

ROYAUME DU MAROC

__**_**_**

OFFICE DE LA FORMATION PROFESSIONNELLE ET DE LA PROMOTION DU TRAVAIL

====*==*

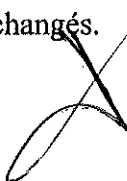
AVIS RECTIFICATIF DE L'APPEL D'OFFRES OUVERT N°98/ 2024

L'Office de la Formation Professionnelle et de la Promotion du Travail porte à la connaissance du public que des modifications, ci-après, ont été apportées au dossier d'appel d'offres ouvert n° 98/2024, relatif au **Projet infrastructure et sécurité SI OFPPT au niveau Siege & directions régionales**

- 1- Des modifications ont été apportées au dossier d'appel d'offres.
- 2- La date d'ouverture des plis est reportée au **30 Septembre 2024 à 10 Heures.**
- 3- Les Prospectus, notices ou autre documents exigés par le dossier d'appel d'offres doivent être déposés **au service des marchés à la Direction de l'Approvisionnement et la Logistique, sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) Casablanca**, au plus tard le **27 Septembre 2024 à 16 Heures,** ou remis séance tenante au président de la Commission d'ouverture des plis.

Le dossier d'appel d'offres rectifié peut être retiré à la Direction de l'Approvisionnement et la Logistique (Service des Marchés), sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) Casablanca, il peut être également téléchargé à partir du portail des marchés de l'Etat www.marchéspublics.gov.ma et du site de l'Office de la Formation Professionnelle et de la Promotion du Travail : www.ofppt.ma.

* Les autres termes et conditions restent inchangés.



المملكة المغربية

مكتب التكوين المهني وإنعاش الشغل إعلان تصحيحي لطلب العروض مفتوح دولي رقم 2024/98

ينهي مكتب التكوين المهني وإنعاش الشغل إلى علم العموم أنه قد أجريت تغييرات على ملف طلب العروض المفتوح رقم 2024/98، لأجل مشروع البنية التحتية والأمن SI لمكتب التكوين المهني وإنعاش الشغل على مستوى المقر الرئيسي و الإدارات الإقليمية.

1. قد أجريت تغييرات على ملف طلب العروض المفتوح.
2. تأجيل تاريخ فتح الأظرفة الى يوم 30 شتنبر 2024 على الساعة العاشرة صباحاً
3. إن النشرات التمهيدية ، الإشعارات أو وثائق أخرى التي يستوجبها ملف طلب العروض يجب إيداعها بمصلحة الصفقات بمديرية التموين واللوجستيك الكائنة بملتقى طريق BO. 50 والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء ، وذلك كحد أقصاه يوم 27 شتنبر 2024 على الساعة الرابعة بعد الزوال، إما تسليمها مباشرة لرئيس لجنة فتح الأظرفة عند بداية الجلسة الفورية.

يمكن سحب ملف طلب العروض المصحح بمصلحة الصفقات بمديرية التموين واللوجستيك الكائنة بملتقى طريق BO. 50 والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء ، كما يمكن كذلك سحبه إلكترونيا من بوابة صفقات الدولة : www.marchéspublics.gov.ma . وكذا من بوابة مكتب التكوين المهني وإنعاش الشغل على العنوان التالي: www.ofppt.ma.

- وأن جميع الشروط والمتطلبات الأخرى تبقى بدون تغيير.



ROYAUME DU MAROC

__**_**_**

OFFICE DE LA FORMATION PROFESSIONNELLE
ET DE LA PROMOTION DU TRAVAIL

AVIS RECTIFICATIF DE L'APPEL D'OFFRES OUVERT INTERNATIONAL
N°98/2024

L'Office de la Formation Professionnelle et de la Promotion du Travail porte à la connaissance du public que des modifications, ci-après, ont été apportées à l'avis d'appel d'offres ouvert international n° 98/2024, relatif au **Projet infrastructure et sécurité SI OFPPT au niveau Siège & directions régionales.**

- Les Prospectus, notices ou autre documents exigés par le dossier d'appel d'offres doivent être déposés au service des marchés à la **Direction de l'Approvisionnement et la Logistique, sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) Casablanca**, au plus tard le **16 Septembre 2024 à 16 Heures**, ou remis séance tenante au président de la Commission d'ouverture des plis.

Le dossier d'appel d'offres rectifié peut être téléchargé à partir du portail des marchés publics accessible à l'adresse www.marchéspublics.gov.ma.

*Les autres termes et conditions restent inchangés.

let n/1

W

المملكة المغربية

مكتب التكوين المهني وإنعاش الشغل إعلان تصحيحي لطلب العروض مفتوح دولي رقم 98/2024

ينهي مكتب التكوين المهني وإنعاش الشغل إلى علم العموم أنه قد أجريت تغييرات على إعلان طلب العروض المفتوح الدولي رقم 98/2024، لأجل مشروع البنية التحتية والأمن SI لمكتب التكوين المهني وإنعاش الشغل على مستوى المقر الرئيسي والإدارات الإقليمية.

- إن النشرات التمهيدية ، الإشعارات أو وثائق أخرى التي يستوجبها ملف طلب العروض يجب إيداعها بمصلحة الصفقات بمديرية التموين واللوجستيك الكائنة بملتقى طريق BO. 50 والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء ، وذلك كحد أقصاه يوم 16 شتنبر 2024 على الساعة الرابعة بعد الزوال، إما تسليمها مباشرة لرئيس لجنة فتح الأظرفة عند بداية الجلسة الفورية.

يمكن سحب ملف طلب العروض المصحح إلكترونيا من بوابة صفقات الدولة : www.marchéspublics.gov.ma

- وأن جميع الشروط والمتطلبات الأخرى تبقى بدون تغيير.

ش

ش
66

ROYAUME DU MAROC

__*_*_*_*_*

OFFICE DE LA FORMATION PROFESSIONNELLE
ET DE LA PROMOTION DU TRAVAIL

AVIS D'APPEL D'OFFRES OUVERT INTERNATIONAL N° 98/2024

Le **17 Septembre 2024 à 10 Heures**, Il sera procédé, dans les bureaux de l'office de la Formation Professionnelle et de la Promotion du Travail, sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) - Casablanca à l'ouverture des plis relatifs à l'appel d'offres sur offres de prix, ayant pour objet **Projet infrastructure et sécurité SI OFPPT au niveau Siege & directions régionales**

Le dossier d'appel d'offres doit être téléchargé à partir du portail des marchés publics accessible à l'adresse www.marchéspublics.gov.ma.

Le cautionnement provisoire est fixé à la somme de **trois cent mille Dirhams (300 000,00 DH)**

L'estimation des coûts des prestations établies par le Maître d'ouvrage est fixée à la somme de : **dix-sept millions trois cent soixante-quatorze mille neuf cent trente-deux Dirhams (17 374 932,00 DH) en TTC.**

Le contenu, la présentation ainsi que le dépôt des dossiers des concurrents doivent être conformes aux dispositions des articles 30 à 34 du décret relatif aux marchés publics.

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

Les pièces justificatives à fournir sont celles prévues par l'article n° 5 du règlement de consultation

un 1

المملكة المغربية
مكتب التكوين المهني وإنعاش الشغل
إعلان عن طلب عروض أثمان مفتوح دولي
رقم 2024/98

في يوم 17 شتنبر 2024 على الساعة العاشرة صباحاً، سيتم في مكتب الإدارة العامة لمكتب التكوين المهني وإنعاش الشغل الكائن بملتقى طريق BO. 50 والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء ، فتح الأظرفة المتعلقة بطلب عروض الأثمان المفتوح، لأجل مشروع البنية التحتية والأمن SI لمكتب التكوين المهني و انعاش الشغل على مستوى المقر الرئيسي و الإدارات الإقليمية.

يوجب سحب ملف طلب العروض إلكترونياً من بوابة صفقات الدولة من العنوان الإلكتروني
www.marchespublics.gov.ma

وتبلغ الضمانة المؤقتة ثلاث مئة ألف درهم (300 000,00)

والكلفة التقديرية للأعمال المحددة من طرف صاحب المشروع تبلغ سبعة عشر مليوناً و ثلاثمائة وأربعة و سبعون ألفاً و تسعمائة و اثنان و ثلاثون درهم (17 374 932,00) مع احتساب جميع الرسوم.

يجب أن يكون كل من محتوى وتقديم ملفات المتنافسين مطابقين لمقتضيات البنود من 30 إلى 34 من المرسوم المنظم للصفقات العمومية.

ويجب على المتنافسين أن يرسلوا أظرفتهم إلكترونياً في بوابة الصفقات العمومية من العنوان الإلكتروني
www.marchespublics.gov.ma

إن الوثائق المثبتة الواجب الإدلاء بها هي تلك المقررة في المادة 5 من نظام الإستشارة.

Oct 1

ROYAUME DU MAROC

MAITRE D'OUVRAGE OFFICE DE LA FORMATION PROFESSIONNELLE ET DE LA PROMOTION DU TRAVAIL

Dossier d'Appel d'offres ouvert international N° 98/2024

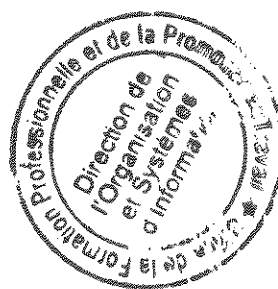
Objet de l'Appel d'Offres :

PROJET INFRASTRUCTURE ET SECURITE SYSTEME
D'INFORMATION DE L'OFPPT AU NIVEAU DU SIEGE & DES
DIRECTIONS REGIONNALES



Handwritten signature and initials.

REGLEMENT DE LA CONSULTATION



Handwritten marks: a checkmark, a circle with a dot, and a stylized signature.

ARTICLE 1 : Objet de règlement de la consultation

Le présent règlement de consultation concerne l'appel d'offres ouvert international, ayant pour objet : projet infrastructure et sécurité système d'information de l'OFPPT au niveau du siège & des directions régionales.

Il est établi en vertu des dispositions de l'article 21, du décret N°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics.

Les prescriptions du présent règlement ne peuvent en aucune manière déroger ou modifier les conditions et les formes prévues par le décret sus cité. Toute disposition contraire à ce décret est nulle et non avenue. Seules sont valables les précisions et prescriptions complémentaires conformes aux dispositions de l'article n°21 susmentionné et des autres articles du décret précité.

ARTICLE 2 : MAITRE D'OUVRAGE

Le maître d'ouvrages du marché qui sera passé à la suite du présent appel d'offres est : l'**Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT)**.

ARTICLE 3 : DEFINITIONS

Au sens du décret n°2-22-431 relatif aux marchés publics on entend par :

1. **Attributaire** : le concurrent dont l'offre a été retenue avant que l'approbation du marché ne lui soit notifiée;
2. **Autorité compétente** : l'ordonnateur ou la personne déléguée par lui à l'effet d'approuver le marché ou toute autre personne habilitée à cet effet par un texte législatif ou réglementaire ;
3. **Concurrent** : toute personne physique ou morale qui participe à un appel à la concurrence dans sa phase antérieure à la remise des offres ou à une procédure négociée avant l'attribution du marché ou qui propose une offre en vue de la conclusion d'un marché ;
4. **Groupeement** : deux ou plusieurs concurrents qui souscrivent un engagement unique, dans les conditions prévues à l'article 150 du décret n°2-22-431 relatif aux marchés publics ;
5. **Maître d'ouvrage** : l'autorité compétente ou toute personne désignée par elle en vertu d'une décision à l'effet d'assurer la préparation, la passation et l'exécution des marchés publics au nom et pour le compte de l'OFPPT.
6. **Titulaire** : attributaire auquel l'approbation du marché a été notifiée.

ARTICLE 4 : CONDITIONS REQUISES DES CONCURRENTS

Conformément aux dispositions de l'article n°27 du Décret n°2-22-431 relatif aux marchés publics :

Peuvent, valablement, participer et être attributaire des marchés publics, dans le cadre des procédures prévues par le décret n°2-22-431 relatif aux marchés publics, les personnes physiques ou morales qui :

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

Ne sont pas admises à participer aux appels d'offres :

- Les personnes en liquidation judiciaire ;
- Les personnes en redressement judiciaire, sauf autorisation spéciale délivrée par l'autorité judiciaire compétente ;



- Les personnes ayant fait l'objet d'une décision d'exclusion temporaire ou définitive prise conformément aux dispositions de l'article 152 du décret n°2-22-431 relatif aux marchés publics ;
- Les personnes qui représentent plus d'un concurrent dans un même marché, lorsqu'il s'agit d'un marché en lot unique ou d'un même lot lorsqu'il s'agit d'un marché alloti ;
- Les prestataires de services ayant contribué à la préparation du présent dossier de l'appel d'offres ;
- Les titulaires dont les marchés ont fait l'objet de résiliation pour une faute qui leur incombe au titre des marchés d'achèvement y afférents.

ARTICLE 5 : JUSTIFICATION DES CAPACITES ET DES QUALITES DES CONCURRENTS

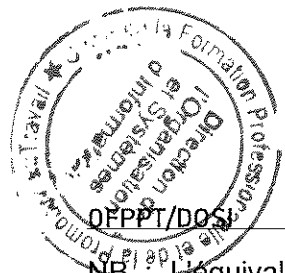
Conformément aux dispositions de l'article 28 du décret 2-22-431 précité, Chaque concurrent est tenu de présenter un dossier administratif et un dossier technique.

A-Un dossier administratif comprenant :

- 1- Pour chaque concurrent au moment de la présentation des offres :
 - a) La ou les pièces justifiant les pouvoirs conférés à la personne agissant au nom du concurrent. Ces pièces varient selon la forme juridique du concurrent :
 - S'il s'agit d'un auto-entrepreneur ou d'une personne physique agissant pour son propre compte, aucune pièce n'est exigée ;
 - S'il s'agit d'un représentant du concurrent, celui-ci doit présenter, selon le cas
 - ✓ Une copie certifiée conforme de la procuration légalisée, lorsqu'il agit au nom d'une personne physique ;
 - ✓ Un extrait des statuts de la société et/ou copie certifiée conforme à l'original du procès-verbal de l'organe compétent lui conférant le pouvoir d'agir au nom de cette société ;
 - ✓ L'acte par lequel la personne habilitée délègue son pouvoir à une tierce personne, le cas échéant.
 - S'il s'agit d'une coopérative ou d'une union de coopératives, la ou les pièces justifiant les pouvoirs conférés à la personne agissant au nom de la coopérative ou de l'union de coopératives
 - b) La déclaration sur l'honneur ;
 - c) L'original du récépissé du cautionnement provisoire ou l'attestation de la caution personnelle et solidaire en tenant lieu, le cas échéant ;

En cas de groupement, le cautionnement provisoire doit être constitué conformément aux dispositions du § C de l'article n°150 du décret n°2-22-431 du 15 Chaâbane 1444 (8 mars 2023) relatif aux marchés publics.
 - d) La convention constitutive du groupement prévue à l'article 150 du décret n°2-22-431 relatif aux marchés publics ou sa copie certifiée conforme, lorsque le concurrent est un groupement.
- Les pièces a), b) et c) ne doivent exprimer aucune restriction ou réserve sous peine d'être rejetées par la commission d'appel d'offres.
- 2- Pour le concurrent auquel il est envisagé d'attribuer le marché dans les conditions fixées à l'article 43 du décret n°2-22-431 relatif aux marchés publics :
 - a) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu à l'article 27 du décret n°2-22-431 relatif aux marchés publics. Cette attestation doit mentionner l'activité au titre de laquelle le concurrent est imposé.
 - b) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale ou par tout autre organisme de prévoyance sociale certifiant que le concurrent est en situation régulière envers l'organisme concerné ;
 - c) Une copie du certificat d'immatriculation au registre de commerce (modèle 9) pour les personnes assujetties à l'obligation d'immatriculation au registre de commerce en vertu de la législation en vigueur ;

09 2



NB. L'équivalent des attestations visées aux paragraphes a), b) et c) ci-dessus, délivrées par les administrations ou les organismes compétents de leurs pays d'origine ou de provenance, pour les concurrents non installés au Maroc.

A défaut de délivrance de ces documents par les administrations ou les organismes compétents, ils sont remplacés par une attestation délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que les documents précités ne sont pas produits.

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

B. Le dossier technique :

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

Chaque attestation précise, notamment, la nature des prestations, leur montant et l'année de réalisation, le nom et la qualité du signataire et son appréciation.

Lorsque le concurrent est un **établissement public**, il doit fournir :

- 1- Au moment de la présentation de l'offre, outre le dossier technique et les pièces du dossier administratif prévues aux b) et c) de l'alinéa 1 du A du I) du présent article, une copie du texte l'habilitant à exercer les missions en relation avec les prestations objet du marché.
- 2- S'il est envisagé de lui attribuer le marché :
 - a) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant qu'il est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu par l'article 27 du décret n°2-22-431 relatif aux marchés publics.

Cette attestation doit mentionner l'activité au titre de laquelle le concurrent est imposé.
L'attestation précitée n'est exigée que des établissements publics soumis à l'impôt.
 - b) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale ou tout autre organisme de prévoyance sociale certifiant que le concurrent est en situation régulière envers l'organisme concerné.

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

Lorsque le concurrent est **une coopérative ou une union de coopératives**, il doit fournir :

- 1- Au moment de la présentation de l'offre, outre le dossier technique et les pièces du dossier administratif, prévues aux a), b) et c) de l'alinéa 1 du A du I) du présent article, l'attestation d'immatriculation au registre local des coopératives.
- 2- Et lorsqu'il est envisagé de lui attribuer le marché :
 - a) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu à l'article 27 du décret n°2-22-431 relatif aux marchés publics.

Cette attestation doit mentionner l'activité au titre de laquelle la coopérative ou l'union de coopératives est imposée ;
 - b) Une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale certifiant que la coopérative ou l'union de coopératives est en situation régulière envers cet organisme conformément aux dispositions de l'article 27 du décret n°2-22-431 relatif aux marchés publics.

Q 7 2

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

Lorsque le concurrent est une **auto-entrepreneur**, il doit fournir :

- 1- Au moment de la présentation de l'offre, outre le dossier technique et les pièces du dossier administratif, prévues aux b) et c) de l'alinéa 1) du A du l) du présent article, l'attestation d'immatriculation au registre national de l'auto-entrepreneur ou sa copie certifiée conforme à l'original, délivrée depuis moins d'un an.
- 2- Et lorsqu'il est envisagé de lui attribuer le marché, une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties tel que prévu à l'article 27 du décret n°2-22-431 relatif aux marchés publics.

Cette attestation doit mentionner l'activité au titre de laquelle l'auto-entrepreneur est imposé.

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

ARTICLE 6 : OFFRE FINANCIÈRE

Chaque concurrent doit présenter une offre financière comprenant :

- 1- L'acte d'engagement par lequel le concurrent s'engage à réaliser les prestations objet du marché conformément aux conditions prévues aux cahiers des charges et moyennant un prix qu'il propose. Il est établi en un seul exemplaire.

Cet acte d'engagement, signé par le concurrent ou son représentant dûment habilité, doit comporter l'ensemble des indications requises y compris le relevé d'identité bancaire (RIB).

Le montant total de l'acte d'engagement doit être libellé en chiffres et en toutes lettres, en tenant compte du rabais éventuel.

Lorsque l'acte d'engagement est souscrit par un groupement tel qu'il est défini à n°150 du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics, 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.

- 2- Le bordereau des prix - détail estimatif figurant dans le dossier d'appel d'offres.

Les prix unitaires du bordereau des prix- détail estimatif doivent être libellés en chiffres.

Les montants totaux du bordereau des prix-détail estimatif doivent être libellés en chiffres.

En cas de discordance entre le montant total de l'acte d'engagement et 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 prévaut pour établir le montant réel de l'acte d'engagement.

Article 7 : OFFRE TECHNIQUE

Conformément aux dispositions de l'article 31 du décret 2-22-431 précité, Chaque concurrent est tenu de présenter :

- Garanties offertes au titre de la prestation :

- o La décision de la DGSSI « Direction Générale de la sécurité de système d'information » portant sur la qualification du concurrent en qualité de prestataire d'audit de la sécurité de système d'information « PASSI » ;
- o Le classement du concurrent par les cabinets d'analystes (tels que Gartner, IDC, Forrester, ou équivalent) dans le domaine des services de conseil en cybersécurité ou équivalent, dans leurs derniers rapports ;
- o Une attestation de(s) constructeur(s) ou éditeur (s) (maison mère, représentant Régional ou local) certifiant que le concurrent est un partenaire, autorisé à commercialiser, intégrer et assurer le support technique des solutions proposées de la partie 2 et des items 3.1 et 3.2 de la partie 3.

- o Une attestation par le constructeur qui confirme que les équipements proposés, dans le cadre de la partie 2, ne seront pas en End-of-Sale ou End-of-Life pour une période de 5 ans au minimum ;
- **L'expérience spécifique et le profil du personnel par rapport à la nature des prestations ;**
 - o Minimum un (01) Chef de projet de formation supérieure (Bac+5 ou MBA) ayant une expérience de 10 ans minimum dans la gestion de projets de sécurité complexes et de grandes envergures ;
 - o Minimum un consultant senior pour la partie 1, de formation supérieure de (Bac+5) en rapport avec la mission, ayant une expérience de 5 ans minimum, et ayant minimum 3 certifications dans les domaines de la partie 1.
 - o Minimum un consultant senior pour la partie 2, de formation supérieure de (Bac+5) en rapport avec la mission, ayant une expérience de 5 ans minimum, et ayant minimum 3 certifications dans les domaines de la partie 2.
 - o Minimum un consultant senior pour la partie 3, de formation supérieure de (Bac+5) en rapport avec la mission, ayant une expérience de 7 ans minimum, et ayant minimum 1 certification dans les domaines de la partie 3.
 - o Minimum un consultant senior pour la partie 4, de formation supérieure de (Bac+5) en rapport avec la mission, ayant une expérience de 7 ans minimum, et ayant minimum 1 certification dans les domaines de la partie 4.

NB : Le concurrent doit présenter pour les profils demandés :

- Les Curriculum vitae des profils proposés doivent indiquer au minimum la partie du CPS objet de leurs interventions, ainsi que leurs diplômes, leurs expériences notamment dans des projets similaires, et leurs certifications dans le domaine d'intervention. Ces CV doivent être dûment cosignés par l'intervenant et le soumissionnaire.
- Les copies certifiées conformes des diplômes des intervenants ;
- Les certifications demandées des intervenants.
- **Méthodologie et organisation proposée :**
 - o La méthodologie proposée, en précisant les avantages techniques qu'elle apporte ;
 - o Présentation détaillée de l'offre technique ressortissant :
 - Les qualités fonctionnelles de la prestation ;
 - Le caractère innovant de l'offre ;
 - La qualité de l'assistance technique ;
 - Le degré de transfert de compétences et de connaissances ;
 - o Le planning envisagé pour la réalisation du projet et décrivant l'ordonnancement des tâches ;
 - o Le chronogramme d'affectation des ressources ;
 - o Le service après-vente des solutions proposées ;

Article 8 : Prospectus, notices et tout autre document technique

Les concurrents sont tenus de présenter les prospectus, notices ou autres documents techniques pour l'ensemble des articles objet du présent appel d'offres. A ce titre, les spécifications techniques desdits articles doivent être renseignés conformément au canevas en annexe du cahier des prescriptions spéciales et ce en faisant ressortir les caractéristiques des articles proposées par le concurrent, **leurs marques et leurs références**.

L'ensemble des documents précités doivent être cachetés sur toutes les pages et portant le numéro de l'appel d'offres et de l'item correspondant. En cas de groupement ces documents sont à signer par l'ensemble 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.

L'ensemble de ces documents sont mis dans un pli distinct déposé au plus tard le jour ouvrable précédant la date d'ouverture des plis contre délivrance par le maître d'ouvrage d'un accusé de réception ou remis, séance tenante, au président de la commission d'appel d'offres, conformément à l'article n°37 du décret. Ce pli doit être fermé et porter de façon apparente la mention « prospectus notices ou autres documents techniques ».

La documentation présentée par les concurrents doit être rédigée de préférence en langue française.



ARTICLE 9 : CONTENU DES DOSSIERS DES CONCURRENTS

Le dossier du concurrent doit contenir trois enveloppes électroniques distinctes :

- La première enveloppe électronique contient, outre les pièces des dossiers administratif et technique prévus à l'article 5 du présent règlement, le cahier des prescriptions spéciales et le règlement de consultation paraphés et signés électroniquement et portant la mention « lu et accepté » par le concurrent ou son représentant dûment habilité ;
- La deuxième enveloppe électronique contient l'offre technique prévue à l'article 7 ;
- La troisième enveloppe électronique contient l'offre financière prévue à l'article 6

Ces dossiers doivent être présentés exclusivement de façon électronique via le portail des marchés publics conformément aux dispositions de l'arrêté du ministre délégué auprès de la ministre de l'économie et des finances chargé du budget n° 1692-23 du 23 juin 2023 relatif à la dématérialisation des procédures, des documents et des pièces relatives aux marchés Publics.

Outre le dossier électronique prévu au premier paragraphe ci-dessus, le concurrent est tenu de présenter, un pli distinct contenant les prospectus, notices ou autres documents techniques, prévus dans l'article 8, déposé au plus tard le jour ouvrable précédant la date d'ouverture des plis auprès du service de Marchés de l'OFPPT contre délivrance d'un accusé de réception ou remis, séance tenante, au président de la commission d'appel d'offres, conformément à l'article n°37 du décret 2-22-431 précité.

Ce pli doit être fermé et porter de façon apparente :

- Le nom et l'adresse du concurrent ;
- L'objet du marché et, le cas échéant, l'indication du ou des lots en cas de marché alloti ;
- La date et l'heure de la séance d'ouverture des plis ;
- L'avertissement que « le pli ne doit être ouvert que par le président de la commission d'appel d'offres lors de la séance publique d'ouverture des plis ».
- La mention « prospectus, notices ou autres documents techniques »

ARTICLE 10 : OFFRE VARIANTE

La présentation des offres variantes par rapport à la solution de base prévue par le cahier des prescriptions spéciales n'est pas autorisée.

ARTICLE 11 : COMPOSITION DU DOSSIER D'APPEL D'OFFRES

Conformément aux dispositions de l'article 22 du décret n°2-22-431 relatif aux marchés publics, le dossier d'appel d'offres ouvert international comprend :

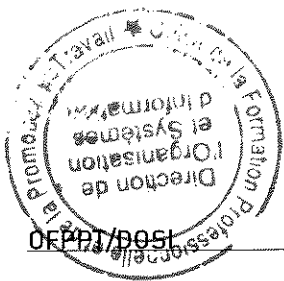
- Une copie de l'avis d'appel d'offres ouvert international ;
- Un exemplaire du cahier des prescriptions spéciales ;
- Le modèle de l'acte d'engagement visé à l'article 5 précité ;
- Le modèle du bordereau des prix - détail estimatif ;
- Le modèle de la déclaration sur l'honneur prévue à l'article 5 précité ;
- Le présent règlement de la consultation.

ARTICLE 12 : DEMANDES D'ECLAIRCISSEMENT OU DE RENSEIGNEMENT ET INFORMATION DES CONCURRENTS

Tout concurrent peut demander au maître d'ouvrage, par lettre transmise par tout moyen pouvant donner date certaine, de lui fournir des éclaircissements ou renseignements concernant l'appel d'offres ou les documents y afférents. Cette demande n'est recevable que si elle parvient au maître d'ouvrage au moins sept jours avant la date prévue pour la séance d'ouverture des plis.

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

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



OFFPPT/DOSI

Dossier d'Appel d'Offres

A0. N°98/2024

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

ARTICLE 13 : MODIFICATION DANS LE DOSSIER D'APPEL D'OFFRES OUVERT INTERNATIONAL

Conformément aux dispositions de l'article n°22 § 7 et 8 du décret n°2-22-431 relatif aux marchés publics, le maître d'ouvrage peut introduire, à titre exceptionnel, des modifications dans le dossier d'appel d'offres sans changer l'objet du marché. Dans ce cas, ces modifications sont communiquées à tous les concurrents ayant retiré ou téléchargé ledit dossier, et introduites dans les dossiers mis à la disposition des autres concurrents.

Ces modifications peuvent intervenir à tout moment à l'intérieur du délai initial de publicité et au plus tard sept jours avant la date de la séance d'ouverture des plis.

Passé ce délai, le maître d'ouvrage doit, par avis rectificatif, reporter la date de la séance d'ouverture des plis.

Lorsque les modifications introduites dans le dossier d'appel d'offres nécessitent la publication d'un avis rectificatif, celui-ci est publié conformément aux dispositions du premier alinéa du deuxième paragraphe de l'article 23 du décret précité.

Dans ce cas, la séance d'ouverture des plis ne peut être tenue qu'après l'expiration d'un délai minimum de dix jours. Ce délai court à partir du lendemain de la date de parution de l'avis rectificatif dans le dernier support de publication, sans que la date de la nouvelle séance ne soit antérieure à celle prévue par l'avis de publicité initial.

Dans tous les cas, le délai de publicité prévu au troisième alinéa du deuxième paragraphe du I) de l'article 23 du décret précité doit être respecté.

Les concurrents ayant retiré ou téléchargé le dossier d'appel d'offres, doivent être informés des modifications qui y ont été apportées et de la nouvelle date d'ouverture des plis, le cas échéant.

Lorsqu'un concurrent estime que le délai prévu par l'avis de publicité pour la préparation des offres n'est pas suffisant au regard de la complexité des prestations objet du marché, il peut, au cours de la première moitié du délai de publicité, demander au maître d'ouvrage, par lettre transmise par tout moyen pouvant donner date certaine, le report de la date de la séance d'ouverture des plis. Cette lettre doit comporter tous les éléments permettant au maître d'ouvrage d'apprécier la demande de report.

Si le maître d'ouvrage reconnaît le bien-fondé de la demande du concurrent dont il est saisi, il procède au report de la date de la séance d'ouverture des plis. Le report, dont la durée est laissée à l'appréciation du maître d'ouvrage, fait l'objet d'un avis rectificatif qui est publié dans les mêmes formes que l'avis d'appel d'offres.

Il ne peut être procédé au report de la date de la séance d'ouverture des plis qu'une seule fois, quel que soit le concurrent qui le demande.

ARTICLE 14 : DÉPÔT DES PLIS DES CONCURRENTS.

Conformément aux dispositions des articles 34 et 135 du décret n° 2.22.431 précité et aux dispositions de l'arrêté du ministre délégué auprès de la ministre de l'économie et des finances chargé du budget n° 1692-23 du 23 juin 2023, relatif à la dématérialisation des procédures de passation des marchés publics et des garanties pécuniaires, les plis doivent être transmis **exclusivement** par voie électronique via le portail des marchés publics www.marchespublics.gov.ma

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

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

092

Lorsqu'il s'agit d'un groupement, ces pièces sont signées, soit par l'ensemble des membres du groupement, soit uniquement par le mandataire conformément aux dispositions du paragraphe C) de l'article 150 du décret n° 2-22-431.

Tout pli électronique déposé postérieurement à la date limite de remise des plis est automatiquement rejeté par le portail des marchés publics.

ARTICLE 15 : RETRAIT DES PLIS DES CONCURRENTS.

Tout pli déposé 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 dépôt des plis.

Les concurrents ayant retiré leurs plis peuvent présenter de nouveaux plis dans les conditions prévues au présent chapitre et avant la date et l'heure limites d'ouverture des plis.

ARTICLE 16 : DELAI DE VALIDITE DES OFFRES

Les concurrents restent engagés par leurs offres pendant un délai de soixante jours qui commence à courir, selon le cas, à compter de la date de la séance d'ouverture des plis ou de la date de signature du marché par l'attributaire dans le cas d'un marché négocié.

