ne devra pas être limitée par le nombre des collecteurs
La licence proposée ne doit imposer aucune pénalité (blocage, suppression), ne doit réduire aucune fonctionnalité ou imposer une période de grâce si le système dépasse la licence EPS fournie et pourra continuer à fonctionner jusqu'à la capacité maximale des ressources hardware allouées. (Ne doit pas mettre en mémoire tampon, mettre en cache, réduire la visibilité ou désactiver toute fonction ou imposer une période de grâce)
La solution proposée doit supporter la haute disponibilité entre leurs composantes
Le concurrent doit prévoir des collecteurs pour couvrir tout le périmètre et les SI de notre organisme
Dashboard doit avoir une seule vue globale sur l'ensemble des données collectées à travers l'ensemble des plateformes
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 800 use cases prédéfinis (règles d'analyse) : Fournir la liste complète. + de 2000 rapports prédéfinis
La solution doit prendre en charge la multi-tenant complète et la séparation complète des données
La solution doit prendre en charge un niveau très granulaire d'accès basé sur les rôles : o Autoriser différentes équipes à accéder au même appareil physique et à afficher la data liée à leur permission uniquement
Les alarmes et recherches de la solution doivent être illimités et ne subir aucune limitation en termes de licences ou de performances hardware par exemple, limitations en nombre de CPUs.
Hardware proposé

Le prestataire doit proposer la plateforme hardware nécessaire à la prise en charge des exigences du CPS et qui peut etre une extension de la plateforme nutanix de l'ONDA
Architecture
Toutes les fonctionnalités de la solution proposée doivent être on-permise (sur site)
L'architecture à proposer doit être All in one .
La solution doit prendre en charge les modes de déploiement ci-dessous : • Standalone • Disaster recovery entre 2 sites • Haute disponibilité (avec failover automatique sans intervention de l'administrateur) • Une combinaison HA et Disaster Recovery Veuillez joindre chaque document de configuration de déploiement
Le concurrent doit détailler l'architecture de la solution à mettre en place et les protocoles utilisés pour la collecte des logs
L'ajout de nouveaux collecteurs ou la mise en place de nouveau agent ne doit pas engendrer de frais supplémentaires et doit être gratuite
L'architecture proposée doit être extensible et évolutive.
Le concurrent doit offrir une solution qui stocke toutes les données localement (sur les plateformes de notre organisme).
Toute communication entre les composants de la solution doit être chiffrée.
Chaque équipement Collector SIEM de la solution doit être installé sur des machines virtuelles sécurisés
La solution proposée doit offrir la possibilité d'utiliser des sources externes pour l'authentification sécurisée des utilisateurs de la solution (ex : Active Directory…).
La solution proposée doit tracer toutes les activités effectuées par les utilisateurs de la solution.
La solution doit s'intégrer avec les outils de test de vulnérabilité tiers. À détailler
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
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.
La solution proposée doit permettre la collecte continue des logs en cas d'interruption temporaire de la communication avec la plateforme back-end.
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.
La solution backend Big-Data proposée doit stocker les logs bruts et aussi les données meta-data
La solution proposée doit fournir un stockage pour la visualisation et l'analyse des tendances à long terme
La solution proposée doit effectuer des contrôles d'intégrité sur les journaux stockés pour une conservation à long terme.
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

La solution proposée doit effectuer une résolution de géolocalisation native au trafic d'adresses IP
La solution proposée doit contextualiser les informations de l'utilisateur avec des 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.
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
Collecte/Regroupement/Normalisation
La solution doit permettre de faire la collecte des données sur les événements par une voie de communication protégée
La solution doit permettre la normalisation ou le formatage des logs en provenance des équipements non supportés
La technologie de collecte doit prendre en charge la collecte depuis « Netflow - Jflow – Sflow-IPfix » nativement et gratuitement sans licence de flux spécifique ni licence supplémentaire ni ajout d'un boitier collecteur de flux
La solution doit prendre en charge la synchronisation automatisée par horodatage au moyen du protocole de synchronisation réseau (NTP)
Les collecteurs doivent avoir un espace de stockage local d'au moins 500Go en local avec protection des données (Raid)
En cas de défaillance du collecteur assigné, les équipements/application devraient être en mesure d'envoyer les logs à un autre collecteur (si disponible) sans perte de données. Dans le cas où la connectivité avec le système de gestion SIEM est perdu, le collecteur devrait être en mesure de stocker les données dans son propre référentiel.
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 …)
La solution doit permettre la collecte en mode agent ou sans agent pour les différents systèmes d'exploitation (Windows, Unix…)
La collecte d'événements doit supporter une variété de méthodes de collecte de logs, incluant : (CEF ou équivalent, OPSEC, SDEE, XML, ODBC-JDBC). À détailler
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.
Le collecteur de solution proposé doit prendre en charge l'équilibrage et le partage de charge automatiques
La solution proposée doit collecter les journaux via un Agent et aussi supporter la collecte en méthode sans agent
La solution proposée pour l'intégrité des fichiers « FIM » , doit inclure la prise en charge des plates-formes Windows et *Nix. Svp Fournissez une liste complète de tous ceux qui sont pris en charge.
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.
La solution proposée doit supporter la planification de l'envoie des logs, la compression et/ou le chiffrement des logs collectés en remote.

Le collecteur de la solution proposée doit supporter un load balacing/sharing automatique.
La solution doit être capable de dropper les « noisy logs » au niveau de la couche de collecte.
Archive/Retention
La solution doit prendre en charge une période de rétention de 12 mois (3 mois en ligne et 9 mois hors ligne)
La solution proposée doit compresser les logs d'archivage
La solution proposée doit fournir un assistant simple pour accéder aux données d'archives.
La solution proposée doit compresser les logs d'archivage
La solution doit permettre la sauvegarde automatique des logs archives et rapport par une solution de sauvegarde externe (DAS, NAS, SAN). À détailler
Mise en corrélation
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
La solution doit être en mesure de suivre l'activité des utilisateurs et lier un individu à une action
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
La solution doit disposer de base de règles de corrélation prédéfinies pour les différents types d'équipements (Top Attacks, Activity by specific username, etc)
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
La solution doit supporter au minimum 1000 règles de corrélation out-of-the-box (fournir la liste complète des règles)
Le prestataire est tenu de donner une liste des solutions de sécurité qui sont supporté par le SIEM (Vulnerability Management, IPS/IDS…)
La solution proposée doit avoir la capacité de créer automatiquement des listes blanches de comportements observés (c'est-à-dire sans intervention manuelle).
La solution proposée doit déterminer automatiquement les menaces en fonction de schémas de comportement suspects.
La solution proposée doit avoir la capacité d'apprendre automatiquement des références comportementales ou statistiques.
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.
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]
La solution doit fournir du UEBA nativement et moyennant des agents pour les utilisateurs
La solution proposée doit pouvoir minimiser les faux positifs
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]

Analyse
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
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).
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…
La solution doit permettre l'évaluation du risque selon la cible
La solution doit générer des notifications en réponse à une attaque de sécurité : Alerte sur Dashboard E-mail SYSLOG, SNMP, etc
La solution doit être capable de détecter les menaces sur la base de la réputation
Gestion des Incident [case Management]
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 prevues 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.
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.
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.
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.
La solution proposée doit offrir des playbook intégrés à la plateforme sans coût additionnel.
La solution proposée doit permettre de s'interfacer avec un système tiers de gestion de la réponse aux incidents (Remedy, etc.)
Sauvegarde et récupération
Le solution SIEM doit fournir une méthode simple pour sauvegarder et restaurer les données de configuration du système automatiquement et manuellement
Traitements des logs
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
La solution doit garantir l'interrogation des logs normalisés en ligne avec une durée de rétention au moins de 12 mois (3 mois en ligne et 9 mois hors ligne).
La solution doit prévoir un mécanisme de reprise des logs en cas de rupture de connexion avec un collecteur
La solution doit être capable de garder les logs collectés avec une taille de cache de 50 Go au minimum en cas de perte de connectivité
Une fois reçu par le collecteur, les logs bruts doivent subir les traitements minimums ci-dessous : o La normalisation

o L'enrichissement o L'agrégation o Filtrage o Cryptage o Compression et 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
La solution de bout-en-bout doit collecter, traiter, et enregistrer des informations d'une manière qui est conforme aux meilleures pratiques de gestion de journal.
La solution doit permettre aux administrateurs d'extraire les journaux dans son format brut pour une période définit.
Les journaux doivent être stockés dans un format chiffré afin d'assurer la sécurité des journaux de toute modification non autorisée.
Intégration du système
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 - …
La solution proposée doit prendre en charge la collecte des journaux Netflow sans appliances supplémentaires ni licence supplémentaire.
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]
Performance de traitement
Le Taux de compression doit aller jusqu'à 8fois
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
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.

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.
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. Le concurrent doit proposer des solutions avec le hardware (serveur/matériel) nécessaire et assurer une capacité de rétention des logs minima de 12 mois (9 mois hors ligne et 3 mois en ligne). Le prestataire peut envisager la plateforme hardware sous forme d'extension de la plateforme nutanix de l'ONDA.
Administration
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)
Administration centralisée depuis un point unique
Rapport et conformité
La solution doit fournir plus de 2000 rapports out of the box, (Fournir la liste des rapports)
Le module de reporting doit inclure nativement les packages de conformité ci-dessous : o GLBA Compliance Module o FISMA Compliance Module o GPG-13 Compliance Module o PCI-DSS Compliance Module o BSI IT-Grundschutz Module o 201 CMR 17 Module o HIPAA Module o ISO 27001 o NERC-CIP Module o ASD Module o SOX Module o HiTech Module o Dodi 8500.2 Module o NRC Module o NEI Module o CCF Module o GDPR Compliance Module o ISO Compliance Module
Source de réputation (Threat Intelligence)
La solution doit être fournie avec une licence basée sur la réputation (IP des botnet, adresse email de phishing, url suspect, …etc)
La solution proposée doit intégrer les données de plusieurs flux de renseignements sur les menaces -sources gratuits- dans ses analyses avancées.
SOAR
La solution proposée doit automatiser la réponse aux menaces

La solution proposée doit permettre d'ajouter des custom actions automatisée. Décrivez en détail le processus d'ajout d'une correction automatisée personnalisée.
Le moteur SOAR proposé doit être intégré dans la plate-forme prête à l'emploi
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.
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
System Dashboard et Interface
• 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)
• Le dashboard doit afficher les logs et alertes en temps réel
• La solution doit donner la possibilité de créer des vues pour chaque utilisateur
• Les différents rapports devront être consolidés et accessibles sur le Dashboard
• La solution doit supporter le téléchargement des rapports sous plusieurs formats (PDF, CSV…)

• La solution doit donner la possibilité de créer tout les dashboard sur la base de n'importe quel champ des logs
Exigence globale de la Solution NDR
La solution proposée doit utiliser plusieurs algorithmes d'intelligence artificielle ainsi que plusieurs techniques de machine learning, contenant au minimum : le deep learning, le machine learning supervisé et le machine learning non supervisé
Utilisation de l'apprentissage automatique non supervisé de manière prédominante : La capacité du logiciel d'utiliser plusieurs techniques d'IA supervisées, non supervisées et de deep learning dans un cadre bayésien, ce qui permet de créer une protection sur mesure pour l'organisation
Corrélation directe entre toutes les sources de données : réseau, nuage, point final, courrier électronique, SaaS, IoT : Le potentiel de protection totale des actifs numériques de l'organisation, sans intégration nécessaire avec une autre technologie de sécurité.
Le système doit avoir la capacité de déployer des capteurs légers sur les points de terminaison pour étendre la visibilité lorsque les appareils sont déconnectés du réseau de l'entreprise sans compter sur les intégrations
Le fournisseur doit fournir des exemples authentiques et réels d'attaques APT zero-day détectées par le système
Le système doit disposer d'une fonction d'analyste IA capable de mener des enquêtes autonomes automatisées
Le système doit disposer d'une fonctionnalité d'analyse de l'IA capable de mener des enquêtes à la demande
Le système doit être en mesure de partager les rapports d'incident d'IA avec les systèmes SIEM, SOAR et SOC à l'aide d'une API externe
Il doit s'agir d'une plateforme d'auto-apprentissage et avec une approche adaptative, qui utilise une intelligence artificielle éprouvée pour en savoir plus sur l'environnement dans lequel elle se trouve, et détecter et répondre aux écarts par rapport à l'activité normale ;
le modèle du réseau appris par la solution doit être suffisamment dynamique pour s'adapter à tout changement de comportement de l'environnement
Modification/création de modèles : Capacité de la solution à modifier/créer des règles comportementales sur des scénarios spécifiques - les critères d'alerting combinent des mesures de 'metric' inhabituelles (Machine Learning) et des conditions classiques: protocoles, évènement, identité...
La solution devrait fonctionner entièrement à base d'apprentissage comportemental quand les technologies basées sur des règles et/ou des signatures ne s'appliquent pas
La solution doit permettre une analyse continue des chemins d'attaque les plus critiques. La solution analyse le risque cyber au niveau du SI (Système d'information) plutôt qu'au niveau de l'IP ou de device (niveau d'analyse inférieur de la concurrence).
La solution doit être capable de regrouper automatiquement les périphériques en groupes et clusters en fonction de leur similitude de comportement
La solution doit représenter visuellement toutes les activités du réseau et les connexions entre toutes les machines et les utilisateurs (en interne et en externe). Interface 3D pour la visualisation et la lecture en temps réel, avec possibilité de revisionner les évènements passés.

La solution doit fournir des rapports de flux de données en temps réel et des vues de tableau de bord
La solution proposée ne doit pas partager des données internes avec le cloud de l'éditeur.
Stockage des données : Toutes les données sont stockées on-premise sur le site du client, sans qu'il soit nécessaire de recourir à un cloud pour l'apprentissage, l'analyse ou la réponse.
La solution doit avoir une fonctionnalité capable de permettre une analyse rétrospective des journaux de l'incident, en retournant sur l'axe temps les données de connexion à quelques secondes, minutes, heures ou jours avant qu'une certaine anomalie ait été identifiée
La solution doit permettre la personnalisation et l'adaptation de l'apprentissage automatique aux conditions et caractéristiques spécifiques du réseau
La solution proposée doit consommer et analyser des données/flux bruts (paquets bruts) via la mise en miroir de ports (SPAN) ou via l'utilisation d'un TAP
La solution proposée doit être une technologie sans agent sans aucun besoin de configuration ou d'installation sur les terminaux
La solution proposée doit prendre en charge une architecture complète et évolutive grâce à l'ajout simple de licences de composants supplémentaires nécessaires pour s'intégrer aux différents environnements numériques, y compris sur site, cloud et hybrides, prenant en charge au moins :
a. Amazon AWS SaaS, EC2, IAM, S3, VPC et LAMBDA b. Microsoft Azure d. Bureau 365 d. Composants virtuels (machines virtuelles) e. Scripts pour l'analyse des serveurs locaux (capteurs pour les systèmes d'exploitation)
La solution proposée doit permettre la création automatique de rapports exécutifs couvrant au moins un aperçu de :
a. le résumé complet du déploiement indiquant le nombre total d'appareils, le nombre total de sous-réseaux et la bande passante multimédia traitée b. un récapitulatif des failles par phase d'attaque c. un récapitulatif des violations d'appareils d. un résumé des appareils TOP violant les conditions de haute priorité e. un résumé des violations les plus fréquentes des principaux éléments de conformité tels que l'utilisation abusive de : USB, google drive, RDP sortant, SQL externe, entre autres f. un résumé TOP des appareils qui enfreignent le plus les conditions de conformité générant un risque pour l'organisation
La technologie doit avoir sa propre application mobile disponible à la fois sur GooglePlay et AppleStore afin de permettre la gestion à distance des incidents
La solution doit avoir la capacité d'effectuer des notifications push pour les alertes
La solution proposée doit identifier les logiciels malveillants dans l'environnement de l'entreprise qui ont contourné les contrôles de sécurité au niveau des défenses du périmètre
La solution proposée doit identifier l'installation de portes dérobées permettant aux utilisateurs malveillants d'accéder aux ressources du réseau interne