Toutefois, lorsque la commission d'appel d'offres considère qu'elle n'est pas en mesure d'effectuer son choix pendant le délai de validité des offres prévu à l'alinéa précédent, le maître d'ouvrage saisit les concurrents concernés, avant l'expiration de ce délai, par lettre recommandée avec accusé de réception, en vue de leur demander une prorogation du délai de validité des offres d'une durée supplémentaire qu'il fixe.

A cet effet, le maître d'ouvrage fixe aux concurrents concernés une date limite pour faire connaître leurs réponses.

Dans ce cas :

- a) Les concurrents ayant donné, dans les mêmes formes, leur accord à la demande de prorogation, avant la date limite de réponse fixée par le maître d'ouvrage, restent engagés pendant le délai supplémentaire convenu ;
- b) Les concurrents qui n'ont pas donné leur accord à la demande de prorogation ou qui n'ont pas répondu dans le délai qui leur est imparti sont libérés de leurs engagements vis-à-vis du maître d'ouvrage et mainlevée leur est donnée de leur cautionnement provisoire, au plus tard quarante-huit heures à compter de la date limite de réponse fixée par le maître d'ouvrage ;

ARTICLE 17 : LANGUE DE L'OFFRE

L'offre préparée par le concurrent ainsi que toute correspondance et tous documents concernant l'offre échangée entre le candidat et l'OFPPT seront rédigés en Langue Française ou en langue arabe.

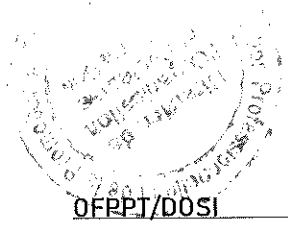
ARTICLE 18 : MONNAIE DE L'OFFRE

La ou les monnaies convertibles dans lesquelles le prix des offres doit être formulé et exprimé, lorsque le concurrent n'est pas installé au Maroc. Dans ce cas, pour être évalués et comparés, les montants des offres exprimées en monnaies étrangères doivent être convertis en dirham. Cette conversion doit s'effectuer sur la base du cours vendeur du dirham en vigueur le premier jour ouvrable de la semaine précédant celle du jour d'ouverture des plis donné par Bank Al-Maghrib.

ARTICLE 19 : DEPENSES ENCOURUES DU FAIT DE L'APPEL D'OFFRES

Le concurrent supporte toutes les dépenses encourues du fait de la préparation et de la présentation de son offre à l'OFPPT qui ne pourra, en aucun cas, en être tenu pour responsable, quel que soit le déroulement ou l'issue de la procédure d'appel d'offres.





ARTICLE 20 : EVALUATION DES OFFRES DES CONCURRENTS

Les offres des concurrents sont examinées conformément aux dispositions des articles 21, 39, 40, 41, 42, 43 et 44 du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics.

Les capacités techniques et financières des concurrents seront appréciées comme suit :

Seuls seront retenus, les concurrents ayant présenté au moins deux attestations de références, conformes aux prescriptions de l'article 5-alinéa B-2 du présent règlement de consultation, se rapportant à des prestations de la même nature de celles objet du présent appel d'offres, dont le montant est minimum de 50 % de l'estimation du présent appel d'offre, réalisées au cours des 5 dernières années

Aussi, il est précisé qu'en cas d'attestation délivrée à un groupement, celle-ci sera appréciée pour la cote part réalisé par le (s) concurrent(s) ou à défaut de renseignement, pour part égale du montant globale de l'attestation.

Les prospectus, notices ou autres documents techniques seront évalués comme suit :

Dans cette phase, ne sont examinés que les prospectus, notices ou autres documents techniques des concurrents retenus à l'issue de l'examen des dossiers administratif et technique.

Seuls seront retenus, les concurrents ayant proposés des « spécifications techniques des solutions » des fiches ou documentation techniques conforme aux spécifications techniques prévues par le cahier des prescriptions spéciales.

Tout item ne répondant pas aux spécifications techniques demandées sera déclaré non conforme.

Tout concurrent ayant une non-conformité par rapport aux spécifications techniques prévues par le cahier des prescriptions spéciales sera écarté.

Les offres techniques seront évaluées comme suit :

Dans cette phase, ne sont examinés que les offres des concurrents retenues à l'issue de l'examen des prospectus, notices ou autres documents techniques.

Pendant cette phase, il sera procédé de l'évaluation des offres techniques sur la base des éléments contenus dans les dossiers des concurrents, et une note technique « Nt » sur 100 points sera attribuée à chaque offre sur la base du barème suivant : $Nt = N1 + N2 + N3$

N1 : Garanties offertes au titre de la prestation

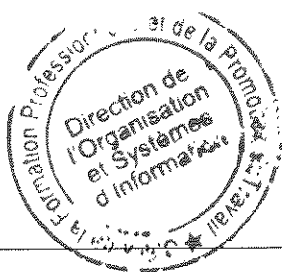
N2 : Note sur l'expérience et la qualification des intervenants

N3 : Note sur la méthodologie et l'organisation du projet

A. Garanties offertes au titre de la prestation. Une note sur 15 points

Critère d'évaluation	Barème de notation
Qualification du concurrent en qualité de prestataire d'audit de la sécurité de système d'information « PASSI » par une décision de la DGSSI « Direction Générale de la sécurité de système d'information »	Décision présentée : offre retenue Décision non présentée : offre écarté
Classement du concurrent par les cabinets d'analystes (tels que Gartner, IDC, Forrester, ou équivalent) dans le domaine des services de conseil en cybersécurité ou équivalent, dans leurs derniers rapports ;	Premier rang du classement (Leader) : 15 points Deuxième rang du classement (Strong performer, major players) : 5 points troisième rang du classement ou inférieur: 0 point

09 7



OFPPT/DOSI

Dossier d'Appel d'Offres

AO. N°98/2024

Une attestation de(s) constructeur(s) ou éditeur (s) (maison mère, représentant Régional ou local) certifiant que le concurrent est un partenaire, autorisé à commercialiser, intégrer et assurer le support technique des solutions proposées de la partie 2 et des items 3.1 et 3.2 de la partie 3.	Attestation présentée : offre retenue Attestation nom présentée : offre écarté
Une attestation par le constructeur qui confirme que les équipements proposés, dans le cadre de la partie 2, ne seront pas en End-of-Sale ou End-of-Life pour une période de 5 ans au minimum ;	Attestation présentée : offre retenue Attestation nom présentée : offre écarté

B. L'expérience spécifique et le profil du personnel par rapport à la nature des prestations. Une note sur 40 points

Critère d'évaluation	Barème de notation
Un Chef de Projet (Note maximale 8)	
Diplôme Formation supérieure de Bac+5 ou MBA	OUI : 2 points Non : 0 point
Nombre d'années d'expérience avec des missions similaires	≥20 ans : 6 points Entre 10 et 19 ans : 3 points < 10 ans : 0 points <u>Si le profil proposé à une expérience inférieure à 10 ans, le profil se fera attribué une note zéro</u>
Un Consultant sénior de la Partie 1 (Note maximale 8)	
Diplôme : Formation supérieure de Bac+5 en rapport avec la mission	OUI : 2 points Non : 0 point
Nombre d'années d'expérience avec des missions similaires	≥10 ans : 3 points Entre 5 et 9 ans : 2 point < 5 ans : 0 points <u>Si le profil proposé à une expérience inférieure à 5 ans, le profil se fera attribué une note zéro</u>
Certifications Certificats en rapport avec la mission de la partie 1	≥ 5 certifications : 3 points Entre 3 et 4 certifications : 1 point < 3 certifications : 0 point <u>Si le profil proposé ne dispose d'aucune certification, le profil se fera attribué une note zéro.</u>

07 7

**Un Consultant sénior de la partie 2 (Note maximale 8)****Diplôme**

Formation supérieure de Bac+5 en rapport avec la mission

OUI : 2 points

Non : 0 point

Nombre d'années d'expérience avec des missions similaires

≥10 ans : 3 points

Entre 5 et 9 ans : 2 point

< 5 ans : 0 points

Si le profil proposé à une expérience inférieure à 5 ans, le profil se fera attribué une note zéro

Certifications

Certifications par l'éditeur/constructeur dans la solution proposée dans la partie 1

≥ 5 certifications : 3 points

Entre 3 et 4 certifications : 1 point

< 3 certifications : 0 point

Si le profil proposé ne dispose d'aucune certification, le profil se fera attribué une note zéro.

Un Consultant sénior de la partie 3 (Note maximale 8)**Diplôme**

Formation supérieure de Bac+5 en rapport avec la mission

OUI : 2 points

Non : 0 point

Nombre d'années d'expérience avec des missions similaires

≥15 ans : 4 points

Entre 7 et 14 ans : 2 point

<7 ans : 0 points

Si le profil proposé à une expérience inférieure à 7 ans, le profil se fera attribué une note zéro

Certifications

Certificats en rapport avec la mission de la partie 3

≥ 3 certifications : 2 points

Entre 1 et 2 certifications : 1 point

Néant : 0 point

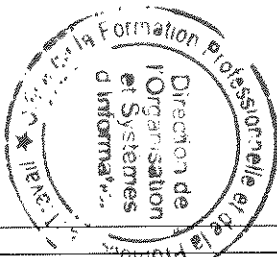
Si le profil proposé ne dispose d'aucune certification, le profil se fera attribué une note zéro.

Un Consultant sénior de la partie 4 (Note maximale 8)**Diplôme**

Formation supérieure de Bac+5 en rapport avec la mission

OUI : 2 points

Non : 0 point

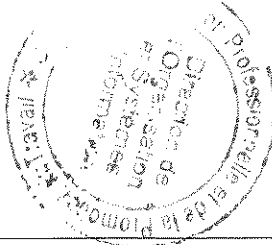


Nombre d'années d'expérience avec des missions similaires	≥15 ans : 4 points Entre 7 et 14 ans : 2 point <7 ans : 0 points <u>Si le profil proposé à une expérience inférieure à 7 ans, le profil se fera attribué une note zéro</u>
Certifications Certificats en rapport avec la mission de la partie 4	≥ 3 certifications : 2 points Entre 1 et 2 certifications : 1 point Néant : 0 point <u>Si le profil proposé ne dispose d'aucune certification, le profil se fera attribué une note zéro.</u>

C. Méthodologie et organisation proposée. Une note sur 45 points

Critère d'évaluation	Approche d'évaluation	Barème de notation
Méthodologie	Méthodologie claire et détaillée	10< Note ≤15
	Méthodologie moyennement claire	5< Note ≤10
	Méthodologie pas claire ou insuffisante	Note≤5
Présentation de l'offre	Présentation claire et fondée	10< Note ≤15
	Présentation moyennement claire et fondée	5< Note ≤10
	Présentation pas claire ou insuffisante	Note≤5
Planning de réalisation	Planning détaillé et pertinent	03< Note ≤5
	Planning peu détaillé et conforme au CPT	1 ≤Note ≤03
	Planning non détaillé ou non conforme	Note = 0 points
Chronogramme d'affectation des ressources	Chronogramme détaillé et pertinent	03< Note ≤5
	Chronogramme peu détaillé et conforme au CPT	1 ≤Note ≤03
	Chronogramme non détaillé ou non conforme	Note = 0 points
Service après-vente des solutions proposées	Service après-vente bien organisé et pertinent	03< Note ≤5
	Service après-vente moyennement organisé et pertinent	1 ≤Note ≤03
	Service après-vente non pertinent	Note = 0 points

272

**Sont considérés éliminés, les offres techniques de tout concurrent :**

- N'ayant pas présenté l'une des pièces demandées dans l'offre technique ;
- N'ayant pas présenté la décision de la DGSSI « Direction Générale de la sécurité de système d'information » portant sur la qualification du concurrent en qualité de prestataire d'audit de la sécurité de système d'information « PASSI » ;
- Ayant une position de troisième rang ou inférieure dans le classement des cabinets d'analystes (tels que Gartner, IDC, Forrester, ou équivalents) dans le domaine des services de conseil en cybersécurité dans leurs derniers rapports.
- Ayant obtenu une note technique globale (NT) strictement inférieure à 70/100 points.

Seront admis à la phase d'évaluation finale, les concurrents ayant obtenu une note technique Nt **supérieure ou égale à 70 points**.

Les offres financières seront évaluées comme suit :

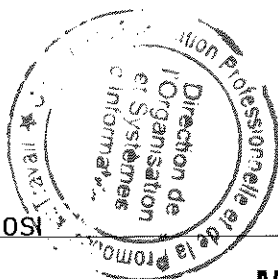
Conformément aux dispositions des articles 42, 43 et 44 du décret précité, l'examen des offres financières concerne les seuls concurrents admis à l'issue de l'examen de leurs dossiers administratifs, techniques, des prospectus notices, documents techniques et de leurs offres techniques.

Un taux de quinze pour cent (15%) à appliquer dans le cadre de la préférence nationale prévue à l'article 147 du décret précité.

Le marché sera attribué au concurrent, retenu à l'issu de l'examen des dossiers administratifs et techniques, des prospectus notices, documents techniques, des offres techniques et de l'offre financière économiquement la plus avantageuse.

Etabli par : effendi el ghannouchi	Vérifié par le Service des Marchés : Achraf HAJJAJI Chef de Service des Marchés
Le maître d'ouvrage Direction Organisation et Système d'information Mme Farah ZAHRAOUI Directeur de l'Organisation et Système d'Information PI	
Le concurrent Lu et accepté	

90

**MODELE DE L'ACTE D'ENGAGEMENT****ACTE D'ENGAGEMENT**

A-Partie réservée à l'Office de la Formation Professionnelle et de la Promotion du Travail

Appel d'offres ouvert international n° du

Objet du marché : Projet infrastructure et sécurité système d'information de l'OFPPT au niveau du siège & des directions régionales.

Passé en application de l'article 19 du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics

B - Partie réservée au concurrent :

a) Pour les personnes physiques : (3)

Je, soussigné : (Prénom, nom et qualité) (1)

Agissant en mon nom personnel et pour mon propre compte, (1)

Adresse du domicile élu :

Numéro tél : Adresse électronique :

Affilié à (4)..... sous le n° : (2)

Inscrit au registre du commerce de..... (Localité) sous le n° (2)

n° de patente..... (2)

Numéro de l'identifiant commun de l'entreprise : (2)

N° du compte courant postal, bancaire ou à la TGR.....(RIB), ouvert auprès de;

b) Pour les personnes morales

Je, soussigné (Prénom, nom et qualité au sein de l'entreprise) (1)

Agissant au nom et pour le compte de..... (Raison sociale et forme juridique de la société) (1)

au capital de :

Adresse du siège social de la société.....

adresse du domicile élu.....

Numéro de tél :Fax.....

adresse électronique :

Affiliée à (4)..... sous le n°.....(2)

Inscrite au registre du commerce..... (Localité) sous le n°.....(2)

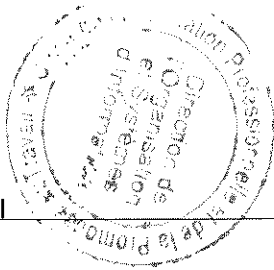
N° de patente.....(2)

N° du compte courant postal, bancaire ou à la TGR.....(RIB), ouvert auprès de

N° de taxe professionnelle (2)

N° de l'Identifiant Commun de l'Entreprise :(2)

702

**c) Pour les coopératives ou union de coopératives (3)**

Je, soussigné (Prénom, nom et qualité au sein de la coopérative) (1)
Agissant au nom et pour le compte de..... (Dénomination de la coopérative ou de l'union de coopératives) au capital de:..... (1)
Adresse du siège de la coopérative ou de l'union de coopératives.....
Numéro de tél : Fax
adresse électronique :
Affiliée à (4)..... sous le n°.....(2)
Inscrite au registre local du coopérative n°..... (Localité) sous le n°.....(2)
N° de patente.....(2)
N° du compte courant postal, bancaire ou à la TGR.....(RIB), ouvert auprès de
N° de taxe professionnelle
N° de l'Identifiant Commun de l'Entreprise :(2)

d) Pour les auto-entrepreneur :

Je, soussigné (Prénom, nom) (1)
Numéro de tél : adresse électronique :
Affiliée à la CNSS sous le n°.....(3)
Inscrit au registre national de l'auto-entrepreneur sous le n°.....(3)
N° de taxe professionnelle
N° de l'Identifiant Commun de l'Entreprise :(3)

En vertu des pouvoirs qui me sont conférés :

Après avoir pris connaissance du dossier d'appel d'offres, concernant les prestations précisées en objet de la partie A ci-dessus ;

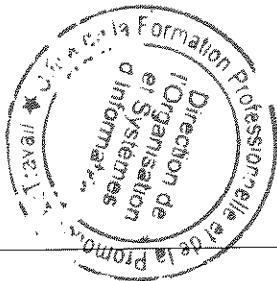
Après avoir apprécié à mon point de vue et sous ma responsabilité la nature et les difficultés que comportent ces prestations :

1) remets, revêtu (s) de ma signature un bordereau de prix - détail estimatif établi (s) conformément aux modèles figurant au dossier d'appel d'offres ;

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

- | | |
|---------------------------------------|-----------------------------|
| - Montant minimum hors TVA..... | (en lettres et en chiffres) |
| - Taux de la TVA..... | (en pourcentage) |
| - Montant de la TVA: | (en lettres et en chiffres) |
| - Montant minimum TVA comprise..... | (en lettres et en chiffres) |
| - Montant total maximum hors TVA..... | (en lettres et en chiffres) |
| - Taux de la TVA..... | (en pourcentage) |

7 02 2



OFPPT/DOSI

Dossier d'Appel d'Offres

AO. N°98/2024

- Montant de la TVA..... (en lettres et en chiffres)
- Montant maximum TVA comprise..... (en lettres et en chiffres)

Lorsque le marché est conclu avec un groupement :

- Part revenant au membre n° 1: (en lettres et en chiffres)
- Part revenant au membre n° 2: (en lettres et en chiffres)
- Part revenant au membre n° n: (en lettres et en chiffres)

L'Office de la Formation Professionnelle et de la Promotion du Travail se libérera des sommes dues par lui en faisant donner crédit au compte (À la Trésorerie Générale, bancaire, ou postal) (5) ouvert à mon nom (ou au nom de la société) (5) à.....(1) (Localité), sous relevé d'identification bancaire (RIB) numéro..... (6)

Fait à..... Le

(Signature et cachet du concurrent)

(1) lorsqu'il s'agit d'un groupement, ses membres doivent :

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)

ajouter l'alinéa suivant : « désignons..... (prénoms, noms et qualité) en tant que mandataire du groupement ».

(2) pour les concurrents non installés au Maroc préciser la référence des documents équivalents ;

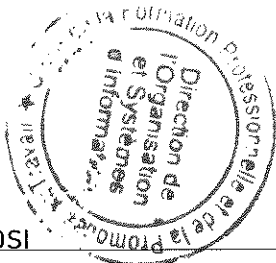
(3) ces mentions ne concernent que les personnes assujetties à cette obligation.

(4) Indiquer la CNSS ou tout autre régime particulier de prévoyance sociale.

(5) Supprimer la mention inutile.

(6) Le relevé d'identité bancaire (RIB) contient 24 positions

702

**MODELE DE DECLARATION SUR L'HONNEUR****DECLARATION SUR L'HONNEUR (*)**

- Mode de passation : Appel d'offres ouvert international n° /2024 , sur offres des prix du ../.../.... à ...h.. min.

Objet du marché : Projet infrastructure et sécurité système d'information de l'OFPPT au niveau du siège & des directions régionales.

A. Pour les personnes physiques

Je, soussigné : (Prénom, nom et qualité)

Agissant en mon nom personnel et pour mon propre compte,

Adresse du domicile élu :

Numéro tél : Adresse électronique :

Affilié à (4) 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 (5).....(6) (RIB), ouvert auprès de

En vertu des pouvoirs qui me sont conférés ;

B. Pour les personnes morales

Je, soussigné(Prénom, nom et qualité au sein de l'entreprise)

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.....

Numéro de tél : Fax

adresse électronique :

Affiliée à (4) 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 (5).....(6)(RIB), ouvert auprès de

N° de taxe professionnelle

N° de l'Identifiant Commun de l'Entreprise :(1)

En vertu des pouvoirs qui me sont conférés ;

C. Pour les coopératives ou union de coopératives

Je, soussigné(Prénom, nom et qualité au sein de la coopérative)

Agissant au nom et pour le compte de.....Dénomination de la coopérative ou de l'union de coopératives) au capital de :

Adresse du siège de la coopérative ou de l'union de coopératives.....

Numéro de tél : Fax

adresse électronique :

702



OFPPT/DOSI

Dossier d'Appel d'Offres

AO. N°98/2024

Affiliée à(4) sous le n°.....(2)

Inscrite au registre local du coopérative n°..... (Localité) sous le n°.....(2)

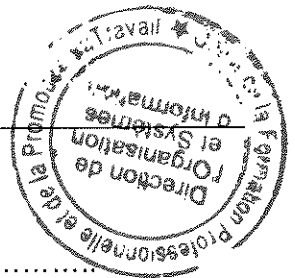
N° de patente.....

N° du compte courant postal, bancaire ou à la TGR (5).....(6)(RIB), ouvert auprès de

N° de taxe professionnelle

N° de l'Identifiant Commun de l'Entreprise :

En vertu des pouvoirs qui me sont conférés ;

**D. Pour les auto-entrepreneur :**

Je, soussigné (Prénom, nom)

Numéro de tél : adresse électronique :

Affiliée à(4) sous le n°.....(2)

Inscrit au registre national de l'auto-entrepreneur sous le n°.....(2)

N° du compte courant postal, bancaire ou à la TGR (5).....(6)(RIB), ouvert auprès de

N° de taxe professionnelle

N° de l'Identifiant Commun de l'Entreprise :

En vertu des pouvoirs qui me sont conférés ;

a) Cas des établissements publics :

Je soussigné.....(nom, prénom et qualité) agissant au nom et pour le compte de (dénomination de l'établissement).

Numéro de tél : adresse électronique :

Adresse du siège:

Affiliée à(4) sous le n°.....(2)

Inscrit au registre du commerce de(7).....(localité) sous le n°.....(2)

N° du compte courant postal, bancaire ou à la TGR (5).....(6)(RIB), ouvert auprès de

N° de taxe professionnelle sous le numéro (8):

N° de l'Identifiant Commun de l'Entreprise (8) :

Références du texte l'habilitant à exercer les missions objet du marché :

Relevé d'identité bancaire.....(postal, bancaire ou à la TGR)(5) numéro(6):

En vertu des pouvoirs qui me sont conférés ;

Déclare sur l'honneur :

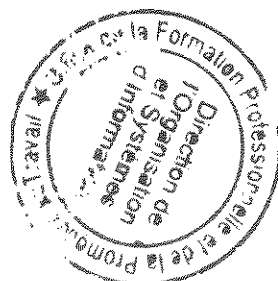
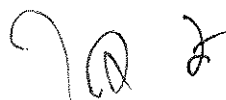
1. m'engager à couvrir, dans les limites fixées dans le cahier des charges, par une police d'assurance, les risques découlant de mon activité professionnelle ;
2. que je remplie les conditions prévues à l'article 27 du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) et fixant les conditions et les formes de passation des marchés publics ainsi que certaines règles relatives à leur gestion et à leur contrôle ;
3. Étant en redressement judiciaire j'atteste que je suis autorisé par l'autorité judiciaire compétente à poursuivre l'exercice de mon activité (2) ;
 - m'engager, si j'envisage de recourir à la sous-traitance :

- à m'assurer que les sous-traitants remplissent également les conditions prévues par l'article 151 du décret précité ;
 - 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 prévues dans ledit cahier ;
 - à confier les prestations à sous-traiter à des PME installées au Maroc ; (3)
4. 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 ;
5. m'engage à ne pas faire par moi-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusions du présent marché.
6. atteste que je remplis les conditions prévues par l'article 1er du dahir n° 1-02-188 du 12 JOMADA I 1423 (23 juillet 2002) portant promulgation de la loi n°53-00 formant charte de la petite et moyenne entreprises (4).
7. atteste que je ne suis pas en situation de conflit d'intérêt.
8. je certifie l'exactitude des renseignements contenus dans la présente déclaration sur l'honneur et dans les pièces fournies dans mon dossier de candidature tel que prévu à l'article 152 du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics .
9. je reconnais avoir pris connaissance des sanctions prévues par l'article 152 du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics , relatives à l'inexactitude de la déclaration sur l'honneur.

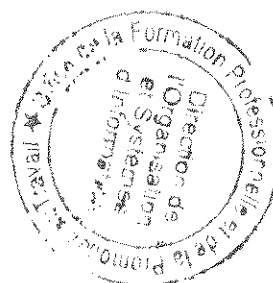
Fait à.....le.....

Signature et cachet du concurrent

-
- (1) Pour les concurrents non installés au Maroc, préciser la référence des documents équivalents et lorsque ces documents ne sont pas délivrés par leurs pays d'origine, la référence à l'attestation délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits.
- (2) à supprimer le cas échéant.
- (3) Lorsque le CPS le prévoit.
- (4) Indiquer la CNSS ou tout autre régime particulier de prévoyance sociale
- (5) Supprimer la mention inutile.
- (6) Le relevé d'identité bancaire (RIB) contient 24 positions.
- (7) Lorsque l'établissement public est assujéti à cette obligation
- (8) Ou tout autre régime particulier de prévoyance sociale.
- (*) En cas de groupement, chacun des membres doit présenter sa propre déclaration sur l'honneur.



CAHIER DES PRESCRIPTIONS SPECIALES (C.P.S.)



702

CAHIER DES PRESCRIPTIONS SPÉCIALES

Marché n° / 2024.

Passé en application de l'article 19, du décret N°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics.

Entre les soussignés :

d'une part : L'OFFICE DE LA FORMATION PROFESSIONNELLE ET DE LA PROMOTION DU TRAVAIL (OFPPT.), représenté par son Directeur Général,

Et,

D'autre part :

La société :

- Titulaire du 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.....

- Adresse du siège social de la société :

- Adresse du domicile élu :

- Affiliée à la CNSS sous le n° :

- Inscrite au registre de commerce de (localité) sous le n° :

- Patente n° :

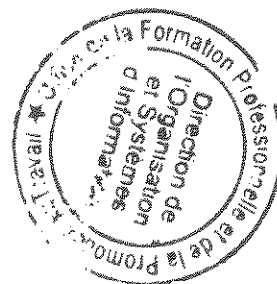
- N° d'identification Fiscale

- ICE.....

- Représentée par : Monsieur

Agissant au nom et pour le compte de ladite société en vertu des pouvoirs qui lui sont conférés

70 2



CHAPITRE I : CLAUSES ADMINISTRATIVES ET FINANCIERES :

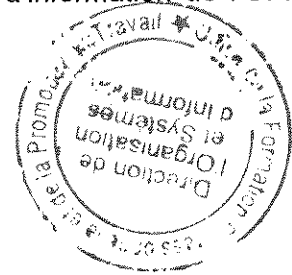
ARTICLE 1 : OBJET DU MARCHÉ

Le présent marché a pour objet « Projet infrastructure et sécurité système d'information de l'OFPPT au niveau du siège & des directions régionales ».

ARTICLE 2 : DOCUMENTS CONSTITUTIFS DU MARCHÉ

Les documents contractuels sont par ordre de priorité :

- 1- L'acte d'engagement ;
- 2- Le présent cahier des prescriptions spéciales ;
- 3- L'offre technique du titulaire ;
- 4- Le bordereau des prix - détail estimatif ;
- 5- Le cahier des clauses administratives générales applicables aux marchés de travaux (CCAGT), approuvé par le Décret n° 2-14-394 du 06 Chaabane 1437 (13 mai 2016).



En cas de discordance ou de contradiction entre les documents constitutifs du marché, autres que celles se rapportant à l'offre financière tel que décrit dans règlement relatif aux marchés publics de l'office de l'OFPPT, ceux-ci prévalent dans l'ordre où ils sont énumérés ci-dessus.

ARTICLE 3 : Autres textes applicables

Le titulaire du marché est soumis aux dispositions notamment des textes suivants :

- Loi N° 1-72-183 instituant l'Office de la Formation Professionnelle et de la Promotion de Travail.
- La loi n°69-00 relative au contrôle financier de l'Etat sur les entreprises publiques et autres organismes (B.O. n°5170 du 18/12/2003).
- Le Décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics.
- Le Décret n° 2-14-394 du 06 Chaabane 1437 (13 mai 2016) approuvant Le cahier des clauses administratives générales applicables aux marchés de travaux.
- L'arrêté 2-3663 du 13 /07/2005 portant organisation financière et comptable de l'OFPPT.
- Le dahir n° 1-15-05 du 29 rabii II 1436 (19 février 2015) portant promulgation de la loi n°112-13 relative au nantissement des marchés publics.
- Les textes officiels réglementant la main d'œuvre et les salaires.
- La décision du ministre des Finances et de la Privatisation - DEPP n° 2-0610 du 26 Février 2008 fixant le visa préalable du contrôleur d'Etat de l'OFPPT pour les marchés de fournitures et de prestation de service dont le montant est supérieur à 1 000 000,00 DHS.
- L'arrêté du ministre délégué au profit de la ministre de l'économie et des finances, chargé du budget n° 1692-23 du 4 hija 1444 (23 Juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics

Ainsi que tous les textes réglementaires ayant trait aux marchés publics rendus applicables à la date limite de réception des offres.

ARTICLE 4 : Consistance des prestations

Les prestations objet du marché portent sur la mise en place de l'infrastructure réseau au niveau du siège et des régions ainsi des solutions de cybersécurité. Les prestations demandées sont organisées en 5 parties :

- Partie 1 : Évaluation des vulnérabilités & Tests de Pénétration

Il s'agit de réaliser un audit de sécurité applicative et des tests d'intrusion afin de détecter d'éventuelles vulnérabilités du SI de l'OFPPT.

- Partie 2 : Sécurité des infrastructures :

Il s'agit de la refonte complète de l'infrastructure réseau du siège et régions, incluant le LAN, le WLAN et le SD-WAN, ainsi que la mise en place de solutions de sécurité telles que les pare-feu de nouvelle génération (NGFW), avec une solution de gestion unifiée et centralisée.

720

- Partie 3 : Sécurité des identités, des accès et des privilèges :

Il s'agit de mettre en place les solutions de gestion des identités et des accès (IAM), de gestion de l'infrastructure à clé publique (PKI) et de gestion des accès privilégiés (PAM) ainsi qu'une solution d'industrialisation du déploiement des postes de travail et une solution de chiffrement.

- Partie 4 : Réorganisation de la gestion des services IT selon le référentiel ITIL ou équivalent

Il s'agit de mettre en œuvre les pratiques et processus ITIL V4 ou équivalent, pour réorganiser la gestion des services informatique.

- Partie 5 : Sécurité des terminaux & Cybersurveillance

Il s'agit de souscrire à une gamme de services, incluant le NOC managé (Network Operations Center), l'EDR managé (Endpoint Detection and Response), et le SOC managé (Security Operations Center).

ARTICLE 5 : Délai d'exécution

Le délai d'exécution du marché est fixé comme suit :

- 3 mois pour la partie 1 : Évaluation des vulnérabilités & Tests de Pénétration
- 9 mois pour la partie 2 : Sécurité des infrastructures
- 7 mois pour la partie 3 : Sécurité des identités, des accès et des privilèges
- 4 mois pour la Partie 4 : Réorganisation de la gestion des services IT selon le référentiel ITIL ou équivalent
- 12 mois pour la partie 5 : Sécurité des terminaux & Cybersurveillance

Le délai de chaque partie prend effet à compter du lendemain de la date de la notification de l'ordre de service, signé par le Maître d'Ouvrage, prescrivant au titulaire du marché de commencer l'exécution des prestations de la partie correspondante.