La solution proposée doit pouvoir revenir sur des anomalies de comportement apparemment sans rapport pour ajouter un contexte à une violation ou à une tentative d'attaque
La solution proposée doit détecter les problèmes de performances sur le réseau
La solution proposée doit identifier une attaque de ransomware et doit permettre une intervention avant que les lecteurs/partages réseau mappés ne soient impactés
La solution proposée doit détecter les sessions actives pendant une période de temps plus longue que celle acceptée, par exemple une session FTP active pendant plus de 15 heures
La solution proposée doit identifier les attaquants utilisant des informations d'identification légitimes volées pour accéder au réseau
La solution proposée doit pouvoir prendre des mesures autonomes pour contenir les menaces en cours, ce qui donne à l'équipe de sécurité le temps d'enquêter et de remédier au besoin. La réponse autonome doit :
a. S'appuyer sur une compréhension de l'activité normale (comportementale) et être capable d'interrompre chirurgicalement l'activité inhabituelle uniquement b. Utiliser l'IA et l'apprentissage automatique comme base de réponse et non sur la base de règles et de signatures prédéfinies. c. Prendre des mesures proportionnées en temps réel - des interruptions spécifiques à la connexion jusqu'à la mise en quarantaine complète des appareils, soit directement, soit via des intégrations avec des pare-feu et/ou des contrôles d'accès au réseau. e. La réponse autonome doit pouvoir être affinée en fonction du type de comportement observé et de la gravité de l'incident. F. La réponse autonome doit avoir à la fois un mode humain et un mode actif, selon le niveau de visibilité que l'équipe de sécurité exige de la réponse automatique. g. Le système doit être capable de répondre de manière autonome à l'aide de contrôles natifs et de ne pas s'appuyer sur des intégrations. La technologie sélectionnée doit être capable de réaliser une réponse de manière totalement autonome, sans aucune intégration nécessaire avec une technologie extérieure (pare-feu, EDR, etc.). Cette réponse doit être effectuée par TCP-Reset et être suffisamment précise afin de pouvoir de réaliser en blocage indépendant en quelques secondes, et uniquement du flux (et non pas tout le poste).
Intégrations avec l'ensemble des produits de l'editeur et hors editeur. La capacité de fournir une sécurité de bout en bout grâce à un système interconnecté de moteurs d'IA qui se répercutent dans un cycle vertueux.
MITRE Attack : 139 techniques d'attaque couvertes pour le client utilisant toute la suite de technologie que propose l'éditeur
Analyse Forensic : Index Advanced Search (basé sur Elastic Search) et entrepôt de fichiers PCAPS. Ces artefacts d'analyse sont générés en continu et sont disponibles indépendamment d'une détection par la solution.
La solution doit être proposée avec le matériel nécessaire, l'extension de la plateforme nutanix peut être envisagée par le prestataire
Le titulaire doit prendre en charge totalement le déploiement des agents sur les endpoints et autres composants du réseau
Spécifications techniques de la solution EDR

• La console centrale permet d'être mise en place en mode sur site (FULL On-Premise). L'interface d'administration et les données doivent être On-premise.
• Les binaires d'installations peuvent être récupérés et intégrés dans un outil de déploiement tiers pour une installation également de manière pleinement silencieuse
• L'installation des agents doit être réalisée et finalisée sans obligation de redémarrage des postes de travail et des serveurs
• Un utilisateur ou administrateur du poste de travail ou du serveur ne doit pas avoir le droit de désinstaller les agents. L'administrateur de la solution EDR doit être l'unique profil habilité à désinstaller les agents
• La solution EDR doit proposer un mode « Apprentissage » permettant d'absorber tous les usages internes et créer des règles de sécurité Zero-Trust / durcissement d'une manière automatique adaptés au contexte interne.
• Outre les règles de sécurité Zero-Trust créées automatiquement par le mode apprentissage, la solution EDR doit intégrer par défaut des règles de durcissement permettant de (liste non exhaustive): • Interdire l'utilisation des outils d'administration (PSexec, PowerShel, WMI, etc) par les malwares • Interdire l'accès d'un processus non authentifié à la mémoire d'un autre processus • Protection des DLL • Protection des processus sensibles (lsaas, VSS, etc)
• La solution doit proposer la possibilité de configurer des règles Zero-Trust permettant de bloquer les TTPs de la matrice MITRE.
• La solution doit proposer des règles Zero-Trust permettant de bloquer les TTPs de la matrice MITRE ciblant les Endpoints.
• La durée de rétention des données doit être paramétrable au niveau de la console centrale.
• La consommation des ressources mémoires et CPU du terminal doit être faible (1% de CPU en utilisation normale, 100Mo de RAM, 100Mo de disque)
• La consommation de la bande passante doit être faible
• Pour un client n'ayant pas de connexion avec la console centrale, le mode offline doit assurer le même niveau de sécurité
• L'EDR doit être capable de pleinement remplacer un antivirus classique : • Smart Scan • Analyse de binaire • Gestion des supports amovible
• L'EDR doit être capable d'être désactivé sur sa fonctionnalité d'AV et travailler en binôme avec une solution antivirale conventionnelle basée sur des signatures uniquement.
• Capacités de mise à jour transparentes des clients dans un LAN qui n'a aucun accès à internet

• Possibilité de mettre à jour l'agent depuis la console centrale sans intervention locale ou à distance sur l'endpoint.
• L'EDR doit alerter à minima par mail les administrateurs suite à l'identification d'un évènement malveillant.
• L'EDR doit proposer une ségrégation par entité. La ségrégation doit être totale en termes de données ainsi qu'en terme d'administration.
• L'EDR doit proposer une configuration permettant la délégation de l'administration par entité ou ensemble d'entités.
• Administration / Exploitation de la console
• Un Système de MultiFactor Authentication comme le OneTime Passwords doit être intégré dans l'EDR
• Historique des données remontées des agents (rétention de logs) dans la console centrale sont paramétrables
• Dans le cadre d'alertes sur de multiples agents, la console regroupe ces alertes et les agrège pour un "hunting" plus efficace
• La solution doit proposer des API afin de permettre l'échange d'information avec d'autres solution de sécurité
• Depuis une alerte de sécurité ou un simple événement, la solution EDR doit permettre de créer automatiquement un schéma sous forme d'arbre d'exécution incluant tous les éléments d'une attaque afin de faciliter l'investigation.
• La console permet un soutien spécifique aux administrateurs pour faciliter la gestion des faux positifs
• La console permet de bloquer ou autoriser certains programmes (scripts, exécutables, etc.) propres au clients
• La solution doit permettre aux administrateurs d'appliquer des règles de sécurité dédiée aux utilisateurs nomade : • Limitation domaine / IP • Limitation sur les périphériques USB • Limitation de l'exécution de binaire • Limitation d'utilisation des support amovibles
• La solution doit permettre d'appliquer des stratégies de sécurité différentes en fonction des machines (serveurs, users, IT, dev, prod …). Et par conséquent fournir de niveau de sécurité différents pour les applications en fonction de la stratégie.
• L'EDR doit être capable de collecter les actions de chaque programme en temps réel (exécution, lecture, écriture, renommage, suppression, accès mémoire, accès réseau) sur la console d'administration de manière détaillée.
• L'EDR doit permettre de mettre en place des blocages spécifiques sur des actions faites par les programmes pour limiter la surface d'attaque. (Exécution, lecture, écriture, renommage, suppression, accès mémoire, accès réseau) Exemple : empêcher l'accès réseau pour les programmes sur les clés USB.
• L'EDR doit détecter les comportement des programmes et limiter l'utilisation des outils nécessaire aux attaques non basé sur des malware.