Les parties peuvent être exécutées concomitamment.

Les délais d'examen par le maître d'ouvrage des dossiers remis par le titulaire à l'issue de l'exécution des prestations, et les délais de la vérification de la conformité technique, ne sont pas inclus dans le délai global d'exécution du marché. Ces délais sont à compter du lendemain de la livraison de la prestation ou de la remise des rapports.

ARTICLE 6 : Droits de timbres

Le titulaire acquitte les droits de timbre dus au titre du marché conformément à la législation en vigueur.

ARTICLE 7 : Cautionnement provisoire et définitif

Le cautionnement provisoire qui reste affecté à la garantie des engagements contractuels du titulaire du marché dans les cas prévus par l'article 18 § 1 du CCACT est **trois cent mille DIRHAMS (300 000 DHS)**.

Le cautionnement provisoire reste acquis au maître d'ouvrage notamment dans les cas cités à l'article 18 du CCACT.

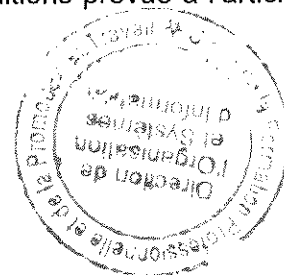
Le montant du cautionnement définitif est fixé à trois pour cent (3%) du montant du marché arrondi au dirham supérieur.

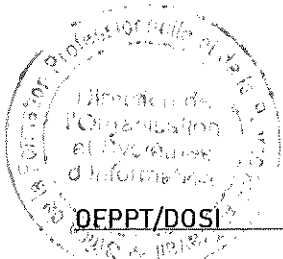
Le cautionnement définitif doit être constitué dans les vingt (20) jours qui suivent la notification de l'approbation du marché.

N.B : Les cautions personnelles et solidaires doivent être choisies parmi les établissements marocains agissant à cet effet conformément à la législation en vigueur.

En cas de groupement, le cautionnement définitif est souscrit dans les conditions prévues à l'article 150 du décret n° 2-22-431.

720



**ARTICLE 8 : Restitution des cautionnements provisoire et définitif**

En application des dispositions de l'article 19 du CCACT, le cautionnement provisoire est restitué au titulaire du marché ou la caution qui le remplace est libérée après que le titulaire aura réalisé le cautionnement définitif.

Le cautionnement définitif est restitué, sauf les cas d'application de l'article 79 du CCACT, et le paiement du la retenu de garantie est effectuée ou bien les cautions qui les remplacent à la suite d'une mainlevée donnée par l'OFPPT dès la signature du procès-verbal de la réception définitive des équipements objet du marché.

ARTICLE 9 : Caractère des prix

Les prix des prestations objet du présent marché sont fermes et non révisables.

Toutefois, si le taux de la taxe sur la valeur ajoutée est modifié postérieurement à la date limite de remise des offres. Le maître d'ouvrage répercute cette modification sur le prix de règlement.

ARTICLE 10 : Nature des prix

Le présent marché est à prix unitaires.

Les sommes dues au titulaire sont calculées par application des prix unitaires portés au bordereau des prix - détail estimatif, aux quantités pour les prestations réellement exécutées conformément au marché.

Les prix du marché sont réputés comprendre toutes les dépenses résultant de l'exécution des prestations y compris tous les droits, impôts, taxes, frais généraux, faux frais et assurer au prestataire de services une marge pour bénéfice et risques et d'une façon générale toutes les dépenses qui sont la conséquence nécessaire et directe du travail.

ARTICLE 11 : Mode de règlement

Les prestations faisant l'objet du marché seront réglées par application des prix unitaires définis et établis pour chaque item par le titulaire aux quantités réellement exécutées et régulièrement constatées, conformément aux descriptions figurant au bordereau des prix-détail estimatif et aux conditions particulières du marché.

Le titulaire adressera au Maître d'ouvrage les factures en six exemplaires.

Les sommes dues au titulaire seront réglées à son compte dont le numéro est précisé dans le marché.

Tout changement du numéro de compte doit faire l'objet d'un avenant.

ARTICLE 12 : Avance

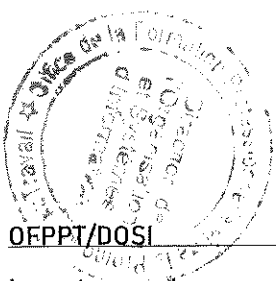
Conformément au décret n° 2-14-272 du 14 Rajab 1435 (14 Mai 2014) relatif aux avances en matière des marchés publics, le titulaire du marché a droit à une avance qui sera calculée par application de l'article 5 du décret susmentionné. L'avance est accordée en une seule fois sur la base du montant total de la première année. Cette avance sera octroyée au titulaire après la notification de l'ordre de service de commencer les prestations objet du marché contre remise d'une caution personnel et solidaire du même montant, ne comportant aucune réserve et demeure affectée aux garanties pécuniaires exigées du titulaire du marché. Le remboursement de cette avance sera effectué par déduction sur chaque acompte d'un montant égal à 25%, de manière que le remboursement de la totalité de l'avance soit opéré lorsque le montant des prestations exécutées aura atteint 80% du montant du marché. si ces sommes n'atteignent pas 80% du montant initial du marché, le solde à rembourser sera prélevé sur le décompte « n » et dernier, si le marché ne donne pas lieu à versement d'acomptes et fait l'objet d'un seul règlement, l'avance est récupérée en une seule fois par précompte sur le règlement.

La révision des prix n'est pas prise en compte dans le calcul du montant de l'avance. Les taux et les conditions de versement et de remboursement de l'avance ne peuvent pas être modifiés par avenant.

ARTICLE 13 : Retenue de garantie

La retenue de garantie sera prélevée sur les factures. Elle est égale à dix pour cent (10%) du montant de chaque facture. Elle cessera de croître lorsqu'elle atteindra sept pour cent (7%) du montant initial du marché augmenté le cas échéant, du montant des avenants.

70 2



La retenue de garantie peut être remplacée, à la demande du prestataire, par une caution personnelle et solidaire dans les conditions prévues par la réglementation en vigueur.

La retenue de garantie est restituée ou la caution qui la remplace est libérée à la suite d'une mainlevée délivrée par le Maître d'Ouvrage dans un délai maximum de trois mois suivant la date de réception définitive du marché.

Toutes les cautions présentées sous forme de garanties bancaires doivent être émises par une banque marocaine agréée à cet effet.

ARTICLE 14 : Pénalités de retard

A défaut par le titulaire d'avoir terminé les prestations objet du marché dans le délai contractuel, il lui sera appliqué, sans mise en demeure préalable, une pénalité de un pour mille (1/1000) du montant initial, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse et ce, par jour calendaire.

Le montant global des pénalités au titre des retards est plafonné à huit pour cent (8)% du montant initial du marché augmenté le cas échéant du montant des avenants.

Quand le montant des pénalités atteint ce plafond, l'autorité compétente se réserve le droit de résilier le marché dans les conditions prévues par l'article 79 du CCAGT.

ARTICLE 15 : Délai de paiement

En application des dispositions prévues par la loi 69-21, le délai de paiement des sommes dues au titulaire de ce marché est de 120 Jours, et ce, conformément aux articles 78-1 et 78-2 de ladite loi.

ARTICLE 16: Modalités de livraison

Livraison des équipements

Les équipements seront livrés aux sites bénéficiaires indiqués dans les tableaux de répartition en annexe II. Toutefois, et pour des raisons exceptionnelles dûment justifiées et à la demande de l'OFPPT, la liste des sites bénéficiaires et la répartition peut être modifiée sans impact sur les prix ou autres conditions des marchés. Le dépôt des équipements ne vaut nullement leurs réceptions dont les modalités sont prévues aux articles 17 et 18 du présent CPS.

En cas d'indisponibilité du Site bénéficiaire pour une livraison directe des équipements, l'OFPPT se réserve le droit de demander au Titulaire d'effectuer le Dépôt dans le magasin du siège de l'OFPPT.

Toutefois, l'acheminement des équipements vers le Site Bénéficiaire est à la charge du Titulaire.

Avant de commencer les livraisons, le titulaire doit transmettre à l'OFPPT :

- Une attestation d'origine des équipements à livrer, délivrée par le constructeur ;
- Un planning prévisionnel de livraison au moins quinze jours avant le début des livraisons dans les sites bénéficiaires

Le magasinier du centre bénéficiaire signe les bons de dépôt des articles livrés en précisant les dates de livraison.

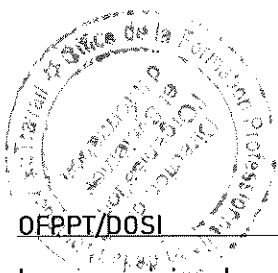
Le titulaire doit communiquer à l'OFPPT le bon de dépôt contre accusé de réception, pour permettre aux services de l'OFPPT de planifier les opérations de vérification de conformité technique.

Livraison de licence logicielle :

Les licences logicielles peuvent être livrées physiquement (via CD, DVD, USB) ou électroniquement à l'OFPPT via l'un des moyens suivants :

- Par email de l'éditeur contenant les références de la licence au nom de l'OFPPT ;
- Via le portail en ligne de l'éditeur contenant les références licences au nom de l'OFPPT.
- Tout autre moyen justifiant la souscription de licence au nom de l'OFPPT (document, attestation...) délivré par l'éditeur

920



Le magasinier du centre bénéficiaire signe les bons de dépôt des articles livrés en indiquant les dates de livraison. Cette date correspondra à l'une des dates suivantes :

- La date de réception de l'email de l'éditeur confirmant la souscription de licences ;
- La date indiquée sur le portail en ligne de l'éditeur confirmant la souscription de licences ;
- La date de dépôt du CD, DVD, USB...

ARTICLE 17 : Modalités de vérification de la conformité technique des articles livrés

Sur la base du programme des livraisons, l'OFPPT organise les opérations de vérification de conformité technique des articles livrés dans le site bénéficiaire suivant un planning communiqué au titulaire.

En cas d'indisponibilité du Site bénéficiaire, les opérations de vérification de conformité technique seront effectuées au siège de l'OFPPT avant l'acheminement des équipements vers le Site bénéficiaire.

Il est bien entendu qu'en cas de livraison au siège de l'OFPPT, la vérification portera sur la conformité technique, tandis que l'installation et la mise en marche se feront sur le site bénéficiaire.

Le retard enregistré dans l'opération de vérification de conformité technique et de réception, après livraison, sera à la charge de l'OFPPT et le délai d'exécution du marché sera prorogé en conséquence.

Le titulaire doit préparer toutes les conditions nécessaires à la vérification de conformité technique avant la date fixée par l'OFPPT. A défaut, l'opération de vérification de conformité technique sera suspendue et reprendra après 3 jours ouvrables. Ce retard sera à la charge du titulaire.

Le titulaire mettra à la disposition du(es) représentant(s) de l'OFPPT la documentation technique nécessaire à la vérification de la conformité technique des articles livrés.

L'OFPPT procédera à la vérification de la conformité technique des articles livrés avec les spécifications du marché (marque, référence, origine, dimensions, capacités, puissance, alimentation électrique, ...) dans les sites bénéficiaires, à la date prévue, en présence d'un représentant qualifié du titulaire devant être habilité à répondre aux remarques de la commission désignée par l'OFPPT.

Les vérifications de la conformité technique sont sanctionnées par l'établissement de procès-verbaux qui doivent être signés par le(s) représentant(s) de l'OFPPT.

Les articles dont les spécifications ne peuvent être vérifiées qu'après exécution des prestations d'installation et de mise en service doivent être consignés dans le procès-verbal de vérification de conformité technique avec la mention « sous réserve de l'achèvement des prestations d'installation et de mise en service ».

Toute divergence par rapport au marché et avenant(s) doit être consignée dans le procès-verbal de vérification de conformité technique.

Une copie du procès-verbal de vérification de conformité technique est remise au représentant du titulaire séance tenante.

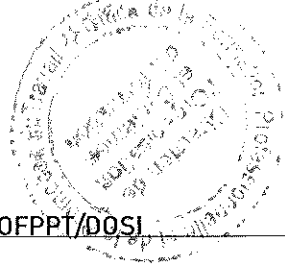
Tout article jugé non conforme par l'OFPPT devra être remplacé dans le délai contractuel.

Les équipements jugés non-conformes sont récupérés séance tenante par le titulaire, ceux présentant des observations doivent faire l'objet de levée de réserves dans un délai maximum de 15 jours qui commencera à courir à partir du lendemain de la notification au titulaire par l'OFPPT des équipements concernés. Le délai de prise en charge des réserves est à la charge du titulaire. Passé ce délai l'OFPPT n'est plus responsable des équipements en question.

Le titulaire remettra aux représentants du site bénéficiaire 5 exemplaires originales des bons de livraison, afin de renseigner les numéros d'enregistrement dans les livres journal et/ou inventaire dans le site bénéficiaire.

Les opérations de transport, de chargement, de déchargement, de déballage et d'emballage sont à la charge exclusive du titulaire et sont effectuées sous sa responsabilité et ce dans les sites bénéficiaires et /ou l'entrepôt dédié.

920



Le titulaire interviendra pour l'installation des différents articles dans un délai de 7 jours qui commencera à courir à partir du lendemain de la saisie du titulaire par l'OFPPT. La durée d'installation est à la charge du titulaire.

Le titulaire prend en charge les accessoires, les composants, la matière d'œuvre et toutes sujétions nécessaire à l'installation, la mise en service et aux différents essais des articles livrés.

ARTICLE 18 : Modalités de réception

Réception des équipements

L'OFPPT procédera à la réception dans le site bénéficiaire :

- Des équipements sur la base du procès-verbal de vérification de conformité technique ;
- Des quantités livrées par rapport à celles du marché ou avenant ;
- De la mise en service des équipements ;

La réception n'est prononcée qu'une fois :

- L'équipement est livré, vérifié conforme, installé, testé ;
- Les prestations de services afférentes à la mise en service, sont réalisées et satisfaites aux spécifications du marché ;
- Tous les essais ont été déclarés satisfaisants ;
- L'attestation, ou tout autre moyen (email éditeur, portail en ligne ...), prouvant la souscription au service support du constructeur, a été présentée ;
- L'attestation, ou tout autre moyen (email éditeur, site web support...), prouvant la souscription de licence au nom de l'OFPPT délivré par le constructeur, a été présentée, pour les équipements ayant une souscription de licence associée.

Les articles réceptionnés sont enregistrés dans le livre journal et éventuellement dans le livre d'inventaire. Les numéros du livre journal et d'inventaire sont portés sur le bon de livraison.

Réception de Licence logicielle

L'OFPPT procédera à la réception dans le site bénéficiaire :

- Des logiciels sur la base du procès-verbal de vérification de conformité technique ;
- Des quantités de licence logicielle activées par rapport à celles du marché ou avenant ;
- De la mise en service des logiciels ;

La réception n'est prononcée qu'une fois :

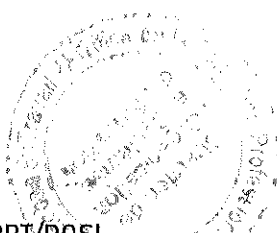
- Le logiciel on prémisses est livré, vérifié conforme, installé et testé ;
- Le logiciel en SAAS est souscrit au nom de l'OFPPT paramétré et testé ;
- Les licences sont activées ;
- Les prestations de services afférentes à la mise en service, sont réalisées et satisfaites aux spécifications du marché ;
- Tous les essais ont été déclarés satisfaisants par le(s) représentant(s) de l'OFPPT ;
- L'attestation, ou tout autre moyen (email éditeur, site web support...), prouvant la souscription de licence au nom de l'OFPPT délivré par l'éditeur, a été présentée.

Le responsable du magasin du siège procédera à l'enregistrement dans le livre journal des articles réceptionnés. Les numéros du livre journal seront portés sur le bon de livraison.

Réception des prestations de services objet de la partie 1 et la partie 4

Les prestations faisant l'objet de la partie 1 et la partie 4 du marché sont soumises à des vérifications destinées à constater qu'elles répondent aux stipulations prévues dans le marché.

La réception des prestations sera prononcée par la commission de réception désignée à cet effet.



Le titulaire avise par écrit le maître d'ouvrage de la date à laquelle les prestations seront présentées en vue de ces vérifications.

Le titulaire soumet le rapport, document ou livrable, établi sous sa forme finale, à l'approbation du maître d'ouvrage.

Les différents rapports doivent être déposée à l'OFPPT contre accusé de réception ;

La commission de réception procèdera à l'examen des rapports produits par le titulaire du marché, et se réservera un délai d'un (1) mois pour l'appréciation desdits rapports. Ce délai n'est pas inclus dans le délai d'exécution précité.

Durant ce délai susvisé, la commission de réception doit :

- soit accepter les rapports sans réserve ;
- soit inviter le titulaire du marché à procéder à des corrections ou à des améliorations pour rendre les rapports conformes aux exigences du CPS ;
- soit, le cas échéant, prononcer un refus motivé des rapports pour insuffisance grave dûment justifiée.

Si le maître d'ouvrage invite le titulaire du marché à procéder à des corrections ou des améliorations, celui-ci dispose d'un délai de 10 jours à compter de la date de notification des remarques soulevées par la commission de réception pour remettre les rapports dans leur forme définitive.

Le délai accordé au titulaire du marché est de dix (10) jours pour procéder aux corrections ou aux améliorations, est inclut dans le délai d'exécution de la mission.

L'OFPPT dispose d'un délai de 10 jours pour la validation des rapports modifiés. Cette validation sera consignée dans un procès-verbal.

En cas de refus par la commission de réception pour insuffisance grave, le titulaire du marché est tenu de soumettre à l'approbation du maître d'ouvrage de nouveaux rapports et la procédure décrite ci-dessus est réitérée, et ce sans préjudice de l'application des dispositions de l'article 10 ci-dessous.

Ainsi, Il y a lieu de préciser que la réception des rapports est subordonnée à l'intégration, par le titulaire du marché, de toutes les remarques et observations soulevées et retenues par la commission de réception.

Les délais que se réserve la commission de réception pour valider les rapports ne sont pas compris dans le délai d'exécution de la mission.

ARTICLE 19 : Garantie technique

Dans le cadre de ce marché, il est prévu une garantie technique de cinq (5) ans pour la partie 2 et de trois (3) ans pour la partie 3.

La période de garantie est à compter de la date de la réception provisoire partielle de la partie correspondante, prononcée par le Maître d'Ouvrage.

Aucune garantie n'est prévue pour la partie1, la partie 4 et la partie 5.

Pendant le délai de garantie, le titulaire est tenu, de procéder immédiatement aux rectifications qui lui seraient demandées en cas de mauvaise qualité, anomalies ou défauts constatés, sans pour autant que ces prestations supplémentaires puissent donner lieu au paiement à l'exception de celles résultant d'un abus d'usage ou de dommages causés par le maître d'ouvrage.

Le délai d'intervention est de 2 heures après déclaration de l'incident et un délai de 4 heures de résolution ou de contournement du problème. Le contournement n'exempte pas de la correction laquelle doit être prise en charge dans un délai maximum de 7 jours.

ARTICLE 20 : Réceptions partielle provisoire et définitive

A l'issue de la procédure de vérification prévue à l'article 17 du présent marché, et suite au modalités de réception prévue à l'article 18, la réception est prononcée partiellement pour chaque partie.

720

Le titulaire avise, par écrit, le maître d'ouvrage de l'achèvement des livraisons et des prestations de service relatives à la partie en question.

La réception des prestations sera prononcée par la commission de réception désignée à cet effet.

La dernière réception partielle définitive marque la réception définitive du marché.

Le titulaire demandera à l'OFPPT d'organiser la réception définitive vingt jours au plus tard avant l'expiration du délai de garantie.

Le titulaire prendra les dispositions nécessaires pour se faire représenter à la réception définitive et qui sera sanctionnée par un procès-verbal.

ARTICLE 21 : Assurance et responsabilités

En application des dispositions de l'article 25 du CCAGT, le titulaire doit souscrire, conformément à la législation et à la réglementation en vigueur, les polices d'assurances qui doivent couvrir les risques inhérents à l'exécution du présent marché.

ARTICLE 22 : Utilisation des documents contractuels et diffusion de renseignements

Le titulaire, sauf consentement préalable donné par écrit par l'OFPPT, ne communiquera le marché, ni aucune de ses clauses, ni aucune des spécifications, des plans, dessins, tracés, ou information fournis par l'OFPPT, ou en son nom et au sujet du marché à aucune personne autre qu'une personne employée par le titulaire à l'exécution du marché. Les informations transmises à une telle personne le seront confidentiellement et seront limitées à ce qui est nécessaire à ladite exécution.

Le titulaire, sauf consentement préalable donné par écrit par l'OFPPT, n'utilisera aucun des documents et aucune des informations énumérées dans le paragraphe précédent, si ce n'est pour l'exécution du marché.

Tout document, autre que le marché lui-même, énuméré dans le 1^{er} paragraphe demeurera la propriété de l'OFPPT, et tous ses exemplaires seront renvoyés à l'OFPPT sur sa demande, une fois les obligations contractuelles du titulaire exécutées.

ARTICLE 23 : Lutte contre la fraude et la corruption

Le titulaire du marché ne doit pas recourir par lui-même ou par personne interposée à des pratiques de fraude ou de corruption des personnes qui interviennent, à quelque titre que ce soit, dans les différentes procédures de passation, de gestion et d'exécution du marché.

Le titulaire du marché ne doit pas faire, par lui-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion d'un marché et lors des étapes de son exécution.

Les dispositions du présent article s'appliquent à l'ensemble des intervenants dans l'exécution du marché.

ARTICLE 24 : BREVETS

Le titulaire garantit formellement l'OFPPT contre toutes les revendications des tiers concernant les brevets d'invention relatifs aux procédés et moyens utilisés, marques de fabrique, de commerce et de service.

Il appartient au titulaire, d'obtenir les cessions, licence d'exploitation ou autorisation nécessaires et de supporter la charge des frais et redevances y afférentes, conformément aux réglementations en vigueur.

ARTICLE 25 : Protection des données à caractère personnel :

Respecter la législation en vigueur au Maroc, notamment en ce qui concerne le traitement des données à caractère personnel (loi n° 09-08), ainsi que tous les textes réglementaires ayant trait à la sécurité et la confidentialité des données.

Afin de garantir le secret, la sécurité et la confidentialité des données, le titulaire s'engage à :

- Prendre toutes les précautions utiles, afin de préserver la sécurité des données, notamment empêcher qu'elles ne soient déformées, endommagées et empêcher tout accès qui ne serait pas préalablement autorisé par le maître d'ouvrage ;

902

- Ne traiter les données que dans le cadre des instructions et de l'autorisation reçues de la part du maître d'ouvrage ;
- Ne traiter les informations qu'entièrement et exclusivement en son sein et dans le cadre du présent marché ;
- S'assurer de la licéité des traitements réalisés dans le cadre de la mission confiée ;
- Respecter son obligation de secret, de sécurité et de confidentialité, à l'occasion de toute opération de maintenance et de télémaintenance, réalisée au sein des locaux du prestataire ou de toute société intervenant dans le cadre du traitement ;
- Prendre toutes mesures de sécurité, notamment matérielle et logique, pour assurer la conservation et l'intégrité des données traitées ;
- Prendre toutes mesures permettant d'empêcher toute utilisation détournée, malveillante ou frauduleuse des données traitées ;
- À la fin du marché et après achèvement des processus de réversibilité, procéder à la destruction sécurisée et définitive des données, en conformité avec les exigences légales et réglementaires, et après validation préalable du maître d'ouvrage. Par données, on entend tous fichiers, qu'ils soient sous forme électronique ou manuscrite, stockés sur n'importe quel support.

Par ailleurs, le titulaire s'interdit :

- De divulguer, sous quelque forme que ce soit, tout ou partie des informations contenues dans des fichiers informatisés ou manuels, ou figurant sur tout support transmis par le maître d'ouvrage ou concernant les informations recueillies au cours de l'exécution du présent marché ;
- D'utiliser les supports ou documents qui lui ont été confiés, par quelque moyen ou finalité que ce soit, pour son compte ou pour le compte de tiers, à des fins professionnelles, personnelles ou privées autres que celles définies dans le présent marché. Cette interdiction s'applique à toute ou partie des informations contenues sur lesdits supports ou recueillies au cours de l'exécution du présent marché ;
- De prendre copie ou stocker, quelles qu'en soient la forme et la finalité, tout ou partie des informations contenues sur les supports ou documents qui lui ont été confiés ou recueillies au cours de l'exécution du présent marché.

Le titulaire s'engage :

- À coopérer avec le maître d'ouvrage dans toutes circonstances mettant en jeu l'obligation de secret, de confidentialité et de sécurité ;
- À permettre la réalisation par le maître d'ouvrage ou toute personne mandatée par cette dernière et sous réserve que les vérificateurs ne soient pas des concurrents directs du prestataire, de toute vérification lui paraissant utile de l'exécution des obligations par le titulaire.
- Le titulaire s'engage à coopérer de bonne foi et sans réserve avec les vérificateurs dès lors qu'il sera avisé de la réalisation d'un audit.

ARTICLE 26: SÉCURITÉ DES SYSTÈMES D'INFORMATION

Le titulaire s'engage à respecter la législation en vigueur au Maroc, notamment en ce qui concerne la cyber sécurité (loi n° 05.20 et son décret d'application n° 2-21-406), ainsi que tous les textes réglementaires relatifs à la sécurité des systèmes d'informations.

Le titulaire est également tenu de respecter la politique de sécurité des systèmes d'information de l'OFPPT ainsi que les règles de conduite internes. Il doit prendre toutes les mesures nécessaires pour garantir que ses employés respectent ces politiques et règles de sécurité.

Dans ce sens, le titulaire est tenu de respecter, entre autres, les règles suivantes :

Règles de conduites générales dans les locaux de l'OFPPT :

- Les intervenants mandatés par le titulaire doivent se limiter uniquement au périmètre précis de leurs interventions objet du marché (local, matériel, équipement) : Ils ne doivent en aucun cas accéder au matériel ou équipements non inclus dans leurs interventions ;
- Ne pas introduire des clés USB, disques durs externes ou tout autre dispositif de stockage amovible non autorisé pouvant potentiellement nuire au système d'information. Toute utilisation de tels dispositifs doit être préalablement validée par le Maître d'Ouvrage ;

- Ne pas accéder aux locaux du Datacenter et aux armoires informatiques sans autorisation préalable du Maître d'Ouvrage et avec l'accompagnement d'un fonctionnaire mandaté par celui-ci ;
- Ne pas introduire des liquides et de la nourriture, de fumer, d'utiliser des produits inflammables, de jeter un déchet ou de laisser des cartons et autres emballages dans les locaux du Datacenter ;
- Ne pas manipuler les équipements d'environnement existant dans les locaux du Data Center (Climatisation, Groupe d'eau glacé, groupé électrogène, tableaux d'alimentation électrique, vidéosurveillance, détection extinction incendie, câblage électrique et informatique, ...) sans autorisation du Maître d'Ouvrage ;

Règles d'intervention sur le Système d'information :

- Toute intervention sur un des éléments critiques des Systèmes d'Information doit faire l'objet d'une autorisation préalable d'une instance impliquant des acteurs compétents en matière de sécurité des SI qui valide les conditions de l'intervention et de la réalisation des tâches en collaboration avec l'entité concernée.
- L'intervention ne doit, dans la mesure du possible, porter préjudice ni à l'intégrité des systèmes et des informations, ni à la continuité des services assurés par ces systèmes.
- Le titulaire doit s'assurer que ses interventions ne portent aucun préjudice à l'état des informations hébergées par le système, tant pour les données de production que pour les données de configuration du matériel et des logiciels.
- Le titulaire s'assure qu'un retour en arrière est possible, dans des délais raisonnables, éventuellement fixés en fonction des attentes des entités concernées.
- Le titulaire s'engage à ne pas altérer la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période-là moins pénalisante pour les entités concernées.
- La détection de toute anomalie ou incident pouvant remettre en cause la sécurité des Systèmes d'Information doit être rapportée immédiatement à l'interlocuteur concerné.
- Enfin, toute dérogation à l'un des principes fondamentaux de sécurité de L'OFPPT ou à l'une des règles décrites dans ce marché doit être soumise à l'autorisation préalable de l'entité concernée. Cette dérogation ne soustrait en rien le titulaire à son obligation de moyens afin de limiter au maximum les risques potentiels qu'il fait encourir au système d'information dans le champ de son intervention.

ARTICLE 27 : Sous-traitance

Si le titulaire envisage de sous-traiter une partie du marché, il doit notifier au maître d'ouvrage :

- L'identité, la raison ou la dénomination sociale, et l'adresse des sous- traitants
- Le dossier administratif des sous-traitants, ainsi que leurs références techniques et financières ;
- La nature des prestations et le montant des prestations qu'il envisage de sous-traiter ;
- Le pourcentage desdites prestations par rapport au montant du marché ;
- Une copie certifiée conforme du contrat de sous-traitance.

Les sous-traitants doivent satisfaire aux conditions requises prévues à l'article 27 du décret n° 2-22-431 du 8 mars 2023.

La sous-traitance ne peut en aucun cas dépasser cinquante pour cent (50%) du montant du marché ni porter sur le lot ou le corps d'état principal du marché.

Les prestations ne pouvant pas faire l'objet de sous-traitance sont celles relatives à la partie 1, la partie 3 et la partie 5 du présent CPS.

La sous-traitance doit être régie par un contrat soumis à la validation préalable du maître d'ouvrage, assurant ainsi le respect des obligations du prestataire en matière de sécurité des systèmes d'information et de protection des données à caractère personnel.

Le titulaire du marché demeure personnellement responsable de toutes les obligations résultant du marché tant envers le maître d'ouvrage que vis-à-vis des ouvriers et des tiers.

Le maître d'ouvrage ne se reconnaît aucun lien juridique avec les sous-traitants.

202

ARTICLE 28 : Validité du marché

Le marché ne sera valable, définitif et exécutoire qu'après sa signature par l'autorité compétente de l'Office ou par son délégataire dûment désigné et son visa par le Contrôleur d'Etat, lorsque ledit visa est requis.

ARTICLE 29 : Délai de notification de l'approbation du marché

L'approbation des marchés doit être notifiée à l'attributaire dans un délai maximum de soixante (60) jours, à compter de la date fixée pour l'ouverture des plis.

Les conditions de prorogation de ce délai sont fixées par les dispositions de l'article 143 du décret n°2-22-431 relatif aux marchés publics

ARTICLE 30 : Domicile du titulaire

Le titulaire du marché 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.

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 cahier des prescriptions spéciales.

En cas de changement de domicile, le titulaire 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 31 : Nantissement

Sous réserve de l'entrée en vigueur des dispositions de l'arrêté du ministre délégué auprès de la ministre de l'économie et des finances, chargé du budget n° 1692-23 du 4 hja 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics, notamment son « Chapitre IX : Conditions et modalités de dématérialisation du nantissement des marchés publics », en cas de nantissement du marché, le Maître d'ouvrage remet au titulaire du marché, sur sa demande et contre récépissé, 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 public, conformément aux dispositions du dahir n° 1-15-05 du 29 rabii II 1436 (19 février 2015) portant promulgation de la loi n° 112-13 relative au nantissement des marchés publics, étant précisé que :

- La liquidation des sommes dues par l'Office de la formation Professionnelle et de la Promotion du Travail en exécution du présent marché sera opérée par les soins du Directeur Général de l'OFPPT ou son délégataire.
- Le fonctionnaire chargé de fournir au titulaire du futur marché ainsi qu'à bénéficier des nantissements ou subrogations les renseignements, qui ont été prévus à l'article 8 du dahir susvisé, est le Directeur Général de l'OFPPT ou son délégataire.
- Les paiements prévus au présent marché seront effectués par le Trésorier Payeur de l'OFPPT seul qualifié pour recevoir les significations des créanciers du titulaire du présent marché.
- Les frais de timbre et d'enregistrement de l'original du présent marché ainsi que de l'exemplaire unique sont à la charge du titulaire du marché.

ARTICLE 32 : Résiliation du marché

Le marché peut être résilié par l'OFPPT de plein droit dans tous les cas de figure prévus par les textes en vigueur (le Décret n° 2-14-394 du 06 Chaabane 1437 (13 mai 2016) - CCAGT et du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics.

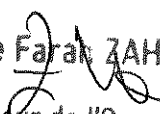


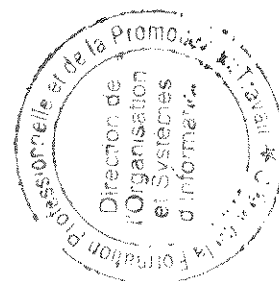
ARTICLE 33 : Mesures coercitives

Il sera fait application des mesures coercitives prévues la CCAG-T, notamment celle prévues par son chapitre VIII et l'article 152 du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics.

ARTICLE 34 : Règlement des contestations

En cas de contestation entre l'administration et le titulaire, il sera fait recours à la procédure prévue par les articles 81, 82 et 84 du Cahier des Clauses Administratives Générales applicables aux marchés de Travaux (CCAGT). Si cette procédure ne permet pas le règlement du litige, celui-ci sera soumis à la juridiction marocaine compétente statuant en matière administrative, conformément à l'article 83 du Cahier des Clauses Administratives Générales applicables aux marchés de Travaux (CCAGT).

LE SOUMISSIONNAIRE	LE MAITRE D'OUVRAGE
<p style="text-align: center;">Lu et accepté</p>	<p style="text-align: center;"> Directeur de la Direction Organisation et Système d'information  Mme Farah ZAHRAOUI Directeur de l'Organisation et Système d'Information PI </p>



70

Chapitre II : CAHIER DES PRESCRIPTIONS TECHNIQUES

Contexte du projet

Afin d'accompagner son développement digital et l'ouverture de son système d'information sur son écosystème, l'OFPPT a élaboré une feuille de route en matière de sécurité. Cette feuille de route vise à se conformer aux standards de la norme ISO 27001, aux exigences réglementaires de la DGSSI, ainsi qu'à la législation en vigueur, notamment la loi 05.20 relative à la cybersécurité et la loi 09-08 relative à la protection des données à caractère personnel.

Dans ce cadre, l'OFPPT lance ce projet pour sécuriser son système d'information, couvrant les aspects suivants :

- Sécurité des infrastructures ;
- Sécurité des identités, des accès et des privilèges ;
- Sécurité des terminaux & Cybersurveillance ;
- Réorganisation de la gestion des services IT selon le référentiel ITIL ou équivalent ;
- Évaluation des vulnérabilités & Tests de Pénétration.

Domaines de compétences de l'OFPPT

Créé par le Dahir portant loi N°1-72-183 du 28 Rabia II 1394 (21 mai 1974), l'Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT) est un opérateur national de formation professionnelle qui joue un rôle majeur dans le développement du Maroc à travers le développement de la compétence et l'amélioration de l'employabilité des jeunes.

L'OFPPT a pour vocation de développer une formation professionnelle adaptée aux besoins des entreprises. Il a pour mission principale de satisfaire les besoins des entreprises en ressources humaines qualifiées et contribuer à l'amélioration de leur compétitivité, développer les compétences nécessaires aux entreprises, favoriser l'insertion des jeunes dans la vie active et promouvoir le travail.

Organisation de l'OFPPT

L'OFPPT est organisé comme suit : Siège Central, les Directions Régionales (DR) et les complexes et les établissements de la formation professionnelle (EFP).

- Le niveau central est composé d'une Direction Générale et de 12 Directions Centrales (DC)
- Le niveau régional est composé de 10 Directions Régionales (DR) qui appuient son réseau de complexes et d'établissements de formation professionnelle répartis sur tout le royaume.
- Le niveau local est composé de plus de 120 complexes regroupant environ 400 établissements.

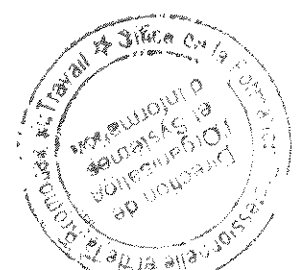
Au niveau central, le siège coordonne et supervise l'activité des directions régionales qui assurent l'assistance, le suivi et la coordination, tant sur le plan administratif que pédagogique, des activités des établissements de la formation professionnelle qui leur sont rattachés.

Chaque direction régionale est composée de plusieurs complexes et établissements autonomes et chaque complexe regroupe un ensemble d'établissements de formation professionnelles.

En plus des établissements, l'OFPPT a lancé des cités des métiers et compétence (CMC), une dans chaque région, qui sont gérées actuellement par l'OFPPT dans une perspective d'avoir leur autonomie financière par la suite.

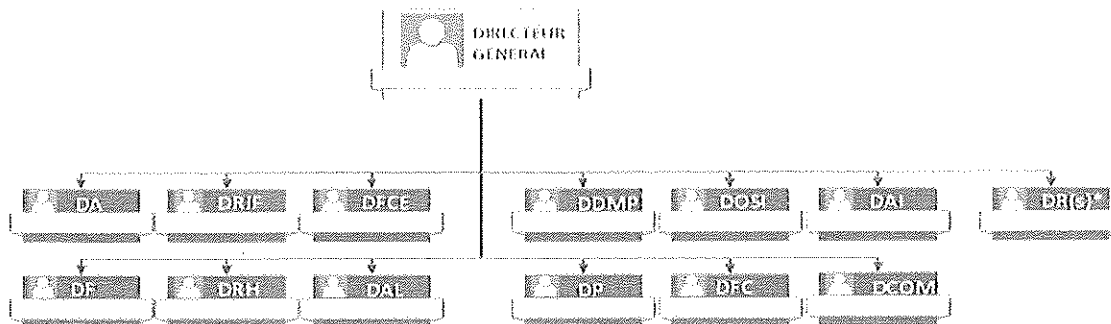
Au niveau local, les établissements assurent la formation professionnelle et mènent les actions stratégiques définies par le système de pilotage de l'OFPPT.

7 20



Organigramme Global

L'organigramme mis en œuvre par l'OFPPT est structuré comme suit :



DA : DIRECTION AUDIT

DAI : DIRECTION AFRIQUE ET INTERNATIONAL

DDMP : DIRECTION DEVELOPPEMENT ET MANAGEMENT DE PROJET

DRIF : DIRECTION RECHERCHE ET INGENIERIE DE FORMATION

DF DIRECTION FORMATION

DFCE: DIRECTION FORMATION EN COURS D'EMPLOI

DRH : DIRECTION DES RESSOURCES HUMAINES

DAL : DIRECTION DE L'APPROVISIONNEMENT ET DE LA LOGISTIQUE

DFC : DIRECTION FINANCIERE ET COMPTABLE

DP : DIRECTION DU PATRIMOINE

DOSI : DIRECTION ORGANISATION ET SYSTEMES D'INFORMATION

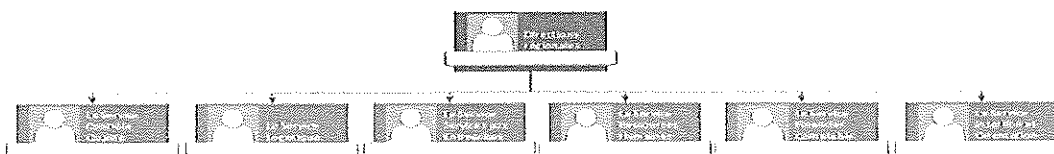
DCOM : DIRECTION DE LA COMMUNICATION

10 DR(s)*: - RABAT SALE KENITRA – MARRAKECH SAFI – TANGER TETOUAN AL HOUCEIMA – ORIENTAL – FES MEKNES – BENI MELLAL KHENIFRA – SOUSS MASSA – DARAA TAFIILET – PROVINCES DU SUD – CASABLANCA SETTAT.

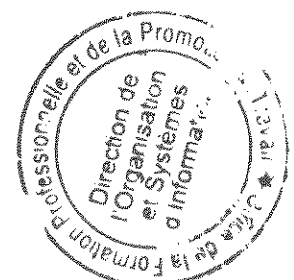
12 CMC(s) : Une CMC pour chaque région du royaume (4 CMC déjà ouverts et le reste en cours).

Organigramme des Directions Régionales

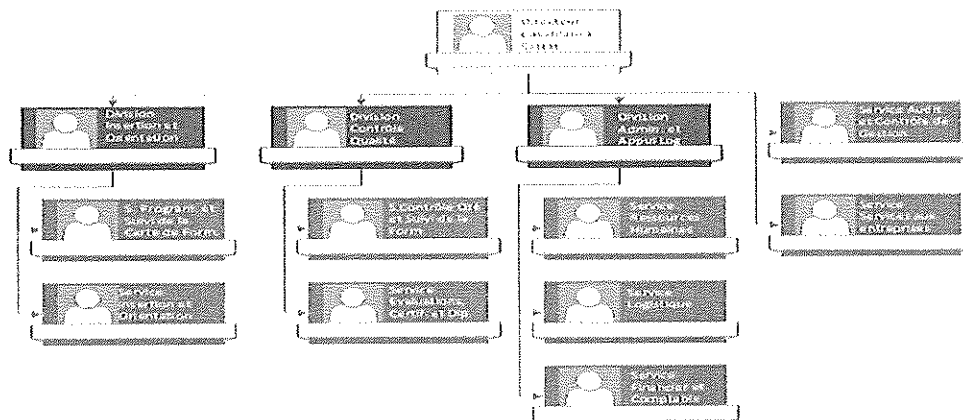
A l'exception de la Direction Casablanca Settata, chaque Direction Régionale est composée de 6 services et dirige en moyenne une trentaine d'établissements de formation.



902



La Direction Régionale Casablanca Settat est structurée en 3 Divisions et 9 Services



DESCRIPTIF DU SYSTEME D'INFORMATION DE L'OFPPT

Les différents constituants du système d'information de l'OFPPT sont :

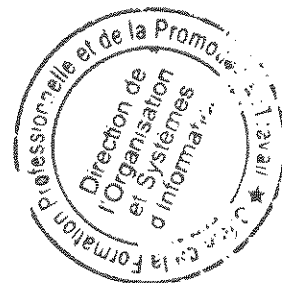
Les infrastructures techniques

Formées d'une infrastructure hyper-convergée, de 20 serveurs physiques, environ 100 machines virtuelles et une vingtaine d'éléments actifs réseau et sécurité localisés dans le Datacenter situés au siège de l'Office.

Deux plateformes sont hébergées au niveau du cloud Azure.

L'OFPPT utilise principalement les systèmes et technologies suivants :

- Environnement de virtualisation AHV et VMware ;
- Systèmes d'exploitation Windows et UNIX/Linux ;
- SGBD Microsoft MySQL, MS SQL, SAP HANA, PostgreSQL
- Plateforme téléphonie full IP ALCATEL
- Solution de sauvegarde (Veeam, Comvault, BRMS)
- Active Directory ;
- Solution sécurité (PALO ALTO, F5 BIG IP)



Le parc informatique

Le parc est constitué d'environ 2000 PC sous Windows dont 500 PC au niveau du siège, 450 au niveau des directions régionales à raison de 30 à 60 par région et 3 à 10 par établissement de formation (staff administratif). Environ 30 MAC sont utilisés au niveau du parc.

Le réseau Lan et Wan

Le réseau informatique WAN de l'OFPPT se compose d'un site central (Siège de l'OFPPT) et de 10 régions. Il se base principalement sur le VPN MPLS de l'opérateur Maroc Télécom.

Le réseau du siège est protégé par un NGFW (en HA) vis-à-vis de l'environnement extérieur.

L'accès à internet est assuré par deux liaisons de ligne louée au niveau du siège et des liaisons de type FTTH.

Les régions disposent chacune d'un accès Internet Fibres Optiques 100 ou 200 M/s, sauf la DRGC qui dispose d'une liaison spécialisée 2 M/s ;

Les établissements de formation EFP ne sont pas reliés au réseau WAN de l'OFPPT. Ils disposent d'un accès Fibre Optique 100 M/s.

Les données suivantes sont données à titre indicatif. En cours de la réalisation du présent marché, et en fonction du besoin le détail sera communiqué.

79 2

L'OFPPT dispose d'un contrat Microsoft permettant l'utilisation des licences Windows Server, SQL server, Azure Entra, Microsoft 365 (2000 A3 et 50 A5), Project, Visio, Power BI.... Ces licences peuvent être utilisées pour le déploiement des solutions objet de ce marché. L'installation et le support est à la charge du prestataire.

L'OFPPT dispose également d'une infrastructure hyper converge Nutanix sur AHV permettant la mise à disposition des ressources pour des machines virtuelles nécessaires pour le déploiement des solutions proposées.

Le prestataire doit assurer le durcissement (hardening) du système d'exploitation sous lequel sa solution logicielle est installée.

Le prestataire doit proposer des solutions, en tenant compte de l'existant, en complétant les licences nécessaires dans son offre. Les solutions proposées doivent être parfaitement intégrées entre eux et avec l'existant.

Le prestataire doit intégrer dans son offre tout module tiers ou prérequis nécessaire pour répondre aux fonctionnalités demandées ci-dessous, et doit les mentionner dans son offre.

Le prestataire doit répondre aux **exigences de l'OFPPT** qui se résument comme suit:

- Fournir une solution qui permet l'intégration avec les flux de travail ainsi qu'un cadre d'exécution commun des meilleures pratiques tel qu'ITIL ou équivalent.
- Faire preuve d'une expertise et d'une expérience démontrée dans la mise en œuvre réussie de solutions technologiques pour une organisation similaire en taille et en portée de la nôtre.
- Avoir des Solutions complètes : une gamme d'offres pouvant répondre à divers aspects de nos opérations, y compris, mais sans s'y limiter, l'infrastructure réseau, la cyber sécurité, la gestion des données, la conformité et les directives opérationnelles.
- Faire preuve d'innovation et d'évolutivité : une approche proactive visant à adopter des technologies émergentes et à fournir des solutions évolutives qui peuvent se développer à mesure du développement de l'OFPPT.
- Faire preuve de partenariats stratégiques mondial avec des leaders/innovateurs technologiques en la matière.
- Assurer le support et la formation nécessaires pour garantir une intégration et une adoption en douceur des nouvelles technologies au sein de notre institution.
- Respecter la Sécurité et la conformité : respect strict des normes de l'industrie en matière de sécurité et de confidentialité des données, ainsi que conformité aux réglementations en vigueur notamment les « Loi 09-08 » et « Loi 05-20 » liées à la Cyber sécurité
- Assurer une bonne gestion de projet avec une méthodologie claire pour la mise en œuvre et la livraison dans les délais.
- Intégrer dans son offre les bonnes pratiques ITIL ou équivalent, pour définir un référentiel adapté aux besoins de l'OFPPT à mettre en œuvre en support de ce chantier depuis la conception jusqu'aux phases de mise en œuvre pour atteindre une intégration et une orchestration efficaces de tous les axes de travail d ce programme sécurité.
- Avoir une adéquation culturelle : une culture organisationnelle qui s'aligne sur la nôtre, mettant l'accent sur la collaboration, l'agilité et l'amélioration continue.

9 2

Le présent appel d'offres est réparti en cinq parties :

- Partie 1 : Évaluation des vulnérabilités & Tests de Pénétration
- Partie 2 : Sécurité des infrastructures
- Partie 3 : Sécurité des identités, des accès et des privilèges
- Partie 4 : Réorganisation de la gestion des services IT selon le référentiel ITIL
- Partie 5 : Sécurité des terminaux & Cybersurveillance



722

PARTIE N°1 : Évaluation des vulnérabilités & Tests de Pénétration

Consistance de la Partie 1 :

Dans le cadre de sa feuille de route de sécurité, l'OFPPT a déployé en 2023 une solution WAAP (Web App and API Protection) pour renforcer la protection de ses applications Web et de ses API contre les attaques avancées, notamment les injections SQL, les attaques par cross-site scripting (XSS), les attaques par force brute, les attaques de robots et les attaques par déni de service distribué (DDoS). A ce stade, l'OFPPT envisage de réaliser un audit de sécurité applicative et des Tests de Pénétration après la mise en place du WAAP non seulement pour confirmer l'efficacité de cette solution, mais aussi pour détecter d'éventuelles vulnérabilités résiduelles au sein des applications et des API cruciales de l'OFPPT.

Item N°1.1 : Evaluation de la sécurité applicative et Test d'intrusion interne et externe

Cette prestation consiste à faire une évaluation approfondie de la sécurité d'une application spécifique. Il vise à identifier les vulnérabilités potentielles, les failles de sécurité et les risques associés à l'application, ainsi qu'à proposer des mesures correctives pour renforcer sa sécurité. Il s'agit de faire :

- **Tests de Pénétration** : Simuler des attaques réelles pour évaluer la résilience de l'application face aux menaces externes.
- **Analyse des Configurations** : Examiner les paramètres de sécurité de l'application, y compris les autorisations d'accès, les configurations réseau, etc.
- **Évaluation des Interfaces Utilisateur** : Vérifier la sécurité des interfaces utilisateur, notamment les formulaires web, les fonctions d'authentification, etc.
- **Audit des Fonctionnalités de Sécurité** : Vérifier que les mécanismes de sécurité de l'application, tels que l'authentification, l'autorisation, la gestion des sessions, et le cloisonnement des profils sont correctement implémentés.
- **Audit des APIs** : consiste à faire une évaluation approfondie de la sécurité des interfaces de programmation applicatives (API), en évaluant la sécurité des interactions entre différentes applications et systèmes via ces API et en vérifiant les processus d'authentification, d'autorisation et de chiffrement.

L'identification des failles se fera sur la base de la dernière version des TOP 10 OWASP ou équivalent.

Le périmètre à couvrir par cet audit est de 4 applications et 2 APIs.

Le prestataire est tenu de réaliser des Tests de Pénétration pour évaluer la robustesse du SI de l'OFPPT et sa capacité à préserver ses données. Il s'agit d'une simulation d'un attaquant externe (depuis internet) et d'un attaquant interne (depuis le réseau de l'OFPPT) afin d'identifier le maximum de points de vulnérabilités des infrastructures, applications et services en ligne.

Les tests doivent être menés selon une méthodologie (à détailler par le prestataire au niveau son offre technique) conformément à l'éthique et aux règles d'art en la matière. Ces tests ne doivent en aucun cas impacter le fonctionnement normal du SI.

L'exploitation de n'importe quelle vulnérabilité ne doit être menée qu'après l'autorisation explicite de l'OFPPT.

9 20

PARTIE 2 :

SECURITE DES INFRASTRUCTURES

Mise en place d'une solution SDWAN, NGFW, LAN et WLAN pour le siège et les directions régionales

Consistance de la partie 2 :

Face à l'obsolescence de ses actifs réseau du siège et des DR, l'OFPPT décide de refondre l'ensemble de son infrastructure réseau en intégrant les solutions de sécurité proposés dans la feuille de route. Il s'agit de mettre en place une nouvelle infrastructure **réseau performante, fiable, sécurisée et évolutive**, avec des **niveaux de service élevés** capable de tenir en condition opérationnelle ses activités actuelles et futures.

L'OFPPT vise à travers ce projet non seulement à améliorer son efficacité opérationnelle mais aussi renforcer sa posture de sécurité contre les cybermenaces croissantes et préparer son infrastructure pour l'avenir.

En vue de disposer d'une sécurité plus robuste, et d'une meilleure performance, d'une gestion simple et centralisée de son réseau et de minimiser l'intervention humaine, l'OFPPT a fait le choix de converger ses équipements de réseau et de sécurité, par la mise en place d'une solution unifiée, centralisée, **de même éditeur**, permettant de gérer par la même plateforme les différentes briques réseau et de sécurité à savoir le NGFW, SD-WAN, le SDN/LAN/WLAN.

L'OFPPT mettra en place des solutions de gestion de la sécurité et de gestion du réseau au niveau de son siège et au niveau de ses directions régionales. Il s'agit de déployer les actifs suivants :

- Item n°2.1 : FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (Siège)
- Item n°2.2 : FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (régions et annexes siège)
- Item n°2.3 : Switch fédérateur
- Item n°2.4 : Switch multi Giga (avec PoE+)
- Item n°2.5 : Switch 48 ports (avec PoE+)
- Item n°2.6 : Switch 24 ports (avec PoE+)
- Item n°2.7 : Point d'accès Wifi
- Item n°2.8 : Solution de management centralisé



Les spécifications techniques minimales

Item n°2.1 : FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (Siège)

La solution cible doit être un firewall Nouvelle Génération qui joue le rôle d'un concentrateur SD-WAN, d'un contrôleur WIFI et qui offre des fonctionnalités SDN et NAC.

LE NGFW doit être classé **leader** (1^{er} rang de classement) dans les derniers **Magic Quadrant** de Gartner (ou équivalent) comme :

- « WAN EDGE infrastructure » ou « SD-WAN » (ou équivalent)
- et
- « Network Firewall » ou « Enterprise Firewall » (ou équivalent)

La solution FIREWALL Nouvelle Génération NGFW sera mis en HA.

La solution doit répondre au minimum aux spécifications techniques suivantes :

Fonctionnalités Next-Generation Firewall

- Module Firewalling statefull pour le filtrage des flux entrants et sortants ;

702

- Permet le filtrage en fonction de l'adresse source, adresse destination, utilisateur, service, protocole, interface d'entrée, Type de Device...
- Permet la création des règles de firewall basé sur l'identité de l'utilisateur en plus d'autres critères : Source/Destination, IP/Sous Réseau, Port Source/Destination
- Possibilité de donner un nom à une règle (l'objectif est de faciliter son suivi dans les logs sur des longues périodes) ;
- Permet de visualiser et de désactiver les règles implicites.
- Permet la gestion des plages d'adresses, des groupes d'IPs (machines, réseaux, plages d'adresses), des groupes d'utilisateurs, groupes de services...
- Permet la gestion de la bande passante par application.
- Permet une Policy Based Routing (routage en fonction de tous les critères d'une règle : l'IP source, l'IP destination, l'interface, protocole, l'interface d'entrée, l'application, FQDN) ;
- Filtrage bloquant par défaut : tout ce qui n'est pas autorisé est interdit.
- Permet la gestion de la répartition de charge et du backup sur plusieurs liens opérateurs par Source/Destination, Utilisateur ou Protocole/Application :
 - Basculement de lien automatique
 - Répartition de charge
 - SDWAN
- Permet le monitoring en temps réel de l'utilisation CPU, Mémoire et disque, les nouvelles sessions, les sessions concurrentes
- Offre une cartographie des connexions logique et physique des équipements (Firewalls, Points d'Acces) et Endpoints (PC, Serveurs et Device mobiles).
- Création et gestion de 10 Firewall Virtuels (licence à fournir)
- Offre le VPN IPsec Site to Site, Client to Site avec ike v1 et v2
- Offre le SSL VPN en mode WEB (pour offrir la possibilité de se connecter a des services sur un portail WEB sans installation de client VPN) et Full (via un client VPN de même marque)
- Permet la ggestion des VLANs (Tag VLAN 802.1q) ;
- Support de l'IPv6 ;
- Support de TLS 1.3 ;
- Support Syslog ;
- Permet l'administration via SSH, https



NB : En vue de renforcer la sécurité du réseau de l'OFPPT, la solution proposée devra être d'une marque différente de PALO ALTO Network utilisée comme firewall dorsal existant

Fonctionnalités SDWAN :

- Permet d'utiliser plusieurs types de liens en Actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VPN MPLS, FTTH, 3G/4G Modem USB,
- Permet de créer des tunnels VPN via Wizard sur le Menu SDWAN pour une facilité de configuration.

90 2

- Permet de créer des SLAs intelligentes pour le basculement et le Load Balancing, ces SLA doivent se baser sur :
 - L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précision
 - Target SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquets
 - Etat de lien pour tester le lien avant de basculer afin de ne pas utiliser un lien non fiable
- Permet la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets.
- Permet les Méthodes de Load Blancing Suivants :
 - IP-Source
 - IP-Source-Destination
 - Spillover
 - Sessions
 - Volume
- Permet d'utiliser des règles de basculement en se basant sur les paramètres suivant suite au mesure SLA :
 - Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)
 - Lowest Cost
 - Maximize Bandwidth
 - Manuel pour obliger le flux à suivre un lien spécifique
- Les règles SDWAN doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,
- Permet d'associer des politiques QoS pour des flux.
- Permet le control des applications afin d'identifier et reconnaitre les applications dans les flux
- Permet l'administration via SSH, https

Fonctionnalités Contrôleur WIFI

- La prise en charge les dernières normes Wi-Fi Alliance telles que Wi-Fi 6 (802.11ax) et 802.11ad, ainsi que les protocoles de sécurité WPA3.
- DNS et SMTP ;
- DHCP ;
- Support SNMP ;
- AAA Security ;
- Support de WIPS ;
- Support de serveur RADIUS ;
- Authentification 802.1x, MAC et WEB (portal captif) ;
- Standards wifi IEEE 802.11ax ;
- Sécurité : AES/WPA2/WPA3 entreprise ;
- Filtrage par MAC



70 2

- IGMP Snooping
- DHCP snooping
- Phishing SSID
- Gestion des accès invités avec isolation sécurisée des ressources internes.
- Il doit assurer l'itinérance transparente pour les utilisateurs se déplaçant dans différentes zones de couverture de points d'accès.
- Configuration à distance à travers une interface graphique WEB (Secure WEB GUI) et interface de gestion centralisée;
- Le contrôleur doit avoir un portail captif afin d'authentifier les utilisateurs,
- Le contrôleur WIFI doit être automatisable via API
- La solution doit permettre la gestion des points d'accès objet de ce CPS (au minimum 250 points d'accès pour le siège et 128 points d'accès pour la région)

Fonctionnalités SDN / LAN & WLAN

- La gestion et l'administration des ressources et équipements réseau LAN et WLAN objet de ce CPS ;
- Le support de l'intégration avec des plateformes Cloud et écosystème tiers via les API ;
- D'offrir une cartographie physique et logique des switches, points d'accès, équipements connectés aux switches objet de ce CPS ;
- L'administration centralisée LAN et WLAN simplifiée :
 - Tagging des ports de plusieurs switches managés par simple clic ;
 - Supervision centralisée de l'état de santé des switches ;
 - Vue de la topologie physique des switches par code couleur (Ring, Uplink, Agrégation des liens, ...)
 - Vue de la consommation POE au niveau de chaque port et chaque switch ;
 - Permet la gestion de tous les aspects de maintenance et gestion opérationnelle des switches et des points d'accès : enregistrement, provisionning, upgrade firmware, commande CLI ;
 - Provisionning des SSIDs simplifié et centralisé ;
 - Possibilité d'importer un Plan architecturale du bâtiment et de positionner les points d'accès sur la carte. Cette fonctionnalité permet d'afficher en temps réel l'état, l'emplacement du point d'accès lors de recherches non structurées ;
 - Module d'analyse spectrale permettant de voir les interférences de signal,
 - Module d'analyse applicative : avoir la capacité de lister tout le trafic applicatif des utilisateurs ;
- La solution doit permettre la gestion des switches objet de ce CPS (au minimum 70 Switchs au niveau du siège et 10 switchs par région)

Fonctionnalités de contrôle d'accès au réseau NAC:

- **Exigences en termes de profiling :**
- Profiling des devices par adresse MAC, Marque, famille d'équipement, type et système d'exploitation ;
- Profiling des utilisateurs par groupe ;
- **Exigences en termes d'authentification :**
- Intégration avec LDAP, RADIUS et Microsoft Active Directory ;
- Support des options d'authentification flexibles comme le 802.1X et MAC Authentication



- Exigences pour la conformité et la remédiation des Endpoints :

- Possibilité d'intégrer des TAGS selon des indices de conformité des postes de travail permettant ainsi de mitiger les risques quant aux postes connectés au réseau : Antivirus à Jours, version d'OS, Patch Windows Installé, présence d'une vulnérabilité ou d'un logiciel installé indésirable. Selon l'état de conformité du poste de travail, il lui sera garantis un niveau d'accès spécifique, ou éventuellement lui assigner un VLAN de quarantaine pour le temps nécessaire à la remédiation

Abonnements des modules de protection

Il s'agit d'un abonnement pour une durée de 5 ans des modules de protection suivants :

Module IPS (prévention des intrusions) (à fournir) pour se protéger contre les menaces réseau existantes et émergentes. Ce module IPS doit avoir deux mécanismes de Détection par signatures et par anomalies ;

- Capable de faire des analyses comportementales de tout type de trafic ;
- Possibilité de créer des signatures personnalisées ;
- Mise à jour automatique des signatures IPS ;
- Création et affectation des politiques IPS par type de zone ou interface ;
- Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, d'envoyer une alarme, d'envoyer un mail, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ;
- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;

Module Antivirus / Antimalware (à fournir) pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;

Module Filtrage URL et de contenu (à fournir), pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux ;

Module Control Applicatif (à fournir), afin d'identifier, reconnaître et contrôler les applications dans les flux

Module Sandboxing cloud (à fournir) pour la protection contre les logiciels malveillants et les attaques zéro days ;

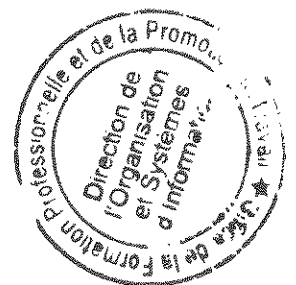
Support Software de 5 ans : 24*7

NB la solution doit supporter le Sandboxing on Premises (local)

Equipement(s) Siège :

Caractéristiques minimales sont :

- Appliances Rackable 19 pouce avec alimentation redondante échangeable à chaud
- Un débit Firewall de 130 Gbps minimum ;
- Un débit IPS Mix de 14 Gbps minimum ;
- Un débit NGFW (FW+IPS+Control Applicatif) de 11 Gbps minimum ;
- Un débit Threat Protection (FW+Antivirus+IPS+Contrôle Applicatif) de 10 Gbps minimum;
- Un débit Inspection SSL de 9 Gbps minimum
- Un débit VPN IPsec de 50 Gbps minimum
- Un débit VPN SSL de 4 Gbps minimum
- Support de 500 000 nouvelles connexions TCP par seconde minimum ;
- Support de 8 millions de connexions TCP simultanées ;
- Support de la haute disponibilité en mode Actif/Passif en mode Actif/Actif Clustering;



- Doté au minimum de 16 ports réseaux 1GbE RJ45;
- Doté au minimum de 8 ports réseaux 1GbE SFP
- Doté au minimum de 4 ports réseaux 10GbE SFP+
- Doté au minimum de 4 ports réseaux 25GE/10GE SFP28
- 1 port pour le HA
- 1 ports 1Gbe RJ45 pour le management
- 1 port console pour le management
- Peut gérer jusqu'à 2 000 tunnels VPN IPSEC Site-to-Site et de 50 000 tunnels VPN IPSEC Client-to-Site ;
- 2 disques SSD (Solid State Drive) d'une capacité minimale de 240 Go en RAID1
- Licence pour création et gestion de 10 Firewall Virtuels
- Licences à fournir : IPS, Antivirus, Contrôle Applicatif, Filtrage URL, et Sandbox Cloud, pour une période de 5 ans
- Support Hardware de 5 ans : 24*7

NB : Tous les ports doivent être activés (avec licence si nécessaire) et livrés avec connecteur
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support.