• L'EDR doit permettre de récupérer toutes les informations en live sur un système : • User connectés • Hardware de chaque composants interne ou périphérique de la machine • Processus / service / driver en cours d'exécution • Observateur d'évènements / logs • Rapports d'erreur système • Programme au démarrage • Variables d'environnement
• L'EDR doit permettre de récupérer la mémoire des programmes à distance afin de faire des investigation forensic
• L'EDR doit permettre de faire du versionning des fichiers sur les disques dur, pour pouvoir les restaurer en cas de compromission, d'altération, ou suppression malveillante.
• L'EDR doit proposer un mécanisme innovant basé sur l'intelligence artificielle (Machine learning ou Deep Learning) afin d'analyser les binaires.
• L'EDR doit proposer une API permettant l'utilisation directe des capacités de détection de l'intelligence artificielle dans d'autres produits.
• L'EDR doit proposer un système de monitoring des capacités Mémoire et CPU du parc afin d'identifier les malwares de type crypto-miner par exemple.
• La solution doit permettre une gestion de vulnérabilités automatique sans lancement ou planification de scan. La gestion de vulnérabilité doit inclure les vulnérabilités applicatives et les correctifs de sécurité système (ex. KB Microsoft)
• La solution doit permettre de lister les logiciels installés sur chaque poste.
• La solution doit permettre de lister tous les binaires connus sur le parc protégé cet sur chaque poste.
• L'EDR doit proposer une vue dédiée aux activités de HUNT. Cette vue doit regrouper tous les évènements (accès à la donnée, accès à la mémoire, accès réseau, etc.) générés sur le parc.
• L'EDR doit proposer des fonctionnalités de durcissement des applicatifs installé : • IP ou domaines autorisés • Type de données autorisés
• La solution EDR doit permettre à l'administrateur d'analyser des binaires sans les exécuter.

• La solution EDR doit permettre à l'administrateur de créer des politiques de sécurité différentes et d'y affecter des postes de travail et/ou des serveurs.
• La solution doit permettre la réalisation d'actions de remédiation et de « Rollback ». • La remédiation doit permettre le nettoyage d'un système de tous les éléments malveillants suite à une attaque. • Le « Rollback » doit permettre la récupération de donnée supprimées, altérées ou chiffrées suite à une attaque.
• La solution doit proposer un panel d'actions d'investigation qui peuvent être exécutées à distance sur un ou plusieurs postes (liste non exhaustive) : • Dump de mémoire d'un processus • Récupération d'une clé de registre • Récupération de la liste des processus en exécution • Isolation de la machine • Eteindre la machine
• La solution EDR doit disposer d'un outil d'aide à l'amélioration de la sécurité qui propose à l'administrateur des actions à réaliser afin d'améliorer le niveau de sécurité du parc.
• La solution doit permettre d'avoir une visibilité sur les fichiers système et programmes afin de vérifier leur intégrité
• La solution doit proposer une Live Map réseau permettant de visualiser les communications réseau en temps réel à l'échelle mondiale.
• L'éditeur doit disposer d'une équipe de support technique locale (Maroc).
• L'éditeur doit disposer d'une offre Cloud souveraine basée sur des serveurs localisés sur le territoire national marocain.
• L'éditeur doit proposer le service MDR opéré par des équipes locales au Maroc.
• L'éditeur doit proposer des rapports périodiques contextualisé au parc de client avec des recommandations personnalisées afin de guider les équipes internes dans l'amélioration du niveau de sécurité du périmètre
• La plateforme hardware est à la charge du prestataire et peut etre une extension de la plateforme nutanix de l'ONDA
• Le titulaire doit prendre en charge totalement le déploiement des agents sur les endpoints (postes de travail et serveurs)
Livrables
Le titulaire doit produire toutes les politiques et procédures exigées dans la DNSSI et la norme ISO27001 qui sont liés aux processus de gestion des incidents de sécurité SI
Le titulaire doit assister les équipes ONDA durant les périodes de garantie pour la mise à jour des politiques et procédures liés aux processus de gestion des incidents de sécurité SI
Le titulaire doit produire à minima les livrables suivants : o Document d'exploitation o Document d'architecture o Document d'installation

○ Rapports d'activité trimestriels ○ Comptes rendu de réunion projet : Comité de suivi et comité de pilotage
Il est demandé au titulaire de documenter tous les processus du SOC, EDR, NDR, SOAR. Cette documentation devra inclure à minima, des procédures, les modes opératoires associés, description des interactions entre ces processus et les activités SI existantes ainsi que les indicateurs de performances à surveiller. En résumé, il s'agit de produire une carte d'identité de chaque processus. Les différentes prestations devront être décrites, en détaillant les inputs, outputs, acteurs et étapes des traitements ainsi que les éventuels prérequis. Pour le processus de traitement des incidents, ce processus doit faire apparaitre, au minima, les acteurs et les actions, voire les outils. Deux processus sont particulièrement à documenter : le traitement d'incident détecté et remonté par la DGSSI (macert), le traitement d'incident détecté et remonté par le SOC ONDA (incident majeur ou normal).
Licences
Toutes les licences utilisées pour la mise en place du projet doivent être au nom de l'ONDA. L'équipe technique de l'ONDA doit être en mesure d'accéder aux plateformes éditeur pour la création de ticket support, consultation des licences, téléchargement des patchs, toute autre action nécessaire durant le cycle de vie des licences
Le titulaire doit justifier la pérennité des solutions proposées sur une durée minimale de six (06) ans, moyennant un document livré par les éditeurs.

Prestations attendues :

- L'équipe projet mise à notre disposition doit avoir au minimum une personne possédant une certification éditeur
- Le titulaire doit Installer et mettre en service la solution, ainsi assurer la configuration des stratégies et des politiques adéquates à l'infrastructure informatique de l'ONDA.
- Test et validation de des configurations et stratégie.
- Le titulaire est ténu de mettre à la disposition de l'ONDA les documents ci-après :
    - Document d'exploitation qui va contenir
        - Guide de configuration
        - Guide d'administration
    - Document d'architecture contenant l'ensemble des configurations effectuées
    - Document d'installation faisant référence à l'ensemble de procédure d'installation
- Le titulaire doit un transfert de compétence à l'équipe projet.

2.1 Installation, configuration et mise en service des solutions SIEM, EDR et NDR :

Cette prestation contient :

- La mise en place des solutions incluant les services d'installation et de paramétrage
- Le paramétrage des sources de log, la configuration des règles de corrélation (issues de l'identification des uses case), l'exploitation, le support et la maintenance.
- La formation de l'équipe ONDA sur l'installation, l'administration, le monitoring, l'exploitation et l'édition des rapports

Préparation du Plan de service SOC

1. PARTIE 2 : PREPARATION DE L'ENVIRONNEMENT DE LA SUPERVISION DES INCIDENTS DE SECURITE (SIEM, EDR, NDR):

L'objectif de cette partie est l'accompagnement de l'ONDA à la préparation de l'environnement de la supervision des incidents de sécurité (SIEM, EDR, NDR).

Cet accompagnement comprend la :

- Revue du périmètre de surveillance (actifs critiques) à travers une analyse de risque basée sur les méthodologies standards.
- Définition et implémentation des processus/procédures relatives au SOC et proposer une organisation SOC adéquate au contexte ONDA. Lors de cette phase, les ressources interne se mettront avec les analystes et experts du prestataire au sein du SOC pour proposer et tester les procédures à mettre en place pour traiter les différents types d'incidents et alertes en fonction des différents contextes possibles.
- Accompagnement de l'équipe sécurité ONDA à définir des use-cases adaptés au contexte de l'ONDA et à ces besoins de sécurité métier (aéroportuaire en particulier) et les implémenter.
- Intégration avec les sources de logs (SIEM, IPS/IDS, messagerie, WorkFlow, Feeds …).
- Adaptation, tunning des règles de corrélations et parsing des logs au niveau du SIEM afin de permettre la remonter des incidents les plus pertinents
- Conformité aux standards et réglementations de sécurité
- Formation de l'équipe ONDA sur les standards de la sécurité IT et organisation de transferts de compétence au sein du SOC
- Organisation de comités projet mensuelles à bimensuelles pour faire le bilan des réalisations et mettre à jour les procédures de fonctionnement (détection, veille, analyse, intervention…) au besoin.

1.1 Phase 1 : Etude de l'environnement et cadrage du périmètre

Durant cette phase, le titulaire doit mener une mission d'étude de l'environnement pour contrôler les prérequis :

- Contrôle et mise à niveau de la politique de sécurité conforme à la directive nationale de sécurité des systèmes d'information.
- L'identification des principaux risques et des menaces associées
- La mise en œuvre des mesures de sécurité de base.

Cette mission consiste à valider les moyens de protection mis en œuvre sur les plans organisationnels, procéduraux et techniques.