Item n°2.2 : FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (régions et annexes)

La solution cible doit être un firewall Nouvelle Génération qui joue le rôle d'un concentrateur SD-WAN, d'un contrôleur WIFI et qui offre des fonctionnalités SDN et NAC.

LE NGFW doit être classé **leader** (1^{er} rang de classement) **dans les derniers Magic quadrant de Gartner** (ou équivalent) comme :

- « **WAN EDGE infrastructure** » ou « **SD-WAN** » (ou équivalent)
- et
- « **Network Firewall** » ou « **Enterprise Firewall** » (ou équivalent)

La solution doit répondre au minimum aux spécifications techniques suivantes :

Fonctionnalités Next-Generation Firewall

- Module Firewalling statefull pour le filtrage des flux entrants et sortants;
- Permet le filtrage en fonction de l'adresse source, adresse destination, utilisateur, service, protocole, interface d'entrée, Type de Device...
- Permet la création des règles de firewall basé sur l'identité de l'utilisateur en plus d'autres critères : Source/Destination, IP/Sous Réseau, Port Source/Destination
- Possibilité de donner un nom à une règle (l'objectif est de faciliter son suivi dans les logs sur des longues périodes) ;
- Permet de visualiser et de désactiver les règles implicites.
- Permet la gestion des plages d'adresses, des groupes d'IPs (machines, réseaux, plages d'adresses), des groupes d'utilisateurs, groupes de services...
- Permet la gestion de la bande passante par application.
- Permet une Policy Based Routing (routage en fonction de tous les critères d'une règle : l'IP source, l'IP destination, l'interface, protocole, l'interface d'entrée, l'application, FQDN) ;



702

- Filtrage bloquant par défaut : tout ce qui n'est pas autorisé est interdit.
- Permet la gestion de la répartition de charge et du backup sur plusieurs liens opérateurs par Source/Destination, Utilisateur ou Protocole/Application :
 - Basculement de lien automatique
 - Répartition de charge
 - SDWAN
- Permet le monitoring en temps réel de l'utilisation CPU, Mémoire et disque, les nouvelles sessions, les sessions concurrentes
- Offre une cartographie des connexions logique et physique des équipements (Firewalls, Points d'Acces) et Endpoints (PC, Serveurs et Device mobiles).
- Création et gestion de 10 Firewall Virtuels (licence à fournir)
- Offre le VPN IPsec Site to Site, Client to Site avec ike v1 et v2
- Offre le SSL VPN en mode WEB (pour offrir la possibilité de se connecter a des services sur un portail WEB sans installation de client VPN) et Full (via un client VPN de même marque)
- Permet la gestion des VLANs (Tag VLAN 802.1q) ;
- Support de l'IPv6 ;
- Support de TLS 1.3 ;
- Support Syslog ;
- Permet l'administration via SSH, https

NB : En vue de renforcer la sécurité du réseau de l'OFPPT, la solution proposée devra être d'une marque différente de PALO ALTO Network utilisée comme firewall dorsal existant

Fonctionnalités SDWAN :

- Permet d'utiliser plusieurs types de liens en Actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VPN MPLS, FTTH, 3G/4G Modem USB,
- Permet de créer des tunnels VPN via Wizard sur le Menu SDWAN pour une facilité de configuration.
- Permet de créer des SLAs intelligentes pour le basculement et le Load Balancing, ces SLA doivent se baser sur :
 - L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précision
 - Target SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquets
 - Etat de lien pour tester le lien avant de basculer afin de ne pas utiliser un lien non fiable
- Permet la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets.
- Permet les Méthodes de Load Blancing Suivants :
 - IP-Source
 - IP-Source-Destination
 - Spillover
 - Sessions
 - Volume



70 2

- Permet d'utiliser des règles de basculement en se basant sur les paramètres suivant suite au mesure SLA :
 - Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)
 - Lowest Cost
 - Maximize Bandwidth
 - Manuel pour obliger le flux à suivre un lien spécifique
- Les règles SDWAN doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,
- Permet d'associer des politiques QoS pour des flux.
- Permet le control des applications afin d'identifier et reconnaitre les applications dans les flux
- Permet l'administration via SSH, https

Fonctionnalités Contrôleur WIFI

- La prise en charge les dernières normes Wi-Fi Alliance telles que Wi-Fi 6 (802.11ax) et 802.11ad, ainsi que les protocoles de sécurité WPA3.
- DNS et SMTP ;
- DHCP ;
- Support SNMP ;
- AAA Security ;
- Support de WIPS ;
- Support de serveur RADIUS ;
- Authentification 802.1x, MAC et WEB (portal captif) ;
- Standards wifi IEEE 802.11ax ;
- Sécurité : AES/WPA2/WPA3 entreprise ;
- Filtrage par MAC
- IGMP Snooping
- DHCP snooping
- Phishing SSID
- Gestion des accès invités avec isolation sécurisée des ressources internes.
- Il doit assurer l'itinérance transparente pour les utilisateurs se déplaçant dans différentes zones de couverture de points d'accès.
- Configuration à distance à travers une interface graphique WEB (Secure WEB GUI) et interface de gestion centralisée ;
- Le contrôleur doit avoir un portail captif afin d'authentifier les utilisateurs,
- Le contrôleur WIFI doit être automatisable via API
- La solution doit permettre la gestion des points d'accès objet de ce CPS (au minimum 250 points d'accès pour le siège et 128 points d'accès pour la région)



Fonctionnalités SDN / LAN & WLAN

- La gestion et l'administration des ressources et équipements réseau LAN et WLAN objet de ce CPS ;

702

- Le support de l'intégration avec des plateformes Cloud et écosystème tiers via les API ;
- D'offrir une cartographie physique et logique des switchs, points d'accès, équipements connectés aux switchs objet de ce CPSs ;
- L'administration centralisée LAN et WLAN simplifiée :
 - Tagging des ports de plusieurs switchs managés par simple clic ;
 - Supervision centralisée de l'état de santé des switchs ;
 - Vue de la topologie physique des switchs par code couleur (Ring, Uplink, Agrégation des liens, ...)
 - Vue du consommation POE au niveau de chaque port et chaque switch ;
 - Permet la gestion de tous les aspects de maintenance et gestion opérationnelle des switchs et des points d'accès : enregistrement, provisionning, upgrade firmware, commande CLI ;
 - Provisionning des SSIDs simplifié et centralisé ;
 - Possibilité d'importer un Plan architecturale du bâtiment et de positionner les points d'accès sur la carte. Cette fonctionnalité permet d'afficher en temps réel l'état, l'emplacement du point d'accès lors de recherches non structurées ;
 - Module d'analyse spectrale permettant de voir les interférences de signal,
 - Module d'analyse applicative : avoir la capacité de lister tout le trafic applicatif des utilisateurs ;
- La solution doit permettre la gestion des switchs objet de ce CPS (au minimum 70 Switchs au niveau du siège et 10 switchs par région)

Fonctionnalités de contrôle d'accès au réseau NAC:

- **Exigences en termes de profiling :**
 - Profiling des devices par adresse MAC, Marque, famille d'équipement, type et système d'exploitation ;
 - Profiling des utilisateurs par groupe ;
- **Exigences en termes d'authentification :**
 - Intégration avec LDAP, RADIUS et Microsoft Active Directory ;
 - Support des options d'authentification flexibles comme le 802.1X et MAC Authentication
- **Exigences pour la conformité et la remédiation des Endpoints :**
 - Possibilité d'intégrer des TAGS selon des indices de conformité des postes de travail permettant ainsi de mitiger les risques quant aux postes connectés au réseau : Antivirus à Jours, version d'OS, Patch Windows Installé, présence d'une vulnérabilité ou d'un logiciel installé indésirable. Selon l'état de conformité du poste de travail, il lui sera garantis un niveau d'accès spécifique, ou éventuellement lui assigner un VLAN de quarantaine pour le temps nécessaire à la remédiation

Abonnements des modules de protection

Il s'agit d'un abonnement pour une durée de 5 ans des modules de protection suivants :

Module IPS (prévention des intrusions) (à fournir) pour se protéger contre les menaces réseau existantes et émergentes. Ce module IPS doit avoir deux mécanismes de Détection par signatures et par anomalies ;

- Capable de faire des analyses comportementales de tout type de trafic ;
- Possibilité de créer des signatures personnalisées ;
- Mise à jour automatique des signatures IPS ;
- Création et affectation des politiques IPS par type de zone ou interface ;

702

- Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, d'envoyer une alarme, d'envoyer un mail, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ;
- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;

Module Antivirus / Antimalware (à fournir) pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;

Module Filtrage URL et de contenu (à fournir), pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux ;

Module Control Applicatif (à fournir), afin d'identifier, reconnaître et contrôler les applications dans les flux

Module Sandboxing cloud (à fournir) pour la protection contre les logiciels malveillants et les attaques zéro days ;

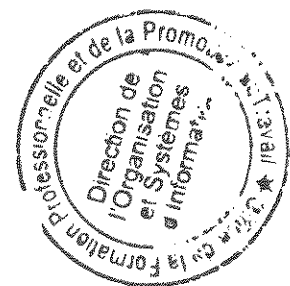
Support Software de 5 ans : 24*7

NB la solution doit supporter le Sandboxing on Premises (local)

Equipement(s) régions et des annexes :

Caractéristiques minimales sont :

- Appliance Rackable 19 pouce avec alimentation redondante ;
- Un débit Firewall de 39 Gbps minimum ;
- Un débit IPS Mix de 5 Gbps minimum ;
- Un débit NGFW (FW+IPS+Control Applicatif) de 3 Gbps minimum ;
- Un débit Threat Protection (FW+Antivirus+IPS+Contrôle Applicatif) de 2.8 Gbps minimum;
- Un débit Inspection SSL de 3 Gbps minimum
- Un débit VPN IPsec de 30 Gbps minimum
- Un débit VPN SSL de 1.5 Gbps minimum
- Support de 140 000 nouvelles connexions TCP par seconde minimum ;
- Support de 3 millions de connexions TCP simultanées ;
- Doté au minimum de 16 ports réseaux 1GbE RJ45 ;
- Doté au minimum de 8 ports réseaux 1GbE SFP ;
- Doté au minimum de 4 ports réseaux 10GbE SFP+;
- Minimum 1 ports 1Gbe RJ45 pour le management
- Minimum 1 port console pour le management
- Peut gérer jusqu'à 2 000 tunnels VPN IPSEC Site-to-Site et de 16 000 tunnels VPN IPSEC Client-to-Site ;
- Licence pour création et gestion de 5 Firewall Virtuels
- Licences à fournir : IPS, Antivirus, Contrôle Applicatif, Filtrage URL, et Sandbox Cloud, pour une période de 5 ans.
- Support Hardware de 5 ans : 24*7



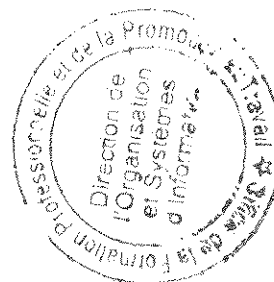
NB : Tous les ports doivent être activés (avec licence si nécessaire) et livrés avec connecteur
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support

70 2

Item n°2.3 : Switch fédérateur

Les Switch fédérateurs doivent être de même marque que l'item n°2.1 de la partie 2 objet de ce CPS et doivent avoir les caractéristiques **minimales** suivantes :

- L'éditeur doit être classé **leader** (1^{er} rang de classement) **dans les derniers Magic quadrant de Gartner** (ou équivalent) comme « **Enterprise Wired and Wireless LAN Infrastructure** » (ou équivalent)
- Rackable 19" ;
- **Minimum 2 ports de 40 G** minimum (face avant du switch) extensible à 4 minimum ;
- **Minimum 2 modules QSFP+ 40Gbe** minimum (A prévoir deux câbles fibre optique adéquats ou le câble AOC (actif optique câble) pour une distance de 10 mètres minimum) ;
- **Minimum 48 ports 10 Gigabit SFP+**
- Minimum un port de management dédié
- Un port de mangement console
- Matrice de commutation **1.7 Tpbs minimum** ;
- Débit de paquet évolutif minimum **1200 Mpps minimum**
- Routage Statique et Dynamique ;
- Agrégation de liens ;
- Support la fonction d'empilement ou regroupement des switchs via des liens 40 Gbps minimum ;
- La pile ou le groupe de 2 switchs minimum
- Support VLAN par port ;
- Support QoS ;
- Sécurité et blocage de ports par adresse MAC ;
- Support DHCP Snooping ;
- Support Inspection ARP Dynamique
- Alimentation redondante échangeable à chaud ;
- Support SSH ;
- Support HTTPS ;
- Support SNMP v3 ;
- Support Syslog ;
- Support SNTP ou NTP ;
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS
- Être livré avec les licences nécessaires,



NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.

Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support

Garantie et support constructeur de 5 ans pièce et main d'œuvre

NB : Les Deux Switchs Fédérateurs doivent :

702

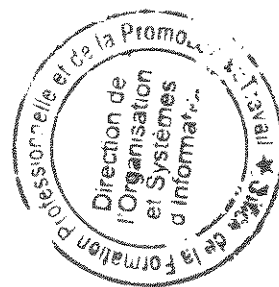
- Fonctionner de façon redondante et en partage de charge ;
- Être équipés de liens d'agrégation de 40 Gbps minimum pour la synchronisation et transfert de données,
- Être livrés avec les câbles et les accessoires nécessaires à leur interconnexion ainsi pour leur pose, raccordement, et mise en service.

Item n° 2.4 : Switch multi Giga (avec PoE+)

Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes, cameras, point d'accès WIFI...).

Ils doivent être de même marque que l'Item n° 2.1 de la partie 2 objet du présent CPS et conformes aux spécifications techniques minimum suivantes :

- Rackable 19" ;
- Minimum 10 ports Multi Giga 1/2.5 min baseT PoE/PoE+
- Minimum 16 ports 1 Gigabits Base T minimum PoE/PoE+
- Minimum 4 ports 10 Gigabit SFP+ dédiés (face avant du switch);
- Minimum un port de management dédié
- Un port de mangement console
- Matrice de commutation **162** Gbps minimum ;
- Débit paquet par seconde de **240** Mpps minimum ;
- Commutation Niveau 2 minimum
- Agrégation de liens ;
- Support la fonction d'empilement ou regroupement des switchs via des liens 10 Gbps minimum ;
- Support VLAN par port ;
- Support QoS ;
- Sécurité et blocage de ports par adresse MAC ;
- Support DHCP Snooping ;
- Support Inspection ARP Dynamique
- Support du PoE 802.3af et PoE+ 802.3at (sur les 24 ports);
- Alimentation redondante ;
- Support SSH ;
- Support HTTPS ;
- Support SNMP v3 ;
- Support Syslog ;
- Support SNTP ou NTP ;
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS
- Être livré avec les licences nécessaires,



NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.

702

Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support

Garantie de 5 ans pièce et main d'œuvre ;

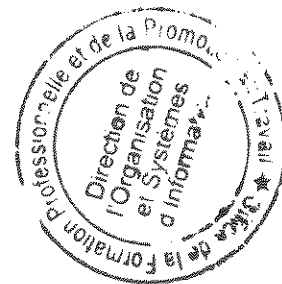
Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.

Item n° 2.5 : Switch 48 ports (avec PoE+)

Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes, cameras...).

Ils doivent être de même marque que l'Item n° 2.1 de la partie 2 objet du présent CPS et conformes aux spécifications techniques minimum suivantes :

- Rackable 19" ;
- minimum 48 ports 10/100/1000 base T PoE/PoE+
- minimum 4 ports 10 Gigabit SFP+ dédiés (face avant du switch) pour l'Uplink avec les Switch fédérateurs ;
- Minimum un port de management dédié
- Un port de management console
- Matrice de commutation 176 Gbps minimum ;
- Débit paquet par seconde de 250 Mpps minimum ;
- Commutation Niveau 2 minimum
- Agrégation de liens ;
- Support la fonction d'empilement ou regroupement des switchs via des liens 10 Gbps minimum ;
- Câble DAC 10 Gbps de 1 m minimum
- Support VLAN par port ;
- Support QoS ;
- Sécurité et blocage de ports par adresse MAC ;
- Support DHCP Snooping ;
- Support Inspection ARP Dynamique
- Support du PoE 802.3af et PoE+ 802.3at (sur les 24 ports) ;
- Support SSH ;
- Support HTTPS ;
- Support SNMP v3 ;
- Support Syslog ;
- Support SNMP ou NTP ;
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS
- Être livré avec les licences nécessaires,



NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.

Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support

Garantie de 5 ans pièce et main d'œuvre ;

Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.

Item n°2.6 : Switch 24 ports (avec PoE+)

Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes, cameras...).

Ils doivent être de même marque que l'Item n° 2.1 de la partie 2 objet du présent CPS et conformes aux spécifications techniques minimum suivantes :

- Rackable 19" ;
- minimum 24 ports 10/100/1000 base T PoE/PoE+
- minimum 4 ports 10 Gigabit SFP+ dédiés (face avant du switch) pour l'Uplink avec les Switch fédérateurs ;
- Minimum un port de management dédié
- Un port de mangement console
- Matrice de commutation 128 Gbps minimum ;
- Débit paquet par seconde 180 Mpps minimum ;
- Commutation Niveau 2 minimum
- Agrégation de liens ;
- Support la fonction d'empilement ou regroupement des switchs via des liens 10 Gbps minimum ;
- Câble DAC 10 Gbps de 1 m minimum
- Support VLAN par port ;
- Support QoS ;
- Sécurité et blocage de ports par adresse MAC ;
- Support DHCP Snooping ;
- Support Inspection ARP Dynamique
- Support du PoE 802.3af et PoE+ 802.3at (sur les 24 ports) ;
- Support SSH ;
- Support HTTPS ;
- Support SNMP v3 ;
- Support Syslog ;
- Support SNTP ou NTP ;
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS
- Être livré avec les licences nécessaires,



NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.

Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support

Garantie de 5 ans pièce et main d'œuvre ;

722

Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.

Item n°2.7 : Point d'accès Wifi

Les points d'accès doivent être des points d'accès haut débit 802.11 ax. Ils doivent être de même marque que l'Item n° 2.1 de la partie 2 objet du présent CPS.

Ils doivent répondre aux spécifications minimales suivantes :

- 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax (OFDMA)
- Dual Radio 802.11ax ;
- MU-MIMO 4x4
- Prise en charge de PoE IEEE 802.3at et 802.3af
- Authentification 802.1x ;
- Prise en charge des protocoles avancés de cryptage et d'authentification :
- AP-TLS, EAP-TTLS et EAP-PEAP
- WPA2/WPA3
- Prise en charge de WIPS et WIDS Radio Modes
- Débit doit atteindre jusqu'à 2.5 Gbps maximum ;
- Minimum 1 port Ethernet 2.5 Gigabit
- Minimum 1 port Ethernet 1 Gbps
- Minimum 4 antennes intégrées ;
- Bluetooth intégré ;
- Support SNMPv3 ;
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS
- Kit de montage mural



Garantie et support constructeur de 5 ans pièce et main d'œuvre

Les Points d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur pose, raccordement, fixation et mise en service.

Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support

Item n° 2.8 : Solution de management centralisé

Le prestataire doit proposer une solution logicielle de gestion et administration centralisée de même éditeur que l'Item n° 2.1 de la partie 2 objet du présent CPS, et devant répondre aux spécifications techniques suivantes :

- Interface unique pour la gestion centralisée des Firewalls, des switches et points d'accès, objet du présent CPS, des différents sites
- La gestion des configurations
- La gestion centralisée des politiques de réseau et de sécurité
- La configuration, le déploiement et la maintenance du SD-WAN.
- La création et le provisionning des templates de configuration par site pour la partie sécurité, WAN, LAN et WLAN
- La gestion des MAJ Firmware

- La gestion des licences, la distribution centralisée du contenu de sécurité et des signatures
- La gestion et la supervision centralisée des tunnels VPN et du SDWAN.
- La gestion et la supervision des performances
- La gestion centralisée des logs des Firewalls, des switchs et points d'accès, objet du présent CPS, des différents sites avec une capacité de traitement de 50 GB de logs par jour minimum
- La supervision du trafic ainsi que la gestion de la Qualité de service.
- Automatiser les flux de travail et les configurations pour les pare-feu, les commutateurs et l'infrastructure sans fil
- Support des API REST, des scripts, des modèles CLI pour l'automatisation et l'orchestration
- La sauvegarde automatisée de la configuration des appareils
- Permet de créer des profils et des domaines d'administration différents
- Support SSL
- Format Appliance virtuelle en promise
- 4 interfaces réseau Giga Ethenet minimum
- Licence pour gestion des items de la partie 2
- Souscription de licences pour une durée de 5 ans ;



Item n° 2.9 : Prestation de service : Installation et mise en service (Siège, Annexes Sièges et Directions Régionales)

Le prestataire doit assurer à sa charge la livraison, l'installation et la mise en service, clé en main, des différents équipements objet de la partie 2 du présent CPS (Firewall, Switchs, contrôleurs, points d'accès WIFI).

Le prestataire doit livrer tous les accessoires et connectiques nécessaires pour la mise en rack et la mise en réseau des équipements objet de ce CPS ;

Dans le cadre des travaux d'installation et de mise en service de la solution clé en main, le prestataire doit réaliser, au préalable une étude d'ingénierie (dossier d'étude détaillée de l'architecture cible) et proposer une configuration cible des éléments actifs réseaux en tenant compte des exigences des services réseaux opérationnels actuellement et ce en concertation avec l'équipe DOSI/OFPPT, et proposer également un plan de migration des anciens switchs mis en production vers les nouveaux switchs objet de ce CPS.

Le prestataire doit se baser sur le plan d'adressage IP, de routage, de découpage VLAN et de gestion de la qualité de service existant avec les adaptations nécessaires.

Le prestataire doit assurer le tirage de câble de bout en bout (cat 6a minimum) des dites points d'accès, leurs fixations, et leurs mises en service.

Le prestataire doit assurer pour la solution wifi :

- De gérer des politiques de sécurité individualisées ou aux groupes d'utilisateurs usant l'accès WIFI ;
- D'appliquer les politiques relatives aux configurations et aux comportements clients pour interdire l'accès au réseau aux unités utilisateurs qui ne disposent pas des configurations de sécurité adéquate ;
- D'offrir une sécurité supplémentaire pour l'accès au réseau de l'entreprise par les utilisateurs invités. Il garantit que ces utilisateurs ne pourront pas accéder au réseau sans passer d'abord par le pare-feu ;

Garantie et maintenance (couvre l'assistance 'sur site ou à distance', l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée de cinq ans avec un délai de prise en charge de 2 heures après déclaration de l'incident et un délai de 4 heures de résolution ou de contournement du problème ;

Livrables du projet :

Le prestataire doit fournir livrables suivants :

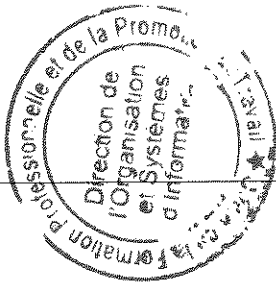
- Un dossier d'ingénierie contenant l'architecture réseau (schéma d'adressage, routage, découpage vlan..);
- Un guide technique d'administration et d'exploitation des équipements ;

Transfert de compétences

Le prestataire doit assurer un transfert de compétence permettant à l'équipe de l'OFPPT d'acquérir les connaissances nécessaires pour assurer l'exploitation des équipements installés objet du présent CPS



90 2



PARTIE 3 :

SECURITE DES IDENTITES, DES ACCES ET DES PRIVILEGES

Mise en place d'une solution IAM, PAM et une infrastructure PKI

Consistance de la partie 3 :

L'OFPPT vise à mener un projet global de sécurité qui assure une gestion complète et efficace des identités, des accès et des privilèges au sein de son organisation, tout en garantissant la sécurité, la conformité et la gouvernance des systèmes informatiques.

Ce projet intègre :

- **Une solution IAM (Identity and Access Management)** combinée à l'**authentification forte** : qui vise à gérer de manière centralisée et sécurisée les identités numériques des utilisateurs ainsi que leurs droits d'accès aux ressources informatiques au sein d'une organisation
- **Une solution de gestion de PKI (Public Key Infrastructure)** : une infrastructure de sécurité utilisée pour créer, gérer, distribuer, stocker et révoquer des certificats numériques qui sont utilisés pour les besoins d'authentification forte, de chiffrement des données et de signature numérique.
- **Une solution PAM (Privileged Access Management)** : offrent des fonctionnalités spécifiques pour gérer et sécuriser les accès privilégiés tels que les comptes d'administrateur système, notamment la gestion des comptes à privilèges, la rotation des mots de passe, la surveillance des sessions privilégiées, l'enregistrement des activités, le contrôle strict pour prévenir les abus et les violations de sécurité.

Cette approche intégrée permet de renforcer la sécurité, de réduire les risques d'accès non autorisés, de violation de données et d'abus de privilèges, d'améliorer la gestion des ressources informatiques, de rationaliser les opérations et d'atteindre l'efficacité opérationnelle.

La gestion globale des identités, des accès et des privilèges implique la mise en œuvre de **politiques**, de **processus** et de **technologies** robustes pour assurer la sécurité et la gouvernance des systèmes informatiques. Cela comprend la définition et l'application de politiques de sécurité, la mise en place de processus de gestion des identités et des accès, le déploiement de solutions IAM, PKI, et PAM adaptées aux besoins spécifiques de l'OFPPT pour assurer une gestion transparente et une protection efficace contre les menaces actuelles et futures.

Le prestataire doit assister l'OFPPT à mettre en place des **processus** solides, une **structure organisationnelle** efficace et une **politique de sécurité et de conformité** pour la gestion des identités, des accès et des privilèges, et ce pour renforcer sa posture de sécurité et garantir un accès sécurisé et autorisé à ses ressources numériques.

Il s'agit de repenser et simplifier son organisation, ses processus et sa politique notamment :

- Les politiques définissant les règles et les normes de sécurité relatives à l'authentification, à l'autorisation et à la gestion des accès
- Structure organisationnelle
- Les processus et les procédures pour la gestion des identités (collaborateur, un partenaire, un stagiaire, un infogérant) et leur cycle de vie complet, y compris la création, la modification, la désactivation/désinscription et la suppression des comptes d'utilisateurs, ainsi que la gestion des attributs d'identification des utilisateurs
- Le Processus d'Identification et d'authentification pour vérifier l'identité des utilisateurs lorsqu'ils accèdent aux systèmes ou aux applications. Cela inclut la définition de la méthode d'authentification selon la criticité du système ou de la donnée à savoir simple authentification par mots de passe, ou d'autres méthodes d'authentification multi-facteurs par de jetons, de certificats...

- Le Processus de Gestion des certificats numériques utilisés pour l'authentification et le chiffrement des données, y compris la création, la distribution, le renouvellement et la révocation des certificats.
- Le Processus de Suivi et de gestion des droits d'accès des utilisateurs tout au long de leur cycle de vie, y compris la revue périodique des droits d'accès pour assurer leur pertinence et leur conformité aux politiques de sécurité. Il inclut le modèle d'attribution des droits d'accès : en fonction des rôles d'utilisateurs dans l'organisation RBAC, en fonction des attributs de l'utilisateur.
- Les processus de surveillance et d'audit des activités d'identification et d'accès pour détecter les anomalies et les comportements suspects.
- Les processus de demande des utilisateurs concernant la création de compte, la demande d'accès, la demande de réinitialisation de mot de passe, de renouvellement de certificat.
- Processus de gestion du cycle de vie des certificats ainsi que les règles de conformité concernant l'usage des certificats électroniques recouvrant ainsi toutes les opérations d'enregistrement ou d'affectation d'une clé dans un système en y incluant aussi la vérification de l'identité de son possesseur, la gestion de ses équipements, des révocations...

Le prestataire doit également assurer la mise en place des solutions IAM, PKI, et PAM qui répondent aux spécifications techniques demandées, le déploiement de ces solutions, ainsi que l'intégration de ces solutions entre elles et avec les systèmes informatiques existants.

Le prestataire doit assurer aussi

- Sécurisation de l'active directory local pour minimiser la compromission des comptes
- Synchronisation Active directory local et Microsoft Entra

Le prestataire doit fournir une conception pour la mise en œuvre des solutions objet de la partie 3 sur mesure en fonction des besoins de sécurité de l'OFPPT. Il doit assurer entre autre

- Le déploiement de ces solutions avec un impact minimal sur les systèmes existants ;
- L'accompagnement des utilisateurs, et leur support pour la conduite de changement et à la mise en œuvre de cas d'usage ;
- Document d'Architecture : Une conception architecturale décrivant les composants des différentes solutions, leur interconnexion et leur intégration avec les systèmes existants de l'organisation
- Documentation des processus
- La formation pour sensibiliser les utilisateurs finaux et les administrateurs aux bonnes pratiques en matière de gestion des identités et des accès

Spécifications techniques minimales

Item n°3.1 : Gestion des identités et des accès (IAM)

La solution IAM, proposée doit permettre de **centraliser** la gestion des identités, garantir l'unicité des identifiants, et automatiser les processus de provisionnement et de dé provisionnement des comptes.

Le prestataire doit assurer la mise en place d'une solution de gestion des identités et des accès notamment la configuration et le support, la solution doit répondre aux exigences techniques détaillées suivantes.

Marque et référence à définir

La solution proposée doit être d'un éditeur classé leader (1er rang de classement) dans les derniers Magic Quadrant de Gartner (ou équivalent) comme « Access Management » ou « Workforce Identity Platform » (ou équivalent)

La souscription des licences de la solution proposée est pour une durée de 3 ans pour un nombre minimum de 1000 utilisateurs

Fonctionnalités

792

La solution IAM doit offrir les fonctionnalités suivantes :

Gestion des identités :

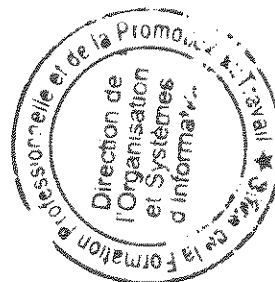
- La création, la modification et la suppression des comptes utilisateurs
- la gestion des attributs d'identité standards tels que le nom, le prénom, l'adresse e-mail, etc
- la gestion des attributs d'identité personnalisés et spécifiques à l'OFPPT
- Stockage sécurisé et cryptage des informations d'identification des utilisateurs, avec des algorithmes avancés de hachage de mot de passe.
- Application de la politique de mot de passe et exigences de sécurité pour garantir des contrôles d'accès sécurisés.
- La synchronisation des identités avec Active directory locale (on prem) avec réécriture des changements de mot de passe.
- Options de réinitialisation de mot de passe en libre-service.
- Gestion centralisée du cycle de vie des identités pour un provisionnement et un déprovisionnement efficaces des utilisateurs.

L'authentification :

Authentification multifacteur (MFA) intégrant deux facteurs ou plus pour une vérification améliorée des utilisateurs.

Méthodes d'authentification :

- Mot de passe
- SMS
- Clé de sécurité FIDO2
- Authentification basée sur des certificats
- Application mobile d'authentification
- Jetons logiciels OATH
- Passe d'accès temporaire (TAP)
- Windows Hello



Authentification unique (SSO) :

- Fonctionnalité SSO transparente permettant aux utilisateurs de se connecter une seule fois pour accéder à plusieurs systèmes ou applications sans avoir à saisir à chaque fois leurs identifiants
- Support des protocoles d'authentification, tels que :
 - Open Autoriaation Oauth 2.0
 - OpenID Connect OIDC
 - Security Assertion Markup Language SAML
 - Authentification basée sur l'en-tête
 - Authentification Windows intégrée
 - Kerberos
 - LDAP
 - Active directory
 - RADIUS

90 2

Authentification adaptative :

- Authentification dynamique basée sur les risques pour ajuster les niveaux de sécurité en fonction des comportements des utilisateurs et de facteurs contextuels (adresse IP, appareil, version du système d'exploitation, ..).
- Analyse des menaces en temps réel pour détecter et répondre aux tentatives de connexion anormales et aux risques de sécurité potentiels.
- Capacités d'authentification continue pour la vérification continue des utilisateurs et la surveillance des sessions.