La deuxième étape de l'étude se concentre sur les besoins SSI à couvrir par le SOC :

- Liste des « use cases » standards portés par le SOC
- Construction des scénarios de menaces métiers à couvrir
- Etude Spire ou autres analyses de risques
- Temps de rétention des différentes traces collectées

Une fois les besoins évalués, l'étude de cadrage se focalise sur la compatibilité technique et organisationnelle du S.I. existant avec la mise en œuvre du SOC. Les éléments suivants viennent donc compléter l'étude de cadrage :

- Revue de l'architecture sécurisée existante
- Existence et disposition des serveurs de temps
- Gestion des journaux d'événements et périmètre de collecte
- Volumétrie des journaux actuellement collectés / Durée de rétention.
- Vérification de la politique des logs (verbosité, chiffrement, signature)

La dernière étape de l'étude de cadrage concerne :

- L'organisation du projet (RACI)
- La définition du périmètre métier adressé et couvert par le SOC
- La définition du socle de base des équipements supervisés :
    - Passerelles internet et de messagerie
    - Système de détection/prévention d'intrusions (IDS/IPS) de flux et de postes
    - Active Directory (et annuaires d'entreprises)
    - Anti-virus de flux et de poste
    - Scan de vulnérabilité

- Firewall et WAF

Exigence de l'équipe projet : Le prestataire doit justifier d'une expérience en aéroportuaire et proposer des profils dans son équipe qui ont déjà travaillé dans des projets similaires dans le domaine aéroportuaire que ce soit en audit, intégration de solution sécurité ou mise en place de SOC.

1.2 Phase 2 : Préparation de l'environnement de la supervision des incidents de sécurité :

Cette phase se concentre dans un premier temps sur **la collecte** et **le traitement** des événements existant :

- Collecte des journaux d'événements (déjà concentré une première fois par le SIEM dans la partie 1).
- Construction des scénarios de corrélation et implémentation dans le SIEM
- Alimentation du SOC en événements et résultats des corrélations.
- L'identification des profils des opérateurs/acteurs du SOC
- Les moyens de réaction
- Elaboration de scénarios de menaces et des priorités de traitement
- Pilotage du niveau de sensibilité (pour améliorer la qualité de l'alerte)

Collecte des évènements :

La collecte des données est réalisée dans l'objectif d'alimenter le service de supervision. Les événements doivent ainsi être formatés pour être exploitables.

Dans un premier temps, la collecte concerne :

- Les équipements de sécurité
- Les équipements réseaux
- Les applications.

En prenant en considération :

- La normalisation des événements collectés pour permettre leur exploitation ;
- Le stockage des événements collectés (dans le respect des contraintes réglementaires) ;
- L'archivage des événements collectés en tenant compte des obligations de non-répudiation et d'intégrité des données

Traitement des évènements :

Le traitement a pour objectif de s'attacher à la détection des risques les plus redoutés en se basant sur le résultat de l'analyse de risque mené dans la première phase de la partie 2.

Le traitement des événements de sécurité est conditionné par les scénarios d'infrastructures et métiers.
Les scénarios d'infrastructures visent à définir les règles de bases liées aux événements produits par les systèmes d'infrastructure et plus particulièrement par les équipements de sécurité.

Le titulaire doit mettre en place un processus de gestion des règles qui permet de s'assurer du suivi de l'efficacité de la détection. Ce processus aborde les points suivants :

- Identifications du besoin de détection
- Conception de la règle
- Test, validation et mise en production de la règle
- Vérification hebdomadaire de l'efficacité de la règle
- Ajustement et enrichissement de la règle
- Identification des axes d'amélioration de la règle
- Modification de la règle

Le processus de traitement est basé sur la norme ISO 27035 (gestion des incidents de sécurité d'un SOC) et sur les indicateurs ETSI GS ISI pour la définition des KPSI.

Il est demandé au titulaire de documenter tous les processus du SOC, cette documentation devra inclure à minima, des procédures, les modes opératoires associés, description des interactions entre ces processus et les activités SI existantes ainsi que les indicateurs de performances à surveiller.
Les différentes prestations devront être décrites, en détaillant les inputs, outputs, acteurs et étapes des traitements ainsi que les éventuels prérequis.
Pour le processus de traitement des incidents, ce processus doit faire apparaitre, au minima, les acteurs et les actions, voire les outils.
Deux processus sont particulièrement à documenter : le traitement d'incident détecté et remonté par la DGSSI (macert), le traitement d'incident détecté et remonté par le SOC ONDA (incident majeur ou normal).

Le SOC devra fournir différents types de TDB adaptés aux besoins ONDA selon les niveaux management/exécutif et opérationnels, ils doivent intégrer tous les outils SOC, SIEM, Ticketing, Threat Intelligence, et ainsi offrir une vue consolidée des activités du SOC et de l'état de santé du SI en matière de sécurité.

En cas de crise à forte gravité, le prestataire déplacera sur le site de l'ONDA les compétences nécessaires qui, avec l'équipe informatique de l'ONDA, prendront les décisions adaptées.

Dans ces circonstances, le prestataire doit mettre en œuvre une stratégie de réponse à l'incident et déployer les outils nécessaires pour identifier le mode opératoire, l'étendue de l'attaque et les mesures de remédiation.

2. PARTIE 3 : MISE EN PLACE DE THREAT INTELLIGENCE :

Le titulaire est tenu à proposer une solution de type Threat intelligence permettant :

- Une solution permettant d'enrichir les composants ONDA avec les différents IOC
- Un service de surveillance de l'exposition sur les réseaux non maitrisé comme le Dark Web et le Deep Web sans frais supplémentaire
- L'anticipation et la détection des attaques prévues par les Cybercriminels
- L'analyse par domaine, IP, noms et emails
- L'identification et le suivi d'arrêt (take down) des domaines de phishing
- La possibilité de partage des IOC entre plusieurs entités
- Le ticketing , attribution et suivi des alertes
- Alerte en cas de détection de fuites de données.
- La possibilité de suivre les divulgations au niveau des réseaux sociaux
- La solution doit inclure les alertes et bulletin de sécurité de la DGSSI
- La solution doit permettre des accès illimités pour l'ensemble des entités affiliés à l'ONDA
- Les données doivent être hébergées dans le territoire nationale
- Permettre l'intégration avec les outils de sécurité et les systèmes existants via des APIs.
- L'ensemble des données au niveau de la solution doivent être hébergées dans le territoire nationale
- Permettre aux différentes entités du groupe de partager des informations sur les menaces, les IoC, les vulnérabilités et les bonnes pratiques de sécurité.
- Faciliter le partage sélectif d'informations en fonction des besoins de chaque entité
- Possibilité de créer des tickets et suivi de la résolution de l'alertes
- La solution doit inclure les alertes identifier par la DGSSI d'une façon automatique
- Permettre l'accès au bulletin de sécurité de Ma-Cert

ARTICLE 15 : DEFINITION DES PRIX

Les prix sont définis conformément aux dispositions de l'article 53 du CCAGT.

Prix n° 1 : Audit, risk assessement et cadrage du périmètre :
Ce prix rémunère l'audit, risk assessement et cadrage du périmètre, tels que définis dans l'article «DESCRIPTION DU PROJET» de la présente tranche du marché.
Prix payé au forfait.
Prix n° 2 : Fourniture de la solution SIEM (U=EPS):
Ce prix rémunère la fourniture de la solution SIEM (U=EPS), tels que définis dans l'article «DESCRIPTION DU PROJET» de la présente tranche du marché.
Prix payé à l'unité **(U= EPS)**.
Prix n° 3 : Fourniture de la solution EDR (U=Endpoints):
Ce prix rémunère la fourniture de la solution EDR, tels que définis dans l'article «DESCRIPTION DU PROJET» de la présente tranche du marché.
Prix payé à l'unité **(U=Endpoints)**
Prix n° 4 : Fourniture de la solution NDR (U=IP)
Ce prix rémunère la fourniture de la solution NDR, tels que définis dans l'article «DESCRIPTION DU PROJET» de la présente tranche du marché.
Prix payé à l'unité **(U= IP)**

Prix n° 5 : Mise en place de Threat intelligence
Ce prix rémunère la mise en place de Threat intelligence, tels que définis dans l'article «DESCRIPTION DU PROJET» de la présente tranche du marché.
Prix payé au forfait.
Prix n° 6 : Installation, Configuration, Formation et Mise en service du SOC
Ce prix rémunère l'installation, Configuration, Formation et Mise en service du SOC, tels que définis dans l'article «DESCRIPTION DU PROJET» de la présente tranche du marché.
Prix payé au forfait.