Gestion des accès et des autorisations

- Mise en œuvre de contrôles d'accès et de privilèges basés sur les rôles pour appliquer les principes du moindre privilège.
- Gestion des groupes et des rôles
- Gestion des privilèges et des accès basés sur les rôles (RBAC)
- Attribution automatique d'utilisateurs/groupes auprès des applications cloud/locales
- Révisions d'accès

Gestion des cycles de vie des identités et des autorisations

Analyse du comportement des utilisateurs pour la surveillance de l'activité des utilisateurs :

- Surveillance et évaluation des interactions des utilisateurs avec les systèmes d'authentification pour l'identification des anomalies.
- Utilisation d'algorithmes d'apprentissage automatique pour la reconnaissance de formes et la détection d'anomalies.
- Alertes et notifications en temps réel en cas de comportement suspect pour contrer de manière proactive les menaces de sécurité potentielles.

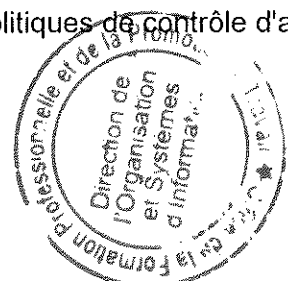
Intégration et évolutivité :

- Intégration transparente avec les applications de l'OFPPT, les services cloud et les systèmes existants pour une couverture complète.
- Évolutivité pour s'adapter à la croissance future et aux exigences d'authentification évolutives.
- Interopérabilité avec des solutions de sécurité tierces et des outils de gestion des terminaux pour des contrôles de sécurité améliorés
- La solution doit supporter en plus de la gestion des identités des collaborateurs de l'OFPPT, la gestion des identités des autres catégories comme partenaire, stagiaire, prestataire, infogérant

Conformité Audit et Journalisation :

- Fonctionnalités de journalisation et de reporting des pistes d'audit pour les audits de conformité et les exigences réglementaires.
- Évaluations de sécurité régulières et examen des mécanismes d'authentification pour maintenir un environnement sécurisé.
- Vérifications de conformité automatisées et mécanismes d'application des politiques pour maintenir un environnement d'authentification sécurisé.
- Génération de journaux d'audit détaillés, de rapports de conformité et de politiques de contrôle d'accès pour les audits réglementaires
- Rapport sur l'état des accès

90 2



Item n°3.2 : Gestion des accès privilégiés (PAM)

Marque et Modèle :

La solution proposée doit être d'un éditeur classé **leader** (1er rang de classement) dans les derniers **Magic Quadrant de Gartner** (ou équivalent) comme « **Privileged Access Management** » ou « **Privileged Identity Management** » (ou équivalent)

- La souscription de licences pour une durée de 3 ans couvrant :
 - o 20 administrateurs
 - o Chaque administrateur doit pouvoir gérer 500 actifs minimum se trouvant sur 11 sites;
- La solution doit permettre de :
- Protéger les administrateurs (administrateur Système, Administrateur réseau, Administrateur base de données, administrateur sécurité...) administrant les actifs avec une traçabilité de leur session.
- Le nombre de comptes utilisateurs (compte root, administrateur local, compte du domaine, comptes de service,) pouvant être gérés par la solution doit être illimité.

Fonctionnalités du PAM :

Découverte des comptes privilégiés

- **Découverte** des comptes locaux, des comptes de domaine, des clés SSH
- **Découverte** des services Windows et des tâches planifiées Windows qui utilisent les comptes privilégiés

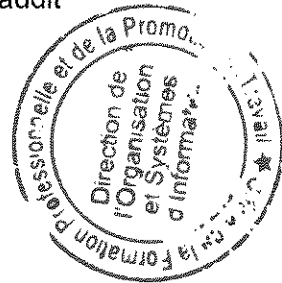
Gestion des comptes et des sessions à privilèges

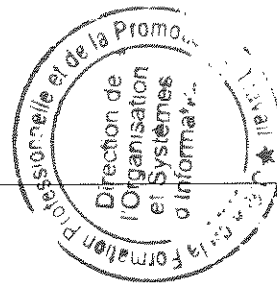
- Stockage sécurisé des informations d'identification avec accès restreint basé sur les rôles.
- Sauvegarde et protection des informations d'identification des comptes privilégiés dans un **coffre-fort** à savoir :
 - Les mots de passe
 - clés SSH
 - Tokens
 - secrets d'accès à des API « clés API »
- Le Coffre-fort doit être sécurisé, chiffré et hautement disponible
- **Rotation** des mots de passe et des clés SSH
 - Selon une périodicité paramétrable
 - Après chaque connexion
 - Selon des politiques de mot de passe :
 - Longueur du mot de passe,
 - Nombre de caractère en minuscule/Majuscule, nombre de caractère spécial et nombre de chiffre,
 - Durée d'expiration
 - À détailler les autres possibilités
- Rotation et gestion automatisées des identifiants pour les comptes privilégiés afin de réduire le risque de vol d'identifiants.



90 2

- **Etablissement automatique des sessions privilégiées via :**
 - RDP,
 - SSH,
 - HTTP/HTTPS
 - MS SQL
 - Établissement de session privilégiée avec injection d'informations d'identification sans dévoiler les mots de passe cibles à l'utilisateur.
 - La consultation des sessions établies (qui est connecté à quoi et depuis quand)
 - Afficher des consignes qui doivent être explicitement acceptées par l'administrateur avant tout accès
 - **Surveillance en temps réel des sessions**
 - Surveillance en temps réel des sessions pour détecter les comportements anormaux et les menaces potentielles pour la sécurité, avec la possibilité de visualiser la session en temps réel avec la possibilité de sa résiliation immédiate
 - Surveiller les actions effectuées par les utilisateurs privilégiés
 - La solution doit permettre de déconnecter automatiquement un utilisateur si une commande ou un texte suspect apparaissent sur la ligne de commande ou à l'écran.
- Alertes et notifications pour les activités inhabituelles ou les violations de politique lors d'un accès privilégié
- **Enregistrement et audit des sessions** des utilisateurs privilégiés (commandes et actions exécutées)
 - Enregistrement de session complet des activités des utilisateurs privilégiés pour les pistes d'audit
 - L'ensemble des activités de la session est enregistré, indexé et stocké dans des pistes d'audit inviolables à savoir :
 - fenêtre active
 - Frappes, Saisie de touches du clavier
 - Clic de souris,
 - Changement de contenu
 - Échange de fichiers via le presse-papiers et les lecteurs locaux redirigés
 - Transfert de fichiers utilisant les différents protocoles, notamment sur les protocoles RDP et SSH.
 - Enregistrement au format vidéo des sessions établies
 - Transcription de l'enregistrement vidéo montrant toutes les métadonnées de session
 - Consultation des enregistrements avec possibilité :
 - De sélectionner directement les événements relatifs aux cliques de la souris ou de la saisie de certaines touches du clavier, ou l'ouverture de certaines fenêtres.
 - D'accélérer les vidéos
 - De prendre des captures de certaines manipulations effectuées lors d'une session.
 - Les enregistrements doivent être chiffrés et horodatés.
 - **Recherche** dans les enregistrements
 - La solution devrait fournir la fonction d'indexation et de recherche des métadonnées de session enregistrées qui permettent de détecter :
 - Le contenu de l'affichage complet de l'écran





- Les commandes exécutées
- Les titres des fenêtres
- Recherche en fonction de commandes, noms d'utilisateurs, date et heure spécifiques exécutées dans une session privilégiée afin de déterminer qui les a exécutées et ce qui s'est passé avant et après
- Recherche rapide (ex : par mots clés, commandes,) des données indexées sur les protocoles en mode texte, en mode graphique.
- Rechercher certains événements dans des sessions avec possibilité de lire l'enregistrement à partir du moment précis où le critère de recherche apparaît.
- La solution doit permettre la gestion du processus de bout en bout de demande d'accès faites par des utilisateurs privilégiés avec des workflows d'approbation.

Demandes d'élévation de privilèges et d'accès :

- Demandes d'accès contrôlées et flux de travail d'approbation pour les privilèges temporairement élevés.
- Fourniture d'accès juste à temps avec autorisations limitées dans le temps et révocation automatique.
- Processus d'authentification et de validation en plusieurs étapes pour les demandes d'élévation de privilèges.
- de validation simple et convivial permettant aux enseignants et aux instructeurs d'accorder aux étudiants l'accès aux machines Labs

Administration et gestion de la solution PAM :

La solution doit fournir une **console d'administration** web intuitive et sécurisée en **HTTPS**

- Prise en charge de l'administration basée sur les rôles (administrateur, utilisateur, auditeur)
- Inventaire des utilisateurs, des ressources et des droits
- La journalisation doit horodater les connexions, les tentatives de connexions, les enregistrements des sessions pour une visualisation ultérieure
- Traçabilité de chaque action (accès aux informations d'identification, actions privilégiées, accès aux enregistrements et données associées (utilisateur, date et heure, type d'action, etc.) de façon exhaustive
- Outil de filtrage et recherche multicritère dans les journaux pour faciliter l'identification des incidents de sécurité.

Rapports d'audit et de conformité :

- La solution proposée doit permettre :
 - de créer manuellement ou automatiquement des rapports selon une fréquence journalière, hebdomadaire ou mensuelle.
 - Envoyer les rapports par email.
- Génération de rapports de conformité - Reporting d'audit et de conformité :
- Création de rapports d'audit détaillés sur les activités d'accès privilégié pour les audits de conformité.
- Options de reporting personnalisables pour suivre les violations des politiques, les avis d'accès et l'activité des utilisateurs.
- Journaux d'audit et rapports sur l'utilisation des informations d'identification et les modifications apportées à des fins de conformité.
- La solution doit être capable de générer des alertes et de notifier automatiquement l'administrateur par message électronique, en cas d'évènement spécifique :
- La solution doit être capable de synchroniser son horloge avec une source de temps NTP

70 2

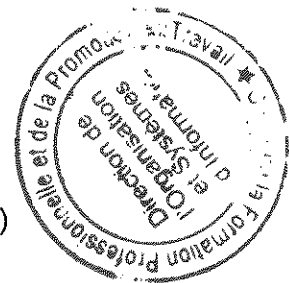
- Permettre la remontée des événements vers une solution SIEM en syslog
- La solution doit fournir une fonctionnalité break glass qui permet de récupérer les mots de passe administrateurs locaux pour l'accès aux actifs en cas d'indisponibilité du PAM.

Intégration et évolutivité :

- Intégration transparente avec les solutions et outils de sécurité existants de gestion des identités et des accès (IAM).
- Évolutivité pour s'adapter à une infrastructure croissante et à un nombre croissant d'utilisateurs privilégiés.
- Prise en charge des intégrations API et de l'interopérabilité avec des applications tierces pour des fonctionnalités étendues.

Les actifs à protéger par le PAM :

- Active Directory
- Windows (comptes administrateurs locaux)
- Unix / Linux (Any Distribution)
- Hyperviseurs (Hyper-V, VMware, AHV, KVM)
- Out-of-Band Management Systems (Lenovo IMM, iDrac, HP iLO,)
- Equipement réseau (ALCATEL CISCO HP)
- Equipement sécurité (PALO ALTO, F5 BIG IP,)
- Database (MySQL, MS SQL, SAP HANA, PostgreSQL)
- Application web
- Les actifs issus du présent CPS



Item n° 3.3 : Infrastructure à clé publique (PKI)

Le prestataire doit assurer la fourniture, la configuration et du support d'une solution PKI complète qui répond aux exigences techniques minimales détaillées suivantes :

Marque et Modèle :

La solution proposée doit être une solution reconnue

- La souscription des licences proposée pour une durée de 3 ans
- La solution doit offrir :
- Un nombre de certificats : par user et par device : 14 000
- Type de certificat :
- SSL/TLS pour les serveurs pour l'authentification serveurs Web, les chiffrements des connexions au serveurs base de données
- Certificat client pour l'authentification (identité numérique), cryptage/signature des email, documents, pour remote network access, aussi chiffrement des données sur les postes nomades, supports amovibles

Objectifs de la solution

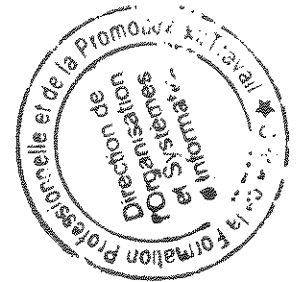
- Mettre en place une infrastructure robuste et sécurisée pour la gestion des certificats numériques.
- Assurer la confidentialité, l'intégrité et l'authenticité des données échangées au sein de l'entreprise.
- Faciliter l'émission, la révocation et le renouvellement des certificats numériques.

702

- Permettre l'intégration avec les systèmes existants, tels que les annuaires LDAP et les applications web.

Les fonctionnalités minimales de la solution :

- Génération de certificats numériques X.509.
- Gestion des demandes de certificats (CSR).
- Révocation des certificats compromis ou expirés.
- Renouvellement automatique des certificats.
- Intégration avec les annuaires LDAP pour l'authentification des utilisateurs.
- Gestion des politiques de sécurité et des profils de certificats.
- Audit et journalisation des opérations effectuées.
- Compatible avec divers systèmes d'exploitation de type Unix, y compris Linux et FreeBSD.
- Bibliothèques cryptographiques pour les opérations cryptographiques.
- Configuration des Politiques : Les administrateurs peuvent définir des politiques pour l'émission et la gestion des certificats en fonction des exigences organisationnelles.
- Application des Politiques : application des politiques pour garantir la conformité aux normes de sécurité et aux exigences réglementaires.
- Scalabilité Horizontale : peut être déployé dans une configuration en grappe pour s'adapter à des charges accrues.
- Haute Disponibilité : Des mécanismes de redondance et de basculement sont pris en charge pour assurer une haute disponibilité des services de certificats.



Déploiement et intégration :

L'OFPPT dispose de plusieurs systèmes existants, le prestataire doit assurer que le serveur PLI devra être capable de s'intégrer avec ces systèmes, notamment :

- Les annuaires LDAP pour l'authentification des utilisateurs.
- Les applications web nécessitant des certificats pour l'authentification SSL/TLS.

Le déploiement du serveur PKI devra être réalisé de manière planifiée et documentée. Des procédures de sauvegarde régulières devront être mises en place pour assurer la disponibilité et l'intégrité des données. Des mises à jour de sécurité devront être appliquées régulièrement pour corriger les vulnérabilités identifiées.

La solution proposée doit assurer au minimum les éléments d'intégration suivants :

- Exposer une API RESTful pour un accès programmable aux fonctionnalités de gestion de certificats.
- Des bibliothèques d'intégration et des SDK sont disponibles pour les langages de programmation populaires (par exemple Python, Java) pour faciliter l'intégration système.

Le prestataire doit impérativement assurer un déploiement de la solution proposée au sein de l'infrastructure de l'établissement.

- Les mesures de sécurité suivantes devront être mises en place par le prestataire :
- Utilisation d'algorithmes cryptographiques robustes pour la génération et la gestion des clés.
- Protection des clés privées avec des mécanismes de stockage sécurisés.
- Contrôles d'accès basés sur les rôles pour limiter l'accès aux fonctionnalités sensibles.
- Intégration avec des mécanismes d'authentification forte, tels que les certificats client ou les jetons d'authentification.
- Utilisation des mécanismes de stockage sécurisé des clés pour protéger les clés privées contre



Support et Formation

Une formation doit être dispensée aux administrateurs chargés de la gestion du serveur PKI avec un support technique disponible après la mise en place de la solution pour la résolution des problèmes rencontrés lors de l'utilisation du serveur PKI.

Le prestataire doit assurer une formation des administrateurs chargés de la gestion de l'infrastructure PKI (5 personnes minimum)

Item n°3.4 : Industrialisation du déploiement des postes de travail

Le prestataire doit mettre en place une solution de déploiement des postes de travail sous Windows, qui consiste à automatiser les tâches quotidiennes répétitives, libérant ainsi l'équipe informatique. Il s'agit de :

- Mettre en place les outils nécessaires pour le déploiement automatisé des postes connecté au réseau de l'OFPPT et les postes de travail hors réseau
- La "masterisation" des postes de travail : création d'une image système standardisée et préconfigurée en personnalisant les configurations et les logiciels selon les besoins de chaque groupe d'utilisateurs
- Durcissement de l'image master « hardening », il s'agit de renforcer la sécurité en appliquant diverses mesures pour réduire les risques d'exploitation par des logiciels malveillants ou des attaquants.
- Automatiser le processus de déploiement des images en utilisant des scripts, des tâches planifiées et des outils de déploiement.
- Maintenance et mise à jour des images ;
- Autonomie utilisateur lors de la réinstallation et restauration en self-service
 - Stratégie de reconstruction de postes en cas de réinstallation de zéro ou de changement de poste de travail
 - Organisation des opérations de réparation des postes de travail et récupération des données utilisateurs

Item n° 3.5 : Solution cryptage des terminaux

- Mise en œuvre d'algorithmes de chiffrement puissants pour protéger les données au repos sur les appareils, notamment les ordinateurs portables, les appareils mobiles et les supports amovibles.
- Les fonctionnalités suivantes devront être respecter au minimum :
 - Chiffrement complet du disque dur
 - Authentification TPM avec connexion automatique pour protéger contre les modifications de l'état du système.
 - Compatibilité avec la norme FIPS 140-2 ou équivalent.
 - Prise en charge de l'authentification multifactorielle
 - Prise en charge avancée du déploiement en masse
 - Gestion centralisée pour, la configuration et la gestion du chiffrement sur un grand nombre de postes de travail.
 - Gestion des clés de récupération centralisée pour pouvoir assurer le rollback en cas de panne.
 - Fonctionnalités de reporting avancées pour surveiller l'état de chiffrement des postes de travail, générer des rapports de conformité et effectuer des audits pour s'assurer que toutes les politiques de sécurité sont correctement appliquées.

9 20

PARTIE N°4 : RÉORGANISATION DE LA GESTION DES SERVICES IT SELON LE RÉFÉRENTIEL ITIL OU EQUIVALENT

Consistance de la partie 4 :

L'OFPPT envisage de réorganiser la gestion de ses services informatiques en adoptant le référentiel ITIL (Information Technology Infrastructure Library) ou équivalent. Cette initiative vise à améliorer la qualité des services informatiques, renforcer la satisfaction des clients, optimiser les opérations IT et renforcer la sécurité des systèmes d'information

Pour ce faire, l'OFPPT fait appel à un professionnel spécialisé en cybersécurité afin de réorganiser ses services informatiques tout en intégrant l'aspect sécurité.

Il s'agit de mettre en œuvre de pratiques et de processus standardisés ITIL V4 ou équivalent, pour réorganiser la gestion de ses services informatiques afin d'améliorer l'efficacité, la qualité, et la sécurité des services IT.

Les pratiques à mettre en œuvre dans cette partie, sont :

➤ Gestion des incidents :

L'objectif de cette pratique est de minimiser l'impact négatif des incidents en rétablissant le fonctionnement normal du service le plus rapidement possible, et ce en définissant :

- la gouvernance, les rôles et les responsabilités qui régissent le processus de gestion des incidents
- les activités qui devraient être impliquées dans la portée du processus de gestion des incidents comprennent :
 - o Identification, journalisation, classification et priorisation des incidents
 - o Enquête sur les incidents, diagnostic, escalade et communication
 - o Résolution et clôture des incidents

➤ Gestion des demandes de service :

L'objectif de cette pratique est de soutenir la qualité convenue d'un service et traitant toutes les demandes de service prédéfinies et initiées par l'utilisateur de manière efficace et conviviale.

➤ Gestion du changement :

L'objectif de cette pratique est de planifier, contrôler et autoriser les modifications apportées à l'environnement informatique d'une manière efficace et coordonné, et ce définissant :

- La gouvernance, les rôles et les responsabilités qui régissent le processus de gestion du changement pour garantir la conformité aux politiques de processus et aux exigences réglementaires.
- Les activités qui devraient être impliquées dans la portée du processus de gestion du changement comprennent
 - o Demande de modification (RFC), évaluation et planification
 - o Approbation du changement
 - o Mise en œuvre, examen et clôture du changement

➤ Gestion des problèmes :

L'objectif de cette pratique est de :

- Faire diminuer le nombre d'incidents : c'est l'objectif principal de ce processus.



9 20

- Prévenir l'apparition de nouveaux incidents et problèmes : cet objectif est le corollaire de l'objectif précédent, mais il va prendre en charge des actions beaucoup plus orientées vers l'anticipation, la proactivité.
- Minimiser l'impact des incidents.
- Optimiser l'efficacité des équipes support.

➤ **Gestion de Centre de service :**

L'objectif de cette pratique la prise en charge de la relation avec les utilisateurs, que ce soit pour le traitement d'un incident ou la gestion d'une demande de services.

➤ **Gestion des actifs :**

Les objectifs principaux de cette pratique sont de planifier et gérer le cycle de vie des actifs de services, de manière à maximiser la valeur de ces actifs, à contrôler leurs coûts, et à gérer leurs risques. Elle va aider la pratique Gestion des fournisseurs en fournissant des informations sur l'acquisition de nouveaux actifs, leurs retraits ou leurs réutilisations

➤ **Gestion de configuration des services :**

La pratique Gestion des configurations est de définir et de contrôler les composants de services et d'infrastructure, et de maintenir des informations précises et exactes sur leurs états actuels, sur leurs historiques et sur leurs états planifiés.

➤ **Gestion du catalogue de services :**

L'objectif de cette pratique est de fournir une source unique d'informations cohérentes sur tous les services et offres de services, et garantir qu'elles sont disponibles pour le public concerné.

➤ **Gestion des niveaux des services :**

L'objectif de cette pratique de garantir que la prestation de services est correctement évaluée, surveillée et gérée par rapport à ces objectifs.

➤ **Gestion de la disponibilité :**

L'objectif de cette pratique est de garantir que les services fournissent des niveaux de disponibilité convenus pour répondre aux besoins des clients et des utilisateurs.

➤ **Gestion des capacités et des performances :**

L'objectif de cette pratique est de garantir que les services atteignent les performances convenues et attendues.

➤ **Gestion de la continuité des services :**

L'objectif de cette pratique de gestion de la continuité des services est de garantir que la disponibilité et les performances d'un service sont maintenues à des niveaux suffisants en cas de sinistre. Cette pratique fournit un cadre pour renforcer la résilience organisationnelle

➤ **Gestion du déploiement :**

L'objectif de cette pratique d'assurer de la gestion du passage d'un environnement test ou recette à un environnement de production nécessitant un déplacement du matériel, les logiciels, la documentation,

➤ **Développement et gestion des logiciels :**

L'objectif de cette pratique est de s'assurer que les applications créées répondent aux besoins des parties prenantes.

➤ **Gestion de l'infrastructure et des plates-formes**

L'objectif de cette pratique est de superviser l'infrastructure et les plateformes utilisées

➤ **Gestion des fournisseurs**

702

L'objectif de cette pratique est de garantir que les fournisseurs de l'organisation et leurs performances sont gérés de manière appropriée pour soutenir la fourniture transparente de produits et de service de qualité. Cela implique de créer des relations plus étroites et plus collaboratives avec les fournisseurs clés pour découvrir et réaliser une nouvelle valeur et réduire le risque d'échec.

➤ **Gestion des connaissances**

L'objectif de cette pratique est de Recueillir, capitaliser et partager les connaissances au sein de l'organisation.

➤ **Mesures et Rapports**

L'objectif de la pratique de mesure et de production de rapports est de permettre une bonne prise de décision en réduisant les niveaux d'incertitude.

L'OFPPT dispose d'un Service Desk sous GLPI qui a pour rôle d'enregistrer les incidents et les demandes de services et qui permet le suivi de leur résolution. Il est le point d'entrée et le point de contact unique avec les collaborateurs de l'OFPPT.

Item N°4.1 : Mise en œuvre des pratiques ITIL ou équivalent

La mission portera sur la formalisation des processus et pratiques ITIL v4 ou équivalent en tenant compte du contexte de l'OFPPT ainsi que sur les actions de conduite de changement en la matière.

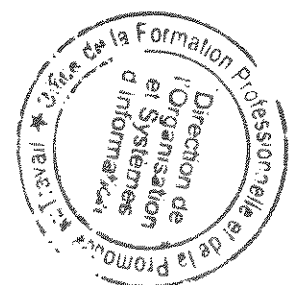
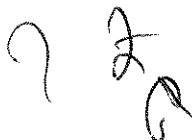
Le prestataire doit proposer une documentation de tous les aspects du projet fournissant ainsi des guides détaillés et des références pour assurer une gestion transparente et une évolution future harmonieuse des processus IT, notamment les documents suivants :

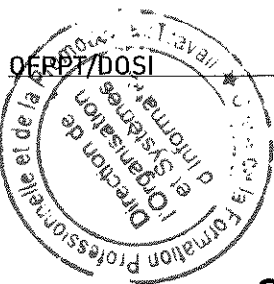
- Document de terminologie ;
- Description détaillée de chaque processus ;
- Procédures opérationnelles d'exécution de chaque processus ;
- Matrice de responsabilité (RACI) : qui définit les responsabilités de chaque acteur impliqué dans les processus ITIL ou équivalent, y compris les responsables, les contributeurs, les approbateurs, etc.
- Mesures de performance et indicateurs de performance clés (KPI) : pour évaluer l'efficacité des processus ITIL ou équivalent mis en place, comme le temps moyen de résolution des incidents, le taux de réussite des changements, etc.
- Plan de communication : pour informer et impliquer les parties prenantes sur l'implémentation des bonnes pratiques ITIL ou équivalent.
- Recommandations en terme d'améliorations organisationnelles.

Le prestataire doit prévoir des séances d'accompagnement et de support pour l'équipe DOSI sur la mise en place des pratiques clé du référentiel ITIL v4 ou équivalent citées ci-dessus..

Item N°4.2 : Formation et certification sur les bases fondamentales ITIL V4 ou équivalent

Le prestataire doit assurer la formation ITIL Fondation ou équivalent avec certification pour le personnel de la DOSI (8 personnes minimum), garantissant une compréhension complète des nouveaux processus et une maîtrise des bonnes pratiques.





PARTIE 5 :

Sécurité des Terminaux & Cybersurveillance

Consistance de la partie 5 :

Face à la pénurie d'experts en cybersécurité, l'OFPPT souhaite externaliser la supervision et la gestion proactive des réseaux et des systèmes, la surveillance des menaces et le maintien en condition opérationnelle du système d'information (SI).

À cet égard, l'OFPPT a souscrit à une gamme de solutions de gestion et de sécurité ainsi qu'à des services managés, incluant notamment :

- **NOC (Network Operations Center) managé :**
 - Supervision et gestion proactive des réseaux et des systèmes.
 - Surveillance en temps réel pour détecter et résoudre les incidents avant qu'ils n'affectent les utilisateurs finaux.
 - Maintenance des infrastructures réseau pour assurer leur disponibilité et performance optimales.
- **EDR (Endpoint Detection and Response) managé :**
 - Surveillance continue des points de terminaison pour détecter et répondre aux menaces.
 - Analyse des comportements pour identifier des activités suspectes ou malveillantes.
 - Capacité à isoler, contenir et remédier aux incidents de sécurité sur les postes de travail et les serveurs.
- **Solution d'industrialisation de déploiement des postes de travail :**
 - Automatisation et standardisation du processus de déploiement des postes de travail.
 - Réduction des temps de déploiement et des erreurs humaines.
 - Gestion centralisée des configurations et des mises à jour des systèmes d'exploitation et des applications.
- **Solution de chiffrement :**
 - Protection des données sensibles grâce au chiffrement des fichiers, des disques et des communications.
 - Prévention de la fuite de données en cas de perte ou de vol des dispositifs.
 - Conformité avec les réglementations et les normes de sécurité des données.
- **SOC (Security Operations Center) managé:**
 - Surveillance et analyse centralisée des événements de sécurité.
 - Réponse aux incidents de sécurité, incluant la détection, l'analyse, la réaction et la récupération.
 - Mise en place de mesures préventives pour améliorer la posture de sécurité de l'organisation.

Externaliser les services NOC, SOC et EDR permettra à l'OFPPT de bénéficier d'une expertise spécialisée, de réduire les coûts, d'accéder aux dernières technologies, de garantir une surveillance continue et une réponse rapide aux incidents, de respecter les exigences de conformité, et de gérer les risques de manière plus efficace. Ces avantages rendent l'externalisation attrayante pour de nombreuses organisations cherchant à renforcer leur sécurité et leur efficacité opérationnelle.

70 2

Les spécifications techniques minimales

Item n°5.1 : NOC (Network Operations Center) managé

Le Network Operations Center (NOC) ou Centre d'Opérations Réseau, a pour objectif le maintien de la disponibilité, de la performance et de la sécurité des infrastructures informatiques de l'OFPPT, contribuant ainsi au bon fonctionnement des activités de l'office.

Le NOC doit assurer la gestion, la supervision, la maintenance, l'assistance et la résolution des problèmes en arrière-plan à travers des services individualisés en fonction des besoins spécifiques à savoir :

- Gestion des actifs :

- Inventaire complet des postes de travail, des serveurs, des applications logicielles, des services
- Fonctions de suivi, de catégorisation et de gestion du cycle de vie des actifs afin d'optimiser leur utilisation et d'améliorer la visibilité.
- Cartographie de l'infrastructure et production des rapports spécifiques
- Intégration avec les systèmes de help desk et les plateformes de gestion des services pour une résolution rationalisée des incidents et un suivi des actifs.

- Gestion des correctifs

Le NOC doit assurer la gestion des correctifs qui consiste à mettre à jour tous les logiciels et périphériques avec des correctifs importants, sans nécessiter de maintenance individuelle. Il s'agit de principalement de :

- Déploiement automatisé de correctifs pour les systèmes d'exploitation (Windows/Linux, Mac), les logiciels bureautiques, les applications, les navigateurs (Edge, Chrome, Firefox) et les dispositifs de réseau afin de remédier aux vulnérabilités et d'assurer la sécurité du système.
- Analyses programmées des correctifs, tests et fonctionnalités de rapport pour suivre l'état et la conformité des correctifs sur l'ensemble du réseau.
- Capacités de retour en arrière des correctifs et tests de compatibilité pour atténuer les risques potentiels et garantir la stabilité du système.
- Intégration avec des outils d'évaluation des vulnérabilités et des flux de renseignements sur les menaces pour une application proactive des correctifs.

- Supervision :

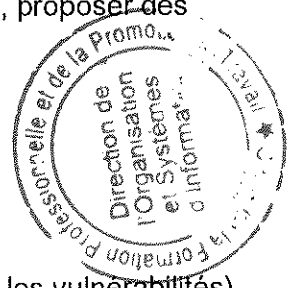
- Surveillance en temps réel des performances, de la disponibilité et de l'état des actifs pour détecter de manière proactive les problèmes et garantir un fonctionnement optimal.
- Mécanismes d'alerte en cas de défaillance du système, de dégradation des performances, d'incidents de sécurité et de comportement anormal des actifs.
- Seuils, notifications et escalades configurables pour une réponse et une résolution rapide des alertes.

- Génération de rapports en temps réel

Le NOC génère des rapports réguliers sur les performances et la disponibilité des actifs. Il effectue également des analyses post-mortem des incidents pour identifier les causes profondes, proposer des solutions d'amélioration et prévenir les problèmes futurs.

Le prestataire est tenu à assurer les services suivants :

- Surveillance de la santé de chaque appareil.
- Surveillance et alerte des bases de données antivirus.
- Fourniture de l'inventaire logiciel de chaque appareil.
- Mises à jour régulières des correctifs (cela garantit que l'appareil est protégé contre les vulnérabilités).



Handwritten signature

- Installation ou de désinstallation des logiciels selon les besoins.
- Vérifications et suivi quotidiens des journaux.
- Vérifications antivirus quotidiennes.
- Vérification des sauvegardes et actions correctives si nécessaire.
- Inclus les fonctionnalité d'assistance à distance des utilisateurs



Le périmètre à couvrir par le NOC managé :

- Les actifs existants :
 - 1000 Postes de travail et serveurs physiques au niveau siège et région
 - 110 machines virtuelles
- Les nouveaux actifs objet des différentes parties de ce marché

Item n°5.2 : Solution EDR managé

Le NOC doit assurer le monitoring des agents de l'Endpoint Detection Response EDR.

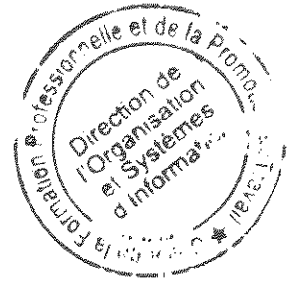
La solution EDR proposée doit permettre la :

- Protection antivirus
 - Protection en temps réel contre les virus, les logiciels malveillants, les ransomwares, les chevaux de Troie et d'autres menaces en analysant les fichiers et les activités en cours d'exécution sur l'ordinateur.
 - Analyse des fichiers téléchargés, les pièces jointes d'e-mails et les périphériques de stockage amovibles pour détecter les menaces potentielles et les isoler avant qu'elles n'endommagent le système.
 - Protection contre les ransomwares pour protéger les fichiers contre le chiffrement non autorisé et les demandes de rançon avec possibilité de restauration après une attaque.
 - Filtrage des sites web malveillants connus pour distribuer des logiciels malveillants, du phishing ou d'autres menaces en ligne.
 - Analyse personnalisée et planifiée pour vérifier les fichiers, les dossiers ou les disques selon un calendrier prédéfini.
 - Mises à jour automatiques des bases de données de signatures de virus et des moteurs de détection pour garantir une protection contre les nouvelles menaces.
 - Gestion à distance qui permettent aux administrateurs de surveiller et de gérer les solutions antivirus installées sur plusieurs ordinateurs depuis une console centralisée.
- Détection et prévention des menaces :
 - Surveillance en temps réel des activités des terminaux, du trafic réseau et du comportement des utilisateurs pour détecter et prévenir les menaces avancées, les logiciels malveillants et les activités suspectes.
 - Analyse comportementale, apprentissage automatique et intégration des renseignements sur les menaces pour une détection et une prévention proactives des menaces.
 - Contrôles de sécurité des terminaux, liste blanche des applications et capacités de chiffrement pour protéger les terminaux contre les activités malveillantes.
- Réponse aux incidents :
 - Capacités de réponse aux incidents rapides, de confinement et de récupération pour atténuer les incidents de sécurité et les cyberattaques sur les terminaux.
 - Outils d'analyse forensique, de recherche de menaces et d'enquête sur les incidents pour identifier les causes profondes et l'attribution des menaces.

- Actions correctives, fonctionnalités de quarantaine et d'isolation pour contenir et atténuer les failles de sécurité des terminaux.

Le périmètre à couvrir par l'EDR managé :

- Les terminaux existants :
 - 1000 Postes de travail et serveurs physiques au niveau siège et région
 - 110 machines virtuelles
- Les nouveaux terminaux objet des différentes parties de ce marché



Item N°5.3 : Solution SOC managé

Le Security Operations Center (SOC) ou le Centre Opérationnel de Sécurité, a pour objectif de surveiller et d'analyser en temps réel la posture de sécurité de l'OFPPT afin d'anticiper les cyberattaques.

Le SOC est chargée de surveiller en continu les systèmes informatiques, les réseaux, les applications et les données afin de détecter, d'analyser et de répondre aux menaces de sécurité

Le SOC analyse l'incident pour comprendre sa nature, son impact potentiel et les techniques utilisées par les attaquants.

Le SOC met en œuvre des mesures de réponse pour contenir et éradiquer la menace. Cela peut inclure l'isolation des systèmes infectés, le blocage des adresses IP malveillantes, la désactivation des comptes compromis, etc.

Le SOC effectue une analyse approfondie des tendances et des modèles d'attaques pour identifier les vulnérabilités potentielles et les faiblesses de sécurité.

Le SOC doit fournir des rapports de remédiation priorités en fonction des risques pour aider à concentrer les efforts là où le meilleur retour sera obtenu, ainsi que des rapports de tendance et des rapports exécutifs à l'intention de la direction (les activités de sécurité, les incidents détectés, les mesures prises et les recommandations d'amélioration).

Le SOC doit permettre une amélioration continue de la posture de sécurité de l'OFPPT à travers l'utilisation des technologies de sécurité de pointe, l'ajustement des stratégies de détection et de réponse, et l'adoption des meilleures pratiques de sécurité.

La plateforme SOC doit permettre de déployer des capteurs physiques et/ou software. Ces capteurs doivent être en mesure de collecter les journaux locaux des dispositifs et de signaler les alertes pour remédiation. Les agents doivent pouvoir être installés sur n'importe quel appareil Windows, MAC, Linux.

La plateforme SOC doit fournir un ensemble de méthodes d'alerte et de détection, y compris, mais sans s'y limiter, les intrusions dans le réseau, le comportement du réseau, les résumés de détection, les menaces émergentes et les événements de suivi.

La plate-forme SOC doit pouvoir s'intégrer à l'"Active Directory" de l'OFPPT et à l'environnement "Microsoft Entra" le plus récent.

La plateforme SOC doit être en mesure de fournir une vue complète de tous les services basés sur le cloud : Entra ID & O365, Azure, AWS...

La plateforme doit être capable d'ingérer tous les types de formats de journaux, l'ingestion doit pouvoir prendre n'importe quel "format" de journal et, s'il n'est pas disponible, la plateforme doit être capable de configurer un processus d'ingestion de journaux. Les types de journaux doivent être (au moins) les suivants : pare-feu, AV & EDR, applications et services.

La plateforme SOC doit également comprendre une "section de renseignement" qui fournit au moins les données de renseignement suivantes : recherches et analyses sur le Dark Web, renseignements sur les menaces, analyse des vulnérabilités, évaluations de la réputation et un fil d'actualité sur la sécurité.

La plateforme doit être gérée par le fournisseur 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

Le SOC doit disposer des outils et des services avancés à savoir :

Détection d'intrusion

La plateforme SOC doit pouvoir s'intégrer avec les solutions existantes et les solutions déployées dans le présent marché pour la détection d'intrusion en se basant sur les IoC et en intégrant IA dans le processus de détection.

Il est nécessaire de disposer d'une sonde de détection qui dispose au minimum des fonctionnalités suivantes :

- Fonctionnement offline (maîtrise des données, etc)
- Analyse avec plusieurs
- Analyse statique et heuristique
- Retro-analyse de fichiers dans le temps
- Détection de communications C&C inconnus
- Interfaçage avec des outils avec des outils de Threat Intelligence
- Possibilité de dropé du flux en se basant sur IP/port/Vlan
- Possibilité de faire de l'agrégation de flux (si TAP branché en direct sur la sonde)
- Interface pour soumettre un fichier et l'analyser avec des moteurs AV
- Pouvoir identifier un flux par IP/port/vlan / sonde de capture / interface de capture
- Ingestion des journaux du pare-feu pour une analyse plus approfondie via les intégrations syslog

Il doit permettre également :

- Détection de compromission de fichiers (contrôle d'intégrité)
- Analyse de la base de registre (windows) ou des LKMs (Linux)
- Analyse et corrélation de logs en provenance de firewalls hétérogènes
- Analyse des flux cryptés
- Vérification de l'intégrité des systèmes

Gestion des vulnérabilités :

Pour détecter les nouvelles vulnérabilités signalées via l'utilisation d'outils de scan de vulnérabilités, l'analyse des bulletins de sécurité et la surveillance des flux de Threat Intelligence

SIEM

Le Security Information and Event Management SIEM pour la collecte, l'analyse et la gestion des informations sur les événements de sécurité informatique à partir de différentes sources (applications, appareils, réseau, serveurs utilisateurs

Le SIEM doit offrir les fonctions de base suivantes :

- Gestion des journaux : Les systèmes SIEM centralisent de grandes quantités de données qu'ils organisent en vue de déterminer si celles-ci présentent des signes de menace, d'attaque ou de violation.
- Corrélation entre les événements : afin de détecter rapidement les menaces potentielles et d'y répondre.
- Surveillance et réponse aux incidents : Les technologies SIEM surveillent les incidents liés à la sécurité sur le réseau d'une organisation, et fournissent des alertes et des audits pour toutes les activités en lien avec ces incidents.



70 2

Plateformes de Threat Intelligence :

Pour agréger les données provenant de diverses sources, telles que des flux de renseignements sur les menaces TIF, des rapports de sécurité, des analyses de vulnérabilités, IDS, SIEM, Firewall, etc. Elles fournissent des fonctionnalités avancées d'analyse et de corrélation pour identifier les schémas et les tendances des menaces

Services de veille sur les menaces :

Ces services fournissent des rapports et des analyses détaillées sur les tendances actuelles des menaces, les groupes de cybercriminels, les vulnérabilités exploitées, etc.

Services de Threat Hunting :

Le Threat Hunting consiste à rechercher activement des indicateurs de compromission (IOC) et des comportements anormaux qui pourraient échapper à la détection automatisée

Le prestataire est tenu à assurer les services suivants :

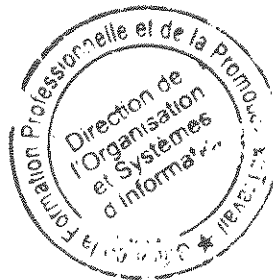
- Surveillance 24/7 :
 - o Surveillance continue des systèmes, des réseaux et des terminaux pour détecter et répondre aux incidents de sécurité en temps réel.
- Détection et Analyse des Menaces :
 - o Utilisation d'outils de détection des menaces, d'analyses comportementales et de technologies avancées pour identifier les activités suspectes et les anomalies.
 - o Analyse des alertes pour déterminer leur gravité et leur pertinence.
- Réponse aux Incidents :
 - o Gestion des incidents de sécurité, y compris l'investigation, la réponse et la résolution des problèmes.
- Gestion des Alertes :
 - o Gestion des alertes de sécurité.
 - o Priorisation des alertes en fonction de leur impact potentiel et de leur urgence.
- Analyse Forensique :
 - o Réalisation d'analyses approfondies pour comprendre les incidents de sécurité, reconstituer les événements et collecter des preuves pour les enquêtes.
- Gestion des Journaux et des Événements :
 - o Collecte, centralisation et analyse des journaux système, des journaux d'application et des événements de sécurité.
- Gestion des Vulnérabilités :
 - o Identification et évaluation des vulnérabilités dans les systèmes et les applications.
- Rapports et Documentation :
 - o Génération de rapports réguliers sur la sécurité, les incidents et les activités du SOC.
 - o Documentation des incidents, des actions entreprises et des leçons apprises.
- Conseil et Optimisation :
 - o Fourniture de recommandations pour améliorer la posture de sécurité globale.
- Formation et Sensibilisation :
 - o Formation sur les meilleures pratiques en matière de sécurité.

708

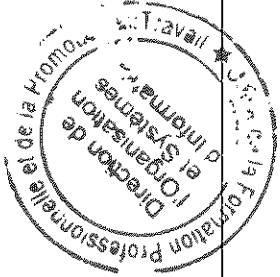
- Sensibilisation aux menaces émergentes et aux nouvelles vulnérabilités.

Le périmètre à couvrir par le SOC managé :

- Les actifs existants :
 - 1000 Postes de travail et serveurs physiques au niveau siège et région
 - 110 machines virtuelles
- Les nouveaux actifs objet des différentes parties de ce marché



7 2 12



OFPPT/DOSI

Dossier d'Appel d'Offres

AO_N° 98/2024

BORDEREAU DES PRIX – DETAIL ESTIMATIF–**Objet : PROJET INFRASTRUCTURE ET SECURITE SYSTÈME D'INFORMATION DE L'OFPPT AU NIVEAU DU SIEGE & DES DIRECTIONS REGIONALES**

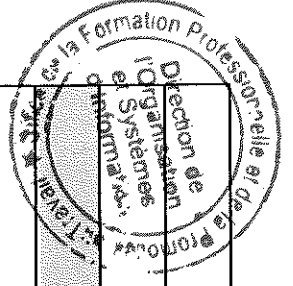
Item n°	Désignation	Unité	Quantité	Prix unitaire en DH HT	Prix total en DH HT
Partie 1 : Évaluation des vulnérabilités & Tests de Pénétration					
1.1	Evaluation de la sécurité applicative et Test d'intrusion interne et externe	JH	55		
Partie 2 : Sécurité des infrastructures					
Mise en place d'une solution NGFW, SDWAN, LAN et WLAN pour le siège et les directions régionales.					
2.1	FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (siège) :	U	2		
2.2	FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (régions et annexes siège)	U	12		
2.3	Switch fédérateur :	U	2		
2.4	Switch multi Giga (avec PoE+)	U	7		
2.5	Switch 48 ports (avec PoE+)	U	41		
2.6	Switch 24 ports (avec PoE+)	U	33		
2.7	Point d'accès Wifi	U	139		
2.8	Solution de management centralisé (souscription de licence)	U	1		
2.9	Prestation de service	Forfait	Forfait		

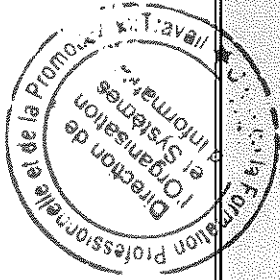
Partie 3 : Sécurité des identités, des accès et des privilèges

Solution de Gestion des identités et des accès (IAM)				
3.1				
3.1.1	Souscription de licences de la solution IAM	U	1000	
3.1.2	Implémentation et déploiement	JH	20	
3.1.3	Formation	JH	10	
3.2	Solution de Gestion des accès privilégiés (PAM)			
3.2.1	Souscription de licences de la solution PAM	U	20	
3.2.2	Déploiement et mise en service	JH	60	
3.2.3	Formation	JH	10	
3.3	Infrastructure à clé publique (PKI)			
3.3.1	Souscription de licences de la solution PKI	U	1	
3.3.2	Déploiement et mise en service	JH	55	
3.3.3	Formation	JH	5	
3.4	Industrialisation du déploiement des postes de travail			
3.5	Solution cryptage des terminaux	JH	10	

Partie 4 : Réorganisation de la gestion des services IT selon le référentiel ITIL ou équivalent

4.1	Mise en œuvre des pratiques ITIL ou équivalent	JH	54	
4.2	Formation et certification	JH	5	





OFPPT/DOSI

Dossier d'Appel d'Offres

AO N° 98/2024

Partie 5 : Sécurité des terminaux & Cybersurveillance

5.1	Solution NOC managé				
5.1.1	Souscription de licences du NOC managé pour les actifs existants	mois	12		
5.1.2	Souscription de service du NOC managé pour les nouveaux actifs	mois	12		
5.1.4	Déploiement et Formation	JH	30		
5.2	Solution EDR managé				
5.2.1	Souscription de licences de l'EDR managé pour les actifs existants	mois	12		
5.2.2	Souscription de licences de l'EDR managé pour les nouveaux actifs	mois	12		
5.2.4	Déploiement et Formation	JH	20		
5.3	Solution SOC managé				
5.3.1	Souscription de licences du SOC managé pour les actifs existants	mois	12		
5.3.2	Souscription de licences du SOC managé pour les nouveaux actifs	mois	12		
5.3.4	Déploiement et Formation	JH	20		
Montant total en DH HT					
Montant TVA en DH (taux TVA=20%)					
Montant total en DH TTC					

Fait à _____, le _____

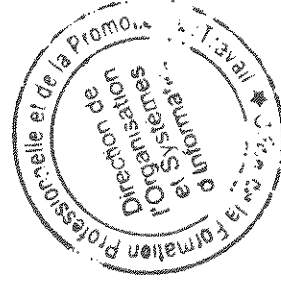
Signature et cachet du concurrent

(1) Le concurrent doit préciser le libellé de la monnaie conformément au RC



2
P
2

ANNEXE

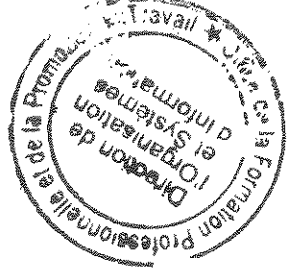


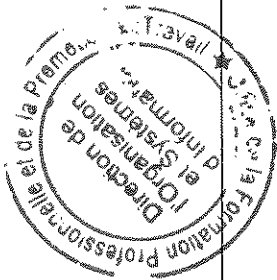
ANNEXE I

CANEVAS

SPECIFICATIONS TECHNIQUES DES SOLUTIONS

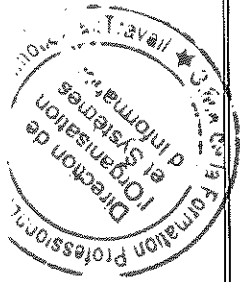
- **N.B :**
- Les soumissionnaires sont invités à remplir la case <<Proposition du soumissionnaire >> en précisant les caractéristiques de la solution proposée.
 - La réponse du soumissionnaire doit être justifiée par des notes explicatives (Comment la solution répond aux exigences techniques), ou des fiches techniques, ou tout autre moyen pouvant justifier la proposition du soumissionnaire
 - Les réponses doivent être claires, exhaustives, parfaitement argumentées.
 - Les réponses ne doivent pas être du type 'A préciser par l'OFPPT'. Les précisions nécessaires doivent faire l'objet de demandes d'éclaircissement à adresser à l'OFPPT selon le délai en vigueur.
 - Les réponses du type 'A paramétrer/A développer en spécifique' doivent être accompagnées de précisions sur les modalités pratiques de mise en œuvre.
 - Les réponses doivent s'appuyer exclusivement sur la solution qui serait déployée à la OFPPT, dans le cadre de l'offre du soumissionnaire. Sont donc à exclure, les réponses relatives à des modules non proposés, à d'autres solutions non associées à l'offre, à des fonctionnalités non disponibles dans la solution proposée à la OFPPT.
 - Toute prestation proposée dans l'offre du soumissionnaire est à sa charge.
 - Tout item ne répondant pas aux spécifications demandées sera déclaré non-conforme.
 - Les colonnes <<Désignations et Fonctions/caractéristiques minimales + Appréciation de l'administration>> ne doivent pas être touchées.





PARTIE N°1 : Évaluation des vulnérabilités & Tests de Pénétration

Désignations et Fonctions / caractéristiques minimales	Proposition du soumissionnaire	Appréciation de l'administration
Item N°1.1 : Evaluation de la sécurité applicative et Test d'intrusion interne et externe		
Cette prestation consiste à faire une évaluation approfondie de la sécurité d'une application spécifique. Il vise à identifier les vulnérabilités potentielles, les failles de sécurité et les risques associés à l'application, ainsi qu'à proposer des mesures correctives pour renforcer sa sécurité. Il s'agit de faire :		
- Tests de Pénétration : Simuler des attaques réelles pour évaluer la résilience de l'application face aux menaces externes.		
- Analyse des Configurations : Examiner les paramètres de sécurité de l'application, y compris les autorisations d'accès, les configurations réseau, etc.		
- Évaluation des Interfaces Utilisateur : Vérifier la sécurité des interfaces utilisateur, notamment les formulaires web, les fonctions d'authentification, etc.		
- Audit des Fonctionnalités de Sécurité : Vérifier que les mécanismes de sécurité de l'application, tels que l'authentification, l'autorisation, la gestion des sessions, et le cloisonnement des profils sont correctement implémentés.		
- Audit des APIs : consiste à faire une évaluation approfondie de la sécurité des interfaces de programmation applicatives (API), en évaluant la sécurité des interactions entre différentes applications et systèmes via ces API et en vérifiant les processus d'authentification, d'autorisation et de chiffrement.		
L'identification des failles se fera sur la base de la dernière version des TOP 10 OWASP.		
Le périmètre à couvrir par cet audit est de 4 applications et 2 APIs.		



OFPPT/DOSI

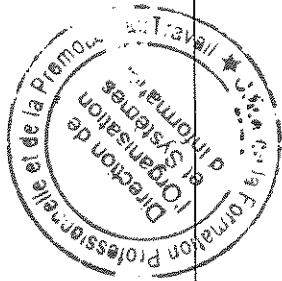
Dossier d'Appel d'Offres

AO. N° 98/2024

Le prestataire est tenu de réaliser des Tests de Pénétration pour évaluer la robustesse du SI de l'OFPPT et sa capacité à préserver ses données. Il s'agit d'une simulation d'un attaquant externe (depuis internet) et d'un attaquant interne (depuis le réseau de l'OFPPT) afin d'identifier le maximum de points de vulnérabilités des infrastructures, applications et services en ligne.			
Les tests doivent être menés selon une méthodologie (à détailler par le prestataire) conformément à l'éthique et aux règles d'art en la matière. Ces tests ne doivent en aucun cas impacter le fonctionnement normal du SI.			
L'exploitation de n'importe quelle vulnérabilité ne doit être menée qu'après l'autorisation explicite de l'OFPPT.			

7
CP

2



OFPPT/DOSI

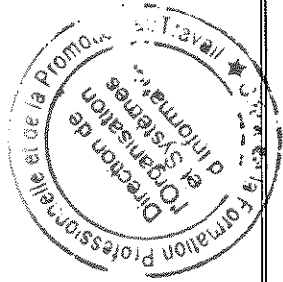
Dossier d'Appel d'Offres

AO. N° 98/2024

PARTIE 2 : SECURITE DES INFRASTRUCTURES :**Mise en place d'une solution SDWAN, NGFW, LAN et WLAN pour le siège et les directions régionales**

Désignations et Fonctions / caractéristiques minimales	Proposition du soumissionnaire	Appréciation de l'administration
Item n°2.1 : FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (Siège)		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
LE NGFW doit être classé leader (1 ^{er} rang de classement) dans les derniers Magic Quadrant de Gartner (ou équivalent) comme : <ul style="list-style-type: none">- « WAN EDGE infrastructure » ou « SD-WAN » (ou équivalent)et- « Network Firewall » ou « Enterprise Firewall » (ou équivalent)		
Fonctionnalités Next-Generation Firewall		
<ul style="list-style-type: none">- Module Firewalling statefull pour le filtrage des flux entrants et sortants ;- Permet le filtrage en fonction de l'adresse source, adresse destination, utilisateur, service, protocole, interface d'entrée, Type de Device...- Permet la création des règles de firewall basé sur l'identité de l'utilisateur en plus d'autres critères : Source/Destination, IP/Sous Réseau, Port Source/Destination- Possibilité de donner un nom à une règle (l'objectif est de faciliter son suivi dans les logs sur des longues périodes) ;- Permet de visualiser et de désactiver les règles implicites.		

2



29

OFPPT/DOSSI

Dossier d'Appel d'Offres

A.O. N° 98/2024

- Permet la gestion des plages d'adresses, des groupes d'IPs (machines, réseaux, plages d'adresses), des groupes d'utilisateurs, groupes de services...		
- Permet la gestion de la bande passante par application.		
- Permet une Policy Based Routing (routage en fonction de tous les critères d'une règle : l'IP source, l'IP destination, l'interface, protocole, l'interface d'entrée, l'application, FQDN) ;		
- Filtrage bloquant par défaut : tout ce qui n'est pas autorisé est interdit.		
- Permet la gestion de la répartition de charge et du backup sur plusieurs liens opérateurs par Source/Destination, Utilisateur ou Protocole/Application : <ul style="list-style-type: none">o Basculement de lien automatiqueo Répartition de chargeo SDWAN		
- Permet le monitoring en temps réel de l'utilisation CPU, Mémoire et disque, les nouvelles sessions, les sessions concurrentes		
- Offre une cartographie des connexions logique et physique des équipements (Firewalls, Points d'Acces) et Endpoints (PC, Serveurs et Device mobiles).		
- Création et gestion de 10 Firewall Virtuels (licence à fournir)		
- Offre le VPN IPsec Site to Site, Client to Site avec ike v1 et v2		
- Offre le SSL VPN en mode WEB (pour offrir la possibilité de se connecter a des services sur un portail WEB sans installation de client VPN) et Full (via un client VPN de même marque)		
- Permet la ggestion des VLANs (Tag VLAN 802.1q) ;		
- Support de l'IPv6 ;		

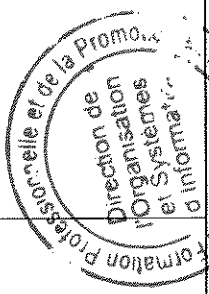
2



OFFPPT/D0.51

Dossier d'Appel d'Offres

AO N° 98/2024

- Support de TLS 1.3 ;			
- Support Syslog ;			
- Permet l'administration via SSH, https			
Fonctionnalités SDWAN :			
- Permet d'utiliser plusieurs types de liens en Actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VPN MPLS, FTTH, 3G/4G Modem USB,			
- Permet de créer des tunnels VPN via Wizard sur le Menu SDWAN pour une facilité de configuration.			
- Permet de créer des SLAs intelligentes pour le basculement et le Load Balancing, ces SLA doivent se baser sur : <ul style="list-style-type: none">o L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précisiono Target SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquetso Etat de lien pour tester le lien avant de basculer afin de ne pas utiliser un lien non fiable			
- Permet la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets.			
- Permet les Méthodes de Load Blancing Suivants : <ul style="list-style-type: none">o IP-Sourceo IP-Source-Destinationo Spillovero Sessionso Volume			

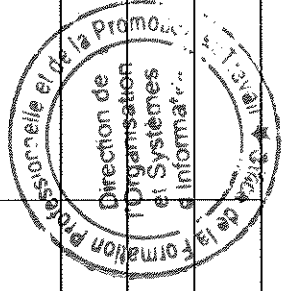


OFPPT/DOSI

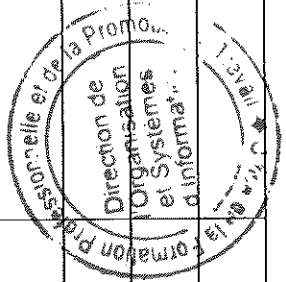
Dossier d'Appel d'Offres

AO. N° 98/2024

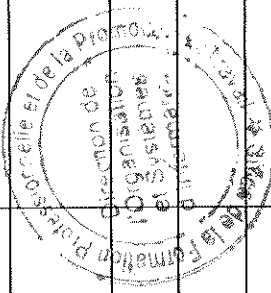
<ul style="list-style-type: none">- Permet d'utiliser des règles de basculement en se basant sur les paramètres suivant suite au mesure SLA :<ul style="list-style-type: none">o Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)o Lowest Costo Maximize Bandwidtho Manuel pour obliger le flux à suivre un lien spécifique		
	<ul style="list-style-type: none">- Les règles SDWAN doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,	
	<ul style="list-style-type: none">- Permet d'associer des politiques QoS pour des flux.	
	<ul style="list-style-type: none">- Permet le control des applications afin d'identifier et reconnaitre les applications dans les flux	
	<ul style="list-style-type: none">- Permet l'administration via SSH, https	
Fonctionnalités Contrôleur WIFI		
<ul style="list-style-type: none">- La prise en charge les dernières normes Wi-Fi Alliance telles que Wi-Fi 6 (802.11ax) et 802.11ad, ainsi que les protocoles de sécurité WPA3.		
<ul style="list-style-type: none">- DNS et SMTP ;		
<ul style="list-style-type: none">- DHCP ;		
<ul style="list-style-type: none">- Support SNMP ;		
<ul style="list-style-type: none">- AAA Security ;		
<ul style="list-style-type: none">- Support de WIPS ;		
<ul style="list-style-type: none">- Support de serveur RADIUS ;		



- Authentification 802.1x, MAC et WEB (portal captif) ;		
- Standards wifi IEEE 802.11ax ;		
- Sécurité : AES/WPA2/WPA3 entreprise ;		
- Filtrage par MAC		
- IGMP Snooping		
- DHCP snooping		
- Phishing SSID		
- Gestion des accès invités avec isolation sécurisée des ressources internes.		
- Il doit assurer l'itinérance transparente pour les utilisateurs se déplaçant dans différentes zones de couverture de points d'accès.		
- Configuration à distance à travers une interface graphique WEB (Secure WEB GUI) et interface de gestion centralisée;		
- Le contrôleur doit avoir un portail captif afin d'authentifier les utilisateurs,		
- Le contrôleur WIFI doit être automatisable via API		
- La solution doit permettre la gestion des points d'accès objet de ce CPS (au minimum 250 points d'accès pour le siège et 128 points d'accès pour la région		
Fonctionnalités SDN / LAN & WLAN		
- La gestion et l'administration des ressources et équipements réseau LAN et WLAN objet de ce CPS ;		
- Le support de l'intégration avec des plateformes Cloud et écosystème tiers via les API ;		



- D'offrir une cartographie physique et logique des switches, points d'accès, équipements connectés aux switches objet de ce CPSs ;		
- L'administration centralisée LAN et WLAN simplifiée :		
• Tagging des ports de plusieurs switches managés par simple clic ;		
• Supervision centralisée de l'état de santé des switches ;		
• Vue de la topologie physique des switches par code couleur (Ring, Uplink, Agrégation des liens, ...) ;		
• Vue du consommation POE au niveau de chaque port et chaque switch ;		
• Permet la gestion de tous les aspects de maintenance et gestion opérationnelle des switches et des points d'accès : enregistrement, provisionning, upgrade firmware, commande CLI ;		
• Provisionning des SSIDs simplifié et centralisé ;		
• Possibilité d'importer un Plan architecturale du bâtiment et de positionner les points d'accès sur la carte. Cette fonctionnalité permet d'afficher en temps réel l'état, l'emplacement du point d'accès lors de recherches non structurées ;		
• Module d'analyse spectrale permettant de voir les interférences de signal,		
• Module d'analyse applicative : avoir la capacité de lister tout le trafic applicatif des utilisateurs ;		
- La solution doit permettre la gestion des switches objet de ce CPS (au minimum 70 Switchs au niveau du siège et 10 switchs par région)		
Fonctionnalités de contrôle d'accès au réseau NAC:		
- Exigences en termes de profiling :		
- Profiling des devices par adresse MAC, Marque, famille d'équipement, type et système d'exploitation ;		





- Profilage des utilisateurs par groupe ;		
- Exigences en termes d'authentification :		
- Intégration avec LDAP, RADIUS et Microsoft Active Directory ;		
- Support des options d'authentification flexibles comme le 802.1X et MAC Authentication		
- Exigences pour la conformité et la remédiation des Endpoints :		
- Possibilité d'intégrer des TAGS selon des indices de conformité des postes de travail permettant ainsi de mitiger les risques quant aux postes connectés au réseau : Antivirus à Jours, version d'OS, Patch Windows Installé, présence d'une vulnérabilité ou d'un logiciel installé indésirable. Selon l'état de conformité du poste de travail, il lui sera garantis un niveau d'accès spécifique, ou éventuellement lui assigner un VLAN de quarantaine pour le temps nécessaire à la remédiation		
Abonnements des modules de protection		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
Module IPS (prévention des intrusions) (à fournir) pour se protéger contre les menaces réseau existantes et émergentes. Ce module IPS doit avoir deux mécanismes de Détection par signatures et par anomalies ; <ul style="list-style-type: none"> - Capable de faire des analyses comportementales de tout type de trafic ; - Possibilité de créer des signatures personnalisées ; - Mise à jour automatique des signatures IPS ; - Création et affectation des politiques IPS par type de zone ou interface ; - Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, d'envoyer une alarme, d'envoyer un mail, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ; - Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ; 		

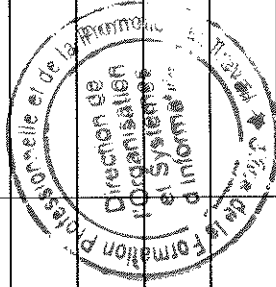


OFFPPT/D05I

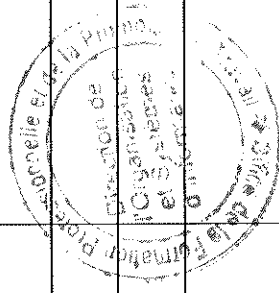
Dossier d'Appel d'Offres

AO N° 98/2024

Module Antivirus / Antimalware (à fournir) pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;		
Module Filtrage URL et de contenu (à fournir) , pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux ;		
Module Control Applicatif (à fournir) , afin d'identifier, reconnaître et contrôler les applications dans les flux		
Module Sandboxing cloud (à fournir) pour la protection contre les logiciels malveillants et les attaques zéro days ;		
Support Software de 5 ans : 24*7		
NB la solution doit supporter le Sandboxing on Premises (local)		
<u>Equipement(s) Siège :</u>		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
- Appliances Rackable 19 pousse avec alimentation redondante échangeable à chaud		
- Un débit Firewall de 130 Gbps minimum ;		
- Un débit IPS Mix de 14 Gbps minimum ;		
- Un débit NGFW (FW+IPS+Control Applicatif) de 11 Gbps minimum ;		
- Un débit Threat Protection (FW+Antivirus+IPS+Contrôle Applicatif) de 10 Gbps minimum ;		
- Un débit Inspection SSL de 9 Gbps minimum		
- Un débit VPN IPsec de 50 Gbps minimum		
- Un débit VPN SSL de 4 Gbps minimum		
- Support de 500 000 nouvelles connexions TCP par seconde minimum ;		



- Support de 8 millions de connexions TCP simultanées ;		
- Support de la haute disponibilité en mode Actif/Passif en mode Actif/Actif Clustering;		
- Doté au minimum de 16 ports réseaux 1GbE RJ45		
- Doté au minimum de 8 ports réseaux 1GbE SFP ;		
- Doté au minimum de 4 ports réseaux 10GbE SFP+		
- Doté au minimum de 4 ports réseaux 25GE/10GE SFP28,		
- 1 port pour le HA		
- 1 ports 1Gbe RJ45 pour le management		
- 1 port console pour le management		
- Peut gérer jusqu'à 2 000 tunnels VPN IPSEC Site-to-Site et de 50 000 tunnels VPN IPSEC Client-to-Site ;		
- 2 disques SSD (Solid State Drive) d'une capacité minimale de 240 Go en RAID1		
- Licence pour création et gestion de 10 Firewall Virtuels		
- Licences à fournir : IPS, Antivirus, Contrôle Applicatif, Filtrage URL, et Sandbox Cloud, pour une période de 5 ans		
- Support Hardware de 5 ans : 24*7		
NB : Tous les ports doivent être activés (avec licence si nécessaire) et livrés avec connecteur		
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support.		