CHAPITRE 3 : CLAUSES TECHNIQUES – Tranche conditionnelle-

ARTICLE 01 : MAITRE D'ŒUVRE

Le maitre d'œuvre de la tranche conditionnelle du présent marché est **Direction des Systèmes d'Information**.

ARTICLE 02 : BREVETS

L'entrepreneur garantira le maître d'ouvrage contre toute réclamation des tiers relative à la contrefaçon ou à l'exploitation non autorisée d'une marque commerciale ou de droit de création industrielle résultant de l'emploi des fournitures ou d'un de leurs éléments.

ARTICLE 03 : NORMES

Les fournitures livrées en exécution de la présente tranche du marché doivent être conformes aux normes Marocaines ou autres normes applicables au Maroc en vertu d'accords internationaux fixées aux prescriptions et spécifications techniques du présent marché ou à des normes internationales en cas d'absence desdites normes.

ARTICLE 04 : GARANTIE PARTICULIERE

Le Prestataire garantit que toutes les fournitures livrées en exécution du marché sont neuves, n'ont jamais été utilisées, sont du modèle le plus récent en service et incluent toutes les dernières améliorations en matière de conception et de matériaux, sauf si le marché en a disposé autrement. Le titulaire garantit en outre que les fournitures livrées en exécution du marché n'auront aucune défectuosité due à leur conception, aux matériaux utilisés ou à leur mise en œuvre (sauf dans la mesure où la conception ou le matériau est requis par les spécifications de l'ONDA) ou à tout acte ou omission du titulaire, survenant pendant l'utilisation normale des fournitures livrées dans les conditions prévalant dans le pays de destination finale.

ARTICLE 05 : CONTROLE ET VERIFICATION

L'ONDA aura le droit de contrôler et/ou d'essayer les fournitures pour s'assurer qu'elles sont bien conformes au marché. L'ONDA notifiera par écrit au titulaire l'identité de ses représentants à ces fins.

Si l'une quelconque des fournitures contrôlées ou essayées se révèle non conforme aux spécifications, l'ONDA la refuse; Le titulaire devra alors remplacer les fournitures refusées sans aucun frais supplémentaire pour l'ONDA.

Le droit de l'ONDA de vérifier, d'essayer et, lorsque cela est nécessaire, de refuser les fournitures ne sera en aucun cas limité, et l'ONDA n'y renoncera aucunement du fait que lui-même ou son représentant les aura antérieurement inspectées, essayées et acceptées.

Rien de ce qui est stipulé dans cet article ne libère le titulaire de toute obligation de garantie ou autre, à laquelle il est tenu au titre du présent marché.

ARTICLE 06 : DUREE DU MARCHE

La présente tranche conditionnelle du marché est valable pour une durée **d'une (1) année** à compter de la date de l'ordre de service prescrivant le commencement des prestations de cette tranche **(après la réception provisoire de la tranche ferme du marché).**

Elle sera reconduite automatiquement d'année en année pour une période globale de **cinq (5) ans**, sauf résiliation demandée par l'une des parties trois mois à l'avance de la fin de fin de chaque année du marché (date d'anniversaire).

ARTICLE 07 : PENALITES POUR RETARD

A défaut par l'Entrepreneur d'avoir exécuté à temps la tranche conditionnelle le marché ou d'avoir respecté tout planning ou délai prévu par la tranche conditionnelle du présent marché, il lui sera appliqué sans préjudice de l'application des mesures prévues par les articles 79 et 80 du CCAGT, une pénalité de **cinq pour mille** (**5 ‰)** du montant initial de la tranche conditionnelle du présent marché éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux, par jour de retard.

1- **En cas de retard dans l'exécution des travaux :** Par application de l'article 65 du CCAGT la pénalité est plafonnée à **huit pour Cent (8 %)** du montant de la tranche conditionnelle du marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux ; au-delà de ce plafond, l'O.N.D.A. se réserve le droit de procéder à la résiliation du marché sans préjudice des mesures coercitives prévues par les articles 79 et 80 C.C.A.G.T.
2- **En cas de retard dans la remise des documents ou rapports ou pour défaut de réalisation de certaines de ses obligations :** Par application de l'article 66 du CCAGT la pénalité est plafonnée à **deux pour Cent (2 %)** du montant de la tranche conditionnelle du marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux.

Les sommes concernant les pénalités seront déduites des décomptes de l'entreprise sans qu'il ne soit nécessaire d'une mise en demeure préalable.

ARTICLE 08 : CAUTIONNEMENT DEFINITIF – RETENUE DE GARANTIE - TRANCHE CONDITIONNELLE

a) Cautionnement : Le cautionnement définitif est fixé à **Trois pour cent (3%)** du montant initial du marché correspondant à la tranche conditionnelle arrondi au dirham supérieur conformément aux dispositions de l'article 15 du C.C.A.G.T.

b) Retenue de garantie : Par dérogation aux dispositions aux articles 16 et 64 du C.C.A.G.T, aucune retenue de garantie ne sera opérée au titre du présent marché.

Toutes les cautions présentées sous forme de cautions personnelles et solidaires doivent contenir la mention « à première demande de l'ONDA » et être émises par un organisme marocain agréé.

ARTICLE 09 : MODE D'EXECUTION

L'exécution du marché se fera par des appels de commande annuels et/ou ponctuels signés par la personne habilitée de l'ONDA et notifiés au titulaire du marché par télécopie au

numéro fourni par le fournisseur (le rapport d'émission fait foi) ou remis en mains propres au siège du fournisseur contre accusé de réception.

Pour chaque année de reconduction du marché et/ou à chaque fois que le besoin se présente, le maître d'ouvrage notifiera au titulaire les quantités de l'appel de commande sur la base des tarifs indiqués au niveau de bordereau des prix.

ARTICLE 10 : RECEPTION DES PRESTATIONS DE TRANCHE CONDITIONNELLE

Les attestations de prestations réalisées sont signées par les responsables habilités et seront établies **trimestriellement.**
La réception définitive sera prononcée à la fin de la durée des prestations objet de la présente tranche du marché.

ARTICLE 11 : NATURE DES PRESTATIONS ET REVISION DES PRIX

La présente tranche conditionnelle concerne des prestations de **service** dont les prix applicables sont fermes et non révisables.

ARTICLE 12 : MODE DE PAIEMENT

L'ONDA se libérera des sommes dues en exécution de la tranche conditionnelle du présent marché en faisant donner crédit au compte ouvert au nom du prestataire indiqué sur l'acte d'engagement.
Les paiements partiels seront effectués trimestriellement à terme échu.
Le paiement des sommes dues est effectué, dans un délai maximum de quatre-vingt-dix jours (90) à compter de la date de réception des prestations demandées et sur présentation de factures en cinq exemplaires.

ARTICLE 13 : DESCRIPTION TECHNIQUE DES PRESTATIONS

Objet :

L'objectif de cette prestation est l'infogérance des services SOC et leur démarrage durant la période du marché. Durant cette phase on doit assurer le fonctionnement nominal et pérenne du SOC et de son maintien en condition opérationnelle par rapport aux objectifs de sécurité qui lui sont assignés et aux périmètres arrêtés en commun accord avec le Maître d'Ouvrage.

1. Infogérance des solutions SIEM, EDR, NDR et services Threat intelligence

a. Supervision des événements de sécurité

Le Titulaire est tenu d'assurer la supervision du SOC en mode 24H/24 et 7J/7 en appliquant les procédures élaborées et validées lors de la phase 2.

A la remontée d'une alerte, le Titulaire doit s'assurer de sa véracité et procéder à sa normalisation en proposant toutes les actions correctives nécessaires. L'ONDA accompagnera le titulaire durant les 3 premiers mois à partir du démarrage des services SOC afin que l'équipe SOC prenne connaissance du contexte ONDA et son SI, au-delàs le titulaire doit être capable d'assurer les services SOC d'une manière autonome.

A cet effet il doit :

- Consultation et supervision continue des différents événements de sécurité générés par le SIEM, trafic réseau et flux inclus ;
- Définir et paramétrer les types des évènements significatifs pour l'activité de supervision ;
- Modifier dans ce cas échéant les règles de corrélation de SIEM suite à la détection d'un évènement suspect.
- Modification des règles de corrélation afin d'éliminer les différents faux positifs ;
- Assurer la continuité des services du Système d'Information ; (=> SLA)
- Fournir des recommandations de correction, en cas de problème/incident de sécurité, tout au long du marché ;
- Assurer l'accompagnement dans la résolution des incidents de sécurité après leur détection par le prestataire ;
- Veiller à l'amélioration du niveau de sécurité.

Le Titulaire pourra utiliser d'autres outils en complément du SIEM, NDR et EDR afin d'assurer les services attendus au SOC.

b. Service NDR Monitoring 24/7

Le prestataire est tenu d'assurer la supervision des flux réseaux à travers la console NDR Il s'agit d'assurer les prestations suivantes :

- Supervision en continu 24/7/365 de tout le périmètre intégré au NDR (Traffic web, réseaux, DMZ, interne,etc…);
- Mise à disposition d'équipe qualifiée (N1, N2,N3) pour la prise en charge des différentes alertes générées par le NDR;
- Traitement des alertes NDR, et réalisation de recherches spécifiques pour identifier les comportements suspects :
    - Communications sortantes vers Internet;
    - Nouvelles communications vers les serveurs critiques;
    - Communications suspicieuses avec des adresses IP publiques;
    - Recherches des derniers IOCs pertinents aux contextes des clients;
    - Etc…
- Alerting du Client en 24/7/365 (par mail ou par appel téléphonique selon incident et le plan de services).

c. Service EDR Monitoring 24/7

Le prestataire est tenu d'assurer la supervision des endpoints à travers la console EDR Il s'agit d'assurer les prestations suivantes :

- Supervision avec des analystes N1, N2, N3 pour les postes de travail, et les serveurs en mode 24/7/365 ;
- Analyse comportementale et corrélation des informations remontées à l'aide de la solution EDR ;
- Recherche des menaces dormantes grâce à la base de Threat Intelligence du CyberSOC ;
- Suppression automatique des fichiers infectés ;
- Confinement rapide, total ou ciblé : par machine ou par type d'actions possibles ;
- Investigation pour comprendre l'attaque ;
- Recommandation pour restaurer le système d'information et le renforcer.

d. Service veille de sécurité

Le Cyber SOC du prestataire devra assurer la détection des vulnérabilités potentielles et définir un plan de remédiation. Assurer une veille technologique en termes de sécurité et

remonter les points stratégiques aux équipes à travers une plateforme. Cette plateforme devra respecter les exigences suivantes :

- Authentification des utilisateurs par login et mot de passe ;
- Rédaction des bulletins de sécurité avec les champs objet, description, type, criticité, exploitation, plateformes impactées, produit concerné, risques et recommandations ;
- Possibilité de modification des bulletins existants ;
- Possibilité d'envoyer des e-mails de test vers la boite de messagerie ;
- Possibilité de lier le produit à un ou plusieurs identifiants CPE avec les caractéristiques :
  - Identifiant
  - Version
  - Mise à jour de version
- Possibilité de créer une alerte de sécurités, lancer une chercher aux alertes (par identifiant, objet, ou par type), ainsi que lister les alertes issues de la recherche pour effectuer les actions nécessaires selon le besoin (afficher détails, modifier ou supprimer) ;
- Disponibilité des profils suivants :
  - Utilisateur
  - Administrateur client
  - Analyste
  - Analyste Validateur
  - Administrateur technique

Le prestataire doit se doter d'un Cyber SOC membre du réseau international FIRST dans l'année en cours.

e. Service Threat Intelligence & Dark web Monitoring en MSSP :

Le prestataire doit proposer le service Threat Intelligence & Dark web Monitoring avec minimum :

- Surveillance du Dark Web à la recherche des données professionnelles et personnelles du Client et notification des équipes pour agir (adresses électroniques, numéros de téléphone et numéros de cartes de crédit, mots de passes, nom et prénoms des responsables, etc.)
- Surveillance des salles de discussion, des blogs, des forums, des sites que les criminels sont connus pour fréquenter
- Information des équipes du Client des menaces potentielles
- Bénéficier automatiquement des derniers IOC, provenant des sources de threat intelligences des CERTs
- Faciliter la recherche, validation et consommation des indicateurs pour la prise de décision vis-à-vis des incidents remontés
- Générer et collecter les informations contextuelles concernant les évènements en cours de traitement, appariement des informations récoltées avec des modes opératoires constatés chez les APTs (Advanced Persistent Threat) et autres groupes adversaires (ATTACK MITRE).
- Permettre de calculer les probabilités relatives aux menaces pouvant toucher à la sécurité SI du Client, en se basant sur des informations et des faits réels.

f. Service Réponse automatique aux incidents

Le prestataire doit proposer le service de la réponse automatique aux incidents avec minimum :

- Blocage des adresses IP malveillantes au niveau des pares-feux ;
- Isolation d'une machine du réseau ;
- Désactivation des comptes utilisateurs au niveau de l'annuaire Active directory, LDAP ;
- Réinitialisation des identifiants d'un compte système ;
- Les actions faites sont considérées comme une réponse/réaction sur l'incident afin de minimiser les risques et endiguer les menaces rapidement.
- Collecte des éléments nécessaires pour le développement des playbooks d'automatisation de la réponse aux incidents à travers l'interfaçage des solutions de sécurité supportées avec le XSOAR ;
- Définition des perspectives d'évolution et de l'organisation à mettre en place par les deux parties ;
- Définition de l'ensemble des éléments techniques et fonctionnels relative à la réponse aux incidents (reporting, indicateurs, protocoles de communication, etc..).
- Réponse aux incidents en continu 24/7/365 ;
- Développement et mise à jour des scénarios de blocage à travers les playbooks XSOAR ;
- Alerting du client en 24/7/365 (par mail ou par appel téléphonique selon incident et le plan de services) ;
- Comité hebdomadaire, mensuel, trimestriel selon la fréquence définie avec le client ;
- KPI du nombre des incidents bloquées par périmètre et catégorie ;
- Amélioration des playbooks pour le contexte de l'ONDA.

g. Le Maintien en Condition Opérationnelle du SOC

Le maintien en condition opérationnelle (MCO) du SOC et son amélioration continue, est à la charge du Titulaire, durant la période du marché qui découlera de cet appel d'offre, le titulaire doit :

- Maintenir à jour et effectuer les montées de versions nécessaires pour tous les composants (matériel ou logiciel) objet du présent marché. Ces évolutions doivent être actées en commun accord avec le Maître d'Ouvrage.
- Surveiller et ajuster les taux et les seuils d'alertes pour éviter une saturation du SOC et une constitution d'un backlog important. Les opérations de tunning de la solution est une action continue durant toute la période du marché.
- Faire de la veille de sécurité et rester à niveau par rapport aux évolutions des menaces afin d'affiner les scénarios de détection mis en place.
- Produire des tableaux de bord opérationnels et managériaux selon la périodicité convenue en commun accord avec le Maître d'Ouvrage.
- Maintenir les uses cases mis en place par la mise en place de nouveaux cas (suite à l'apparition d'une nouvelle menace de sécurité par exemple), la suppression ou la modification de cas existants. Ceci doit être mené en commun accord avec le Maître d'Ouvrage.
- Faire le suivi des incidents sécurité et Participer à leur résolution ci l'ONDA juge nécessaire.
- Animer des réunions de suivi.

- L'administration des solutions SOC y compris le SIEM est à la charge du titulaire dans le cadre du dispositif SOC. Une ressource Administrateur SIEM doit être prévu sur site ou à distance afin d'assurer les différentes activités et MCO.

Le Maître d'Ouvrage s'engage à informer le Titulaire de tout changement opéré sur son Système d'Information pouvant avoir un impact sur la solution SIEM ou le service SOC mis en place dans le cadre du marché qui découlera du présent Apple d'offre. Ceci permettra d'éviter des changements non répertoriés pouvant provoquer un accroissement des incidents et/ou une saturation des équipes en charge.

h. SLA

Le niveau de service attendu est soumis au minimum aux SLA suivants. La liste complète des SLA sera élaborée en commun accord avec le Maître d'Ouvrage. Les pénalités relatives au non-respect desdits SLAs

La prestation de support à distance consiste à suivre des incidents de sécurité en tenant compte des critères d'impact, d'urgence et de criticité, définis de la manière suivante :

- **L'impact** mesure l'effet d'un incident ou d'une demande sur le métier du Client. On peut évaluer l'impact selon différents critères :
  - le nombre d'utilisateurs affectés
  - les pertes financières potentielles
  - le nombre de services affectés
  - le manquement aux règlements et aux lois
  - la réputation de l'entreprise
- **L'urgence** représente le temps que peut mettre un incident. L'urgence est mesurée par l'analyste du SOC et de son analyse de la situation tel que décrite par le(s) utilisateur(s) qui déclare(nt) l'incident
- **La sévérité** d'un incident dépend des deux valeurs de l'impact et de l'urgence de l'incident selon le tableau ci-dessous :

Criticité		Impact		
		Elevé	**Moyen**	**Bas**
Urgence	**Urgent**	Critique	Haute	Moyenne
	Standard	Haute	Moyenne	Basse

Autres définitions :

HO = Heures ouvrées, représente dans le cadre de ce Contrat les heures ou sont réalisées les activités de supervision, à savoir de 0h à 23 :59, sept jours sur sept

JO = représentent les jours travaillés de l'année, n'incluant pas les jours fériés religieux, nationaux, et les weekends

ISC = Incidents de sécurité à Sévérité Critique

ISH = Incidents de sécurité à Sévérité Haute

ISM = Incidents de sécurité à Sévérité Moyenne

ISB = Incidents de sécurité à Sévérité Basse

Délai de prise en compte : Il s'agit du délai pour l'affectation de la demande ou de l'incident à un collaborateur du Prestataire pour traitement. Pour les demandes, cette affectation est aussi tracée à travers un retour par Email.

Délai de traitement : Il s'agit du délai pour le traitement de l'incident ou de la demande. Ce délai concerne uniquement les traitements par les équipes du prestataire, et en est déduis le

délai de tout traitement par le client ou un de ses fournisseurs, ou du délai de traitement par l'éditeur dans le cas de problèmes traités par ce dernier.

Aussi, les niveaux de service pour les prestations objets de ce Contrat peuvent être définis comme suit :

Délai de traitement des demandes de changement de configuration standards

	Délai de prise en compte (à partir de la réception de la demande)	**Délai de traitement** (à partir de la réception de la demande)
Délai de traitement des demandes de changement de configuration standards	Sous 4 HO dans 95% des cas	Sous 1,5 JO dans 95 % des cas

Délai de traitement des demandes de changement de configuration non standards

	Délai de prise en compte (à partir de la réception de la demande)	**Délai de traitement** (à partir de la réception de la demande)
Délai de traitement des demandes de changement de configuration non standards	Sous 8 HO dans 95% des cas	Sous 5 JO dans 95 % des cas

Délai de prise en compte des incidents de sécurité

	Sévérité Critique	**Sévérité Haute**	**Sévérité Moyenne**	**Sévérité Basse**
Délai de prise en compte des incidents de sécurité	Sous 4 HO dans 95% des cas	Sous 4 HO dans 95% des cas	Sous 1 JO dans 95% des cas	Sous 2 JO dans 95 % des cas

Délai de traitement des incidents de sécurité

	Sévérité Critique	**Sévérité Haute**	**Sévérité Moyenne**	**Sévérité Basse**
Délai de traitement des incidents de sécurité	Sous 1 JO dans 95% des cas	Sous 1 JO dans 90% des cas	Sous 2 JO dans 90% des cas	Sous 5 JO dans 90 % des cas

Le Titulaire est tenu, selon les SLA, d'appliquer les procédures de correction et/ou de contournement afin de réussir la résolution des incidents détectés.

Le Titulaire est tenu de suivre les tickets ouverts jusqu'à résolution de l'incident et la documentation du rapport d'incident.

En cas de crise à forte gravité, le prestataire déplacera sur le site de l'ONDA les compétences nécessaires qui, avec l'équipe informatique de l'ONDA, prendront les décisions adaptées.
Le prestataire est tenu, selon les SLAs (voir tableau SLA), d'appliquer les procédures de correction et/ou de contournement pour la résolution des incidents détectés par ses propres outils en concertation avec l'équipe de l'ONDA.

Livrables de l'infogérance SOC

- Rapport de supervision trimestrielle
- Tableaux de bord produits mensuel

2. Services SOC Annexe

Les services Annexes du SOC sont à la demande et selon le besoin de l'ONDA.

Le titulaire doit mettre à la disposition de l'ONDA des compétences pointues selon le besoin. Après réception du CV de l'intervenant l'ONDA examine le CV, et peut refuser et demander le changement si la ressource ne donne pas satisfaction.

Les services SOC Annexe consistent à :

- Les Investigations et diagnostic des incidents confirmés (incident response, Forensics);
- Réalisation des tests d'intrusion internes et/ou externes (2 fois par ans).
- Simulation de crise (1 fois par ans)
- Formations des équipes ONDA à la demande
- Exercices RedTeam/BlueTeam (2 fois par an)

Cette partie sera coté en Jours/Homme, le titulaire doit coter le prix du jour/homme sur le Bordereau de prix-Détail estimatif (BDP-DE).

ARTICLE 14 : DEFINITION DES PRIX

Les prix sont définis conformément aux dispositions de l'article 53 du CCAGT.

Prix n° 1 : Infogérance des services de supervision SOC (U=EPS) :
Ce prix rémunère l'infogérance des services de supervision SOC, tels que définis dans l'article «DESCRIPTION TECHNIQUE DES PRESTATIONS» de la présente tranche du marché.
Prix payé à l'unité **(U=EPS)**.

Prix n° 2 : Infogérance des services de supervision EDR (U=Endpoint) :
Ce prix rémunère l'infogérance des services de supervision EDR, tels que définis dans l'article «DESCRIPTION TECHNIQUE DES PRESTATIONS» de la présente tranche du marché.
Prix payé à l'unité **(U= Endpoint)**.

Prix n° 3 : Infogérance des services de supervision NDR (U=IP) :
Ce prix rémunère l'infogérance des services de supervision NDR, tels que définis dans l'article «DESCRIPTION TECHNIQUE DES PRESTATIONS» de la présente tranche du marché.
Prix payé à l'unité **(U= IP)**.

Prix n° 4 : Dark web monitoring
Ce prix rémunère le Dark web monitoring, tels que définis dans l'article «DESCRIPTION TECHNIQUE DES PRESTATIONS» de la présente tranche du marché.
Prix payé au forfait.

Prix n° 5 : Incidense response via SOAR
Ce prix rémunère l'incidense response via SOAR, tels que définis dans l'article «DESCRIPTION TECHNIQUE DES PRESTATIONS» de la présente tranche du marché.
Prix payé au forfait.

Prix n° 6 : Veille de vulnérabilité
Ce prix rémunère la veille de vulnérabilité, tels que définis dans l'article «DESCRIPTION TECHNIQUE DES PRESTATIONS» de la présente tranche du marché.
Prix payé à l'ensemble.

Prix n° 7 : Services annexes SOC
Ce prix rémunère les services annexes SOC, tels que définis dans l'article «DESCRIPTION TECHNIQUE DES PRESTATIONS» de la présente tranche du marché.
Prix payé au jour/Homme.

Appel d'offres ouvert N° 014-24-AOO

Acquisition, déploiement et infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence

Tranche ferme : Acquisition et déploiement des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Tranche conditionnelle : Infogérance des solutions de cybersécurité SIEM, EDR, NDR et Threat intelligence.

Direction concernée	Direction des Achats et de la Logistique
M. Mohamed Amine BAKRI Chef du Service Base de Données M. Driss AOUI Chef du Département Infrastructures et Exploitation M. EL KARIMI Abdelhalim Directeur des Systèmes d'information	Le Directeur des Achats et de la Logistique Abdellah BOUKHLOUF

Direction Générale de l'ONDA
05 DEC. 2023 La Directrice Générale Habiba LAKLALECH Direction Générale OFFICE NATIONAL DES AEROPORTS

Concurrent
CPS lu et accepté sans réserve