Item n°2.2 : FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (régions et annexes)

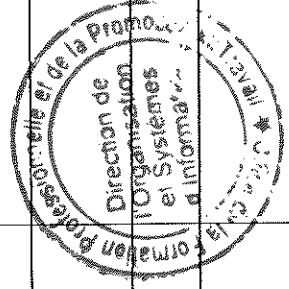
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée

LE NGFW doit être classé **leader** (1^{er} rang de classement) **dans les derniers Magic Quadrant de Gartner** (ou équivalent) comme :

- « WAN EDGE infrastructure » ou « SD-WAN » (ou équivalent)
- et
- « Network Firewall » ou « Enterprise Firewall » (ou équivalent)

Fonctionnalités Next-Generation Firewall

- Module Firewalling statefull pour le filtrage des flux entrants et sortants ;
- Permet le filtrage en fonction de l'adresse source, adresse destination, utilisateur, service, protocole, interface d'entrée, Type de Device...
- Permet la création des règles de firewall basé sur l'identité de l'utilisateur en plus d'autres critères : Source/Destination, IP/Sous Réseau, Port Source/Destination
- Possibilité de donner un nom à une règle (l'objectif est de faciliter son suivi dans les logs sur des longues périodes) ;
- Permet de visualiser et de désactiver les règles implicites.
- Permet la gestion des plages d'adresses, des groupes d'IPs (machines, réseaux, plages d'adresses), des groupes d'utilisateurs, groupes de services...
- Permet la gestion de la bande passante par application.
- Permet une Policy Based Routing (routage en fonction de tous les critères d'une règle : l'IP source, l'IP destination, l'interface, protocole, l'interface d'entrée, l'application, FQDN) ;



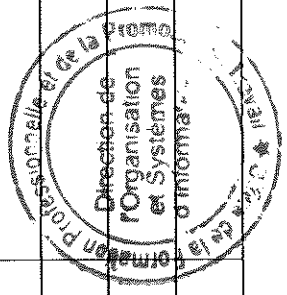


20

Dossier d'Appel d'Offres

AO. N° 98/2024

- Filtrage bloquant par défaut : tout ce qui n'est pas autorisé est interdit.		
- Permet la gestion de la répartition de charge et du backup sur plusieurs liens opérateurs par Source/Destination, Utilisateur ou Protocole/Application : <ul style="list-style-type: none">o Basculement de lien automatiqueo Répartition de chargeo SDWAN		
- Permet le monitoring en temps réel de l'utilisation CPU, Mémoire et disque, les nouvelles sessions, les sessions concurrentes		
- Offre une cartographie des connexions logique et physique des équipements (Firewalls, Points d'Acces) et Endpoints (PC, Serveurs et Device mobiles).		
- Création et gestion de 10 Firewall Virtuels (licence à fournir)		
- Offre le VPN IPsec Site to Site, Client to Site avec ike v1 et v2		
- Offre le SSL VPN en mode WEB (pour offrir la possibilité de se connecter a des services sur un portail WEB sans installation de client VPN) et Full (via un client VPN de même marque)		
- Permet la ggestion des VLANs (Tag VLAN 802.1q) ;		
- Support de l'IPv6 ;		
- Support de TLS 1.3 ;		
- Support Syslog ;		
- Permet l'administration via SSH, https		
Fonctionnalités SDWAN :		





Dossier d'Appel d'Offres

AO. N° 98/2024

OFPPT/DOSI

- Permet d'utiliser plusieurs types de liens en Actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VPN MPLS, FTTH, 3G/4G Modem USB,		
- Permet de créer des tunnels VPN via Wizard sur le Menu SDWAN pour une facilité de configuration.		
- Permet de créer des SLAs intelligentes pour le basculement et le Load Balancing, ces SLA doivent se baser sur : <ul style="list-style-type: none">o L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précisiono Target SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquetso Etat de lien pour tester le lien avant de basculer afin de ne pas utiliser un lien non fiable		
- Permet la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets.		
- Permet les Méthodes de Load Blancing Suivants : <ul style="list-style-type: none">o IP-Sourceo IP-Source-Destinationo Spillovero Sessionso Volume		
- Permet d'utiliser des règles de basculement en se basant sur les paramètres suivant suite au mesure SLA : <ul style="list-style-type: none">o Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)o Lowest Costo Maximize Bandwidtho Manuel pour obliger le flux à suivre un lien spécifique		

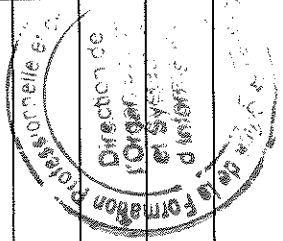
2

209
OFPPT/D051

Dossier d'Appel d'Offres

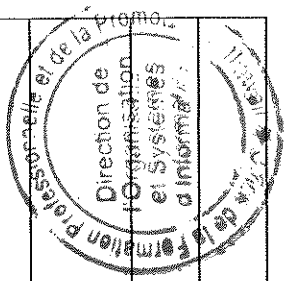
AO N° 98/2024

- Les règles SDWAN doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,		
- Permet d'associer des politiques QoS pour des flux.		
- Permet le control des applications afin d'identifier et reconnaitre les applications dans les flux		
- Permet l'administration via SSH, https		
Fonctionnalités Contrôleur WIFI		
- La prise en charge les dernières normes Wi-Fi Alliance telles que Wi-Fi 6 (802.11ax) et 802.11ad, ainsi que les protocoles de sécurité WPA3.		
- DNS et SMTP ;		
- DHCP ;		
- Support SNMP ;		
- AAA Security ;		
- Support de WIPS ;		
- Support de serveur RADIUS ;		
- Authentification 802.1x, MAC et WEB (portal captif) ;		
- Standards wifi IEEE 802.11ax ;		
- Sécurité : AES/WPA2/WPA3 entreprise ;		
- Filtrage par MAC		





- IGMP Snooping			
- DHCP snooping			
- Phishing SSID			
- Gestion des accès invités avec isolation sécurisée des ressources internes.			
- Il doit assurer l'itinérance transparente pour les utilisateurs se déplaçant dans différentes zones de couverture de points d'accès.			
- Configuration à distance à travers une interface graphique WEB (Secure WEB GUI) et interface de gestion centralisée;			
- Le contrôleur doit avoir un portail captif afin d'authentifier les utilisateurs,			
- Le contrôleur WIFI doit être automatisable via API			
- La solution doit permettre la gestion des points d'accès objet de ce CPS (au minimum 250 points d'accès pour le siège et 128 points d'accès pour la région			
Fonctionnalités SDN / LAN & WLAN			
- La gestion et l'administration des ressources et équipements réseau LAN et WLAN objet de ce CPS ;			
- Le support de l'intégration avec des plateformes Cloud et écosystème tiers via les API ;			
- D'offrir une cartographie physique et logique des switches, points d'accès, équipements connectés aux switches objet de ce CPSs ;			
- L'administration centralisée LAN et WLAN simplifiée : <ul style="list-style-type: none">• Tagging des ports de plusieurs switches managés par simple clic ;			



2

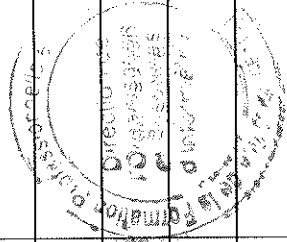


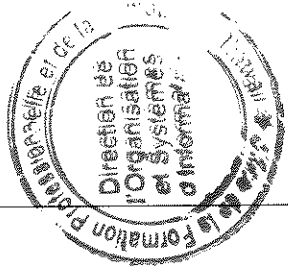
ORPPT/DOSI

Dossier d'Appel d'Offres

AO, N° 98/2024

<ul style="list-style-type: none">Supervision centralisée de l'état de santé des switches ;		
<ul style="list-style-type: none">Vue de la topologie physique des switches par code couleur (Ring, Uplink, Agrégation des liens, ...) ;		
<ul style="list-style-type: none">Vue du consommation POE au niveau de chaque port et chaque switch ;		
<ul style="list-style-type: none">Permet la gestion de tous les aspects de maintenance et gestion opérationnelle des switches et des points d'accès : enregistrement, provisionning, upgrade firmware, commande CLI ;		
<ul style="list-style-type: none">Provisionning des SSIDs simplifié et centralisé ;		
<ul style="list-style-type: none">Possibilité d'importer un Plan architecturale du bâtiment et de positionner les points d'accès sur la carte. Cette fonctionnalité permet d'afficher en temps réel l'état, l'emplacement du point d'accès lors de recherches non structurées ;		
<ul style="list-style-type: none">Module d'analyse spectrale permettant de voir les interférences de signal,		
<ul style="list-style-type: none">Module d'analyse applicative : avoir la capacité de lister tout le trafic applicatif des utilisateurs ;		
<ul style="list-style-type: none">La solution doit permettre la gestion des switches objet de ce CPS (au minimum 70 Switchs au niveau du siège et 10 switchs par région)		
Fonctionnalités de contrôle d'accès au réseau NAC:		
<ul style="list-style-type: none">Exigences en termes de profiling :		
<ul style="list-style-type: none">Profiling des devices par adresse MAC, Marque, famille d'équipement, type et système d'exploitation ;		
<ul style="list-style-type: none">Profiling des utilisateurs par groupe ;		
<ul style="list-style-type: none">Exigences en termes d'authentification :		
<ul style="list-style-type: none">Intégration avec LDAP, RADIUS et Microsoft Active Directory ;		



-	Support des options d'authentification flexibles comme le 802.1X et MAC Authentication		
-	Exigences pour la conformité et la remédiation des Endpoints :		
-	Possibilité d'intégrer des TAGS selon des indices de conformité des postes de travail permettant ainsi de mitiger les risques quant aux postes connectés au réseau : Antivirus à Jours, version d'OS, Patch Windows Installé, présence d'une vulnérabilité ou d'un logiciel installé indésirable. Selon l'état de conformité du poste de travail, il lui sera garantis un niveau d'accès spécifique, ou éventuellement lui assigner un VLAN de quarantaine pour le temps nécessaire à la remédiation		
Abonnements des modules de protection			
	Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
	Module IPS (prévention des intrusions) (à fournir) pour se protéger contre les menaces réseau existantes et émergentes. Ce module IPS doit avoir deux mécanismes de Détection par signatures et par anomalies ;		
-	Capable de faire des analyses comportementales de tout type de trafic ;		
-	Possibilité de créer des signatures personnalisées ;		
-	Mise à jour automatique des signatures IPS ;		
-	Création et affectation des politiques IPS par type de zone ou interface ;		
-	Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, d'envoyer une alarme, d'envoyer un mail, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ;		
-	Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;		
	Module Antivirus / Antimalware (à fournir) pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;		
	Module Filtrage URL et de contenu (à fournir) , pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux ;		
	Module Control Applicatif (à fournir) , afin d'identifier, reconnaître et contrôler les applications dans les flux		



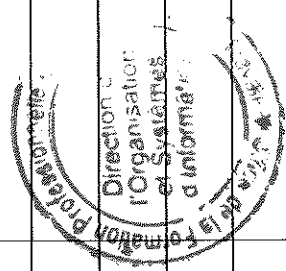
29

OFPPT/D.O.S.I

Dossier d'Appel d'Offres

A.O. N° 98/2024

Module Sandboxing cloud (à fournir) pour la protection contre les logiciels malveillants et les attaques zéro days ;		
Support Software de 5 ans : 24*7		
NB la solution doit supporter le Sandboxing on Premises (local)		
<u>Equipement(s) Siège :</u>		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
Caractéristiques minimales sont :		
- Appliance Rackable 19 pouce avec alimentation redondante ;		
- Un débit Firewall de 39 Gbps minimum ;		
- Un débit IPS Mix de 5 Gbps minimum ;		
- Un débit NGFW (FW+IPS+Control Applicatif) de 3 Gbps minimum ;		
- Un débit Threat Protection (FW+Antivirus+IPS+Contrôle Applicatif) de 2.8 Gbps minimum;		
- Un débit Inspection SSL de 3 Gbps minimum		
- Un débit VPN IPsec de 30 Gbps minimum		
- Un débit VPN SSL de 1.5 Gbps minimum		
- Support de 140 000 nouvelles connexions TCP par seconde minimum ;		
- Support de 3 millions de connexions TCP simultanées ;		
- Doté au minimum de 16 ports réseaux 1GbE RJ45;		



2

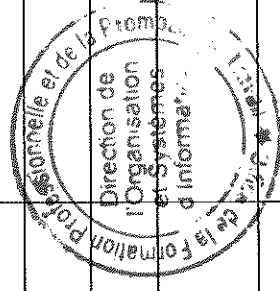


OFPPT/D05I

Dossier d'Appel d'Offres

AO N° 98/2024

- Doté au minimum de 8 ports réseaux 1GbE SFP ;		
- Doté au minimum de 4 ports réseaux 10GbE SFP+		
- 1 ports 1Gbe RJ45 pour le management		
- 1 port console pour le management		
- Peut gérer jusqu'à 2 000 tunnels VPN IPSEC Site-to-Site et de 16 000 tunnels VPN IPSEC Client-to-Site ;		
- Licence pour création et gestion de 5 Firewall Virtuels		
- Licences à fournir : IPS, Antivirus, Contrôle Applicatif, Filtrage URL, et Sandbox Cloud, pour une période de 5 ans.		
- Support Hardware de 5 ans : 24*7		
NB : Tous les ports doivent être activés (avec licence si nécessaire) et livrés avec connecteur		
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support		
Item n°2.3 : Switch fédérateur		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
Les Switch fédérateurs doivent être de même marque que l'item n°2.1 de la partie 2 objet de ce CPS et doivent avoir les caractéristiques minimales suivantes :		
- L'éditeur doit être classé leader (1 ^{er} rang de classement) dans les derniers Magic quadrant de Gartner (ou équivalent) comme « Enterprise Wired and Wireless LAN Infrastructure » (ou équivalent)		
- Rackable 19" ;		



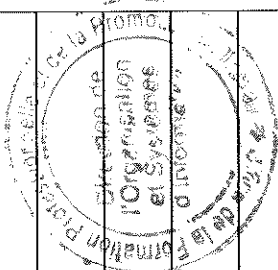


OFPPT/DOSI

Dossier d'Appel d'Offres

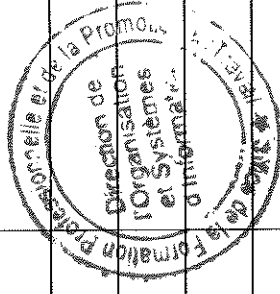
A0. N° 98/2024

-	Minimum 2 ports de 40 G minimum (face avant du switch) extensible à 4 minimum ;		
-	Minimum 2 modules QSFP+ 40Gbe minimum (A prévoir deux câbles fibre optique adéquats ou le câble AOC (actif optique câble) pour une distance de 10 mètres minimum) ;		
-	Minimum 48 ports 10 Gigabit SFP+		
-	Minimum un port de management dédié		
-	Un port de mangement console		
-	Matrice de commutation 1.7 Tpbs minimum ;		
-	Débit de paquet évolutif minimum 1200 Mpps minimum		
-	Routage Statique et Dynamique ;		
-	Agrégation de liens ;		
-	Support la fonction d'empilement ou regroupement des switches via des liens 40 Gbps minimum ;		
-	La pile ou le groupe de 2 switches minimum		
-	Support VLAN par port ;		
-	Support QoS ;		
-	Sécurité et blocage de ports par adresse MAC ;		
-	Support DHCP Snooping ;		
-	Support Inspection ARP Dynamique		
-	Alimentation redondante échangeable à chaud ;		

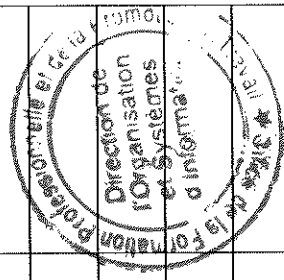


20

- Support SSH ;		
- Support HTTPS ;		
- Support SNMP v3 ;		
- Support Syslog ;		
- Support SNTP ou NTP ;		
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS		
- Être livré avec les licences nécessaires,		
NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.		
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support		
support constructeur de 5 ans pièce et main d'œuvre		
NB : Les Deux Switchs Fédérateurs doivent :		
- Fonctionner de façon redondante et en partage de charge ;		
- Être équipés de liens d'agrégation de 40 Gbps minimum pour la synchronisation et transfert de données,		
- Être livrés avec les câbles et les accessoires nécessaires à leur interconnexion ainsi pour leur pose, raccordement, et mise en service.		
Item n° 2.4 : Switch multi Giga (avec PoE+)		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		



Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes, caméras, point d'accès WIFI...).			
Ils doivent être de même marque que l'item n° 2.1 de la partie 2 objet du présent CPS et conformes aux spécifications techniques minimum suivantes :			
- Rackable 19" ;			
- Minimum 10 ports Multi Giga 1/2.5 min baseT PoE/PoE+			
- Minimum 16 ports 1 Gigabits Base T minimum PoE/PoE+			
- Minimum 4 ports 10 Gigabit SFP+ dédiés (face avant du switch);			
- Minimum un port de management dédié			
- Un port de mangement console			
- Matrice de commutation 162 Gbps minimum ;			
- Débit paquet par seconde de 240 Mpps minimum ;			
- Commutation Niveau 2 minimum			
- Agrégation de liens ;			
- Support la fonction d'empilement ou regroupement des switches via des liens 10 Gbps minimum ;			
- Support VLAN par port ;			
- Support QoS ;			
- Sécurité et blocage de ports par adresse MAC ;			



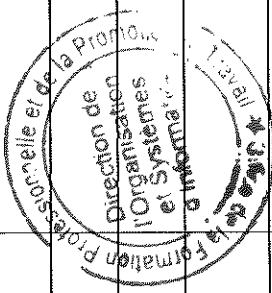


OFFPPT/D05I

Dossier d'Appel d'Offres

AO. N° 98/2024

- Support DHCP Snooping ;		
- Support Inspection ARP Dynamique		
- Support du PoE 802.3af et PoE+ 802.3at (sur les 24 ports);		
- Alimentation redondante ;		
- Support SSH ;		
- Support HTTPS ;		
- Support SNMP v3 ;		
- Support Syslog ;		
- Support SNMP ou NTP ;		
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS		
- Être livré avec les licences nécessaires,		
NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.		
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support		
Garantie de 5 ans pièce et main d'œuvre ;		
Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.		
Item n° 2.5 : Switch 48 ports (avec PoE+)		

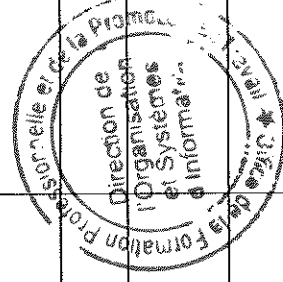


2

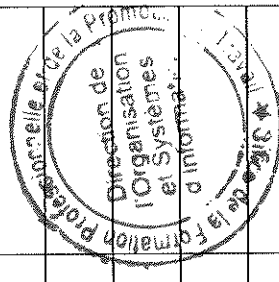


Director
Organization
and Information

- Sécurité et blocage de ports par adresse MAC ;		
- Support DHCP Snooping ;		
- Support Inspection ARP Dynamique		
- Support du PoE 802.3af et PoE+ 802.3at (sur les 24 ports) ;		
- Support SSH ;		
- Support HTTPS ;		
- Support SNMP v3 ;		
- Support Syslog ;		
- Support SNTP ou NTP ;		
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS		
- Être livré avec les licences nécessaires,		
NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.		
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support		
Garantie de 5 ans pièce et main d'œuvre ;		
Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.		
Item n°2.6 : Switch 24 ports (avec PoE+)		



Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée	
Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes, caméras...).	
Ils doivent être de même marque que l'item n° 2.1 de la partie 2 objet du présent CPS et conformes aux spécifications techniques minimum suivantes :	
- Rackable 19" ;	
- minimum 24 ports 10/100/1000 base T PoE/PoE+	
- minimum 4 ports 10 Gigabit SFP+ dédiés (face avant du switch) pour l'Uplink avec les Switch fédérateurs ;	
- Minimum un port de management dédié	
- Un port de mangement console	
- Matrice de commutation 128 Gbps minimum ;	
- Débit paquet par seconde 180 Mpps minimum ;	
- Commutation Niveau 2 minimum	
- Agrégation de liens ;	
- Support la fonction d'empilement ou regroupement des switches via des liens 10 Gbps minimum ;	
- Câble DAC 10 Gbps de 1 m minimum	
- Support VLAN par port ;	
- Support QoS ;	



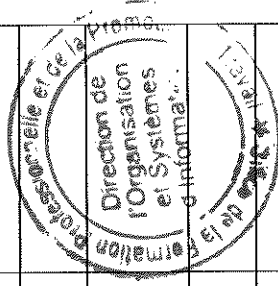


OFPPT/DOSI

Dossier d'Appel d'Offres

AO. N° 98/2024

- Sécurité et blocage de ports par adresse MAC ;		
- Support DHCP Snooping ;		
- Support Inspection ARP Dynamique		
- Support du PoE 802.3af et PoE+ 802.3at (sur les 24 ports) ;		
- Support SSH ;		
- Support HTTPS ;		
- Support SNMP v3 ;		
- Support Syslog ;		
- Support SNMP ou NTP ;		
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS		
- Être livré avec les licences nécessaires,		
NB : Tous les ports demandés doivent être activés (avec licence si nécessaire) et livrés avec connecteur.		
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support		
Garantie de 5 ans pièce et main d'œuvre ;		
Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.		
Item n°2.7 : Point d'accès Wifi		



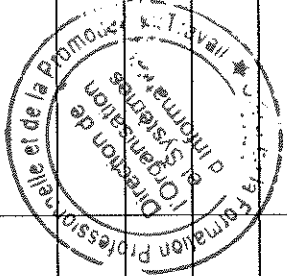


OFPPT/DOSI

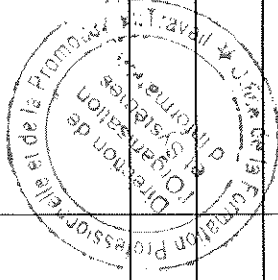
Dossier d'Appel d'Offres

A.O. N° 98/2024

Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée			
Les points d'accès doivent être des points d'accès haut débit 802.11 ax. Ils doivent être de même marque que l'item n° 2.1 de la partie 2 objet du présent CPS.			
Ils doivent répondre aux spécifications minimales suivantes :			
- 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax (OFDMA)			
- Dual Radio 802.11ax ;			
- MU-MIMO 4x4			
- Prise en charge de PoE IEEE 802.3at et 802.3af			
- Authentification 802.1x ;			
- Prise en charge des protocoles avancés de cryptage et d'authentification :			
- AP-TLS, EAP-TTLS et EAP-PEAP			
- WPA2/WPA3			
- Prise en charge de WPS et WIDS Radio Modes			
- Débit doit atteindre jusqu'à 2.5 Gbps maximum ;			
- Minimum 1 port Ethernet 2.5 Gigabit			
- Minimum 1 port Ethernet 1 Gbps			
- Minimum 4 antennes intégrées ;			
- Bluetooth intégré ;			



- Support SNMPv3 ;		
- Manageable centralement depuis la même console de gestion de l'item 2.8 de la partie 2 objet du présent CPS		
- Kit de montage mural		
Garantie et support constructeur de 5 ans pièce et main d'œuvre		
Les Points d'accès doivent être livré avec les câbles et accessoires nécessaires à leur pose, raccordement, fixation et mise en service.		
Les équipements proposés ne doivent pas figurer dans la liste des équipements en fin de commercialisation et doivent bénéficier d'au moins 5 ans de support		
Item n° 2.8 : Solution de management centralisé		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
Le prestataire doit proposer une solution logicielle de gestion et administration centralisée de même éditeur que l'item n° 2.1 de la partie 2 objet du présent CPS, et devant répondre aux spécifications techniques suivantes :		
- Interface unique pour la gestion centralisée des Firewalls, des switches et points d'accès, objet du présent CPS, des différents sites		
- La gestion des configurations		
- La gestion centralisée des politiques de réseau et de sécurité		
- La configuration, le déploiement et la maintenance du SD-WAN.		





OFPPT/D05I

Dossier d'Appel d'Offres

A.O. N° 98/2024

- La création et le provisioning des templates de configuration par site pour la partie sécurité, WAN, LAN et WLAN		
- La gestion des MAJ Firmware		
- La gestion des licences, la distribution centralisée du contenu de sécurité et des signatures		
- La gestion et la supervision centralisée des tunnels VPN et du SDWAN.		
- La gestion et la supervision des performances		
- La gestion centralisée des logs des Firewalls, des switches et points d'accès, objet du présent CPS, des différents sites avec une capacité de traitement de 50 GB de logs par jour minimum		
- La supervision du trafic ainsi que la gestion de la Qualité de service.		
- Automatisez les flux de travail et les configurations pour les pare-feu, les commutateurs et l'infrastructure sans fil		
- Support des API REST, des scripts, des modèles CLI pour l'automatisation et l'orchestration		
- La sauvegarde automatisée de la configuration des appareils		
- Permet de créer des profils et des domaines d'administration différents		
- Support SSL		
- Format Appliance virtuelle en promesse		
- 4 interfaces réseau Giga Ethernet minimum		
- Licence pour gestion des items de la partie 2		
- Souscription de licences pour une durée de 5 ans ;		

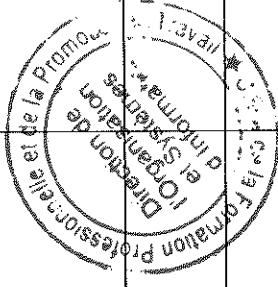


20

Dossier d'Appel d'Offres

AO. N° 98/2024

Item n° 2.9 : Prestation de service : Installation et mise en service (Siège, Annexes Sièges et Directions Régionales)			
Le prestataire doit assurer à sa charge la livraison, l'installation et la mise en service, clé en main, des différents équipements objet de la partie 2 du présent CPS (Firewall, Switchs, contrôleurs, points d'accès WIFI).			
Le prestataire doit livrer tous les accessoires et connectiques nécessaires pour la mise en rack et la mise en réseau des équipements objet de ce CPS ;			
Dans le cadre des travaux d'installation et de mise en service de la solution clé en main, le prestataire doit réaliser, au préalable une étude d'ingénierie (dossier d'étude détaillée de l'architecture cible) et proposer une configuration cible des éléments actifs réseaux en tenant compte des exigences des services réseaux opérationnels actuellement et ce en concertation avec l'équipe DOSI/OFPPT, et proposer également un plan de migration des anciens switchs mis en production vers les nouveaux switchs objet de ce CPS.			
Le prestataire doit se baser sur le plan d'adressage IP, de routage, de découpage VLAN et de gestion de la qualité de service existant avec les adaptations nécessaires.			
Le prestataire doit assurer le tirage de câble de bout en bout (cat 6a minimum) des dites points d'accès, leurs fixations, et leurs mises en service.			
Le prestataire doit assurer pour la solution wifi :			
- De gérer des politiques de sécurité individualisées ou aux groupes d'utilisateurs usant l'accès WIFI ;			
- D'appliquer les politiques relatives aux configurations et aux comportements clients pour interdire l'accès au réseau aux unités utilisateurs qui ne disposent pas des configurations de sécurité adéquate ;			
- D'offrir une sécurité supplémentaire pour l'accès au réseau de l'entreprise par les utilisateurs invités. Il garantit que ces utilisateurs ne pourront pas accéder au réseau sans passer d'abord par le pare-feu ;			
Garantie et maintenance (couvre l'assistance 'sur site ou à distance', l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée de cinq ans avec un délai de prise en charge de 2 heures après déclaration de l'incident et un délai de 4 heures de résolution ou de contournement du problème ;			





2P

OFPPT/DOSI

Dossier d'Appel d'Offres

AO. N° 98/2024

Livrables du projet :		
Le prestataire doit fournir livrables suivants :		
- Un dossier d'ingénierie contenant l'architecture réseau (schéma d'adressage, routage, découpage vlan..);		
- Un guide technique d'administration et d'exploitation des équipements ;		
Transfert de compétences		
Le prestataire doit assurer un transfert de compétence permettant à l'équipe de l'OFPPT d'acquérir les connaissances nécessaires pour assurer l'exploitation des équipements installés objet du présent CPS		

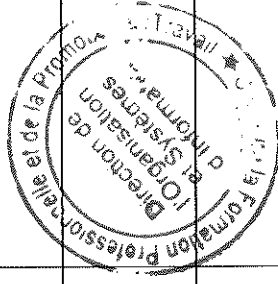


2



PARTIE 3 : SECURITE DES IDENTITES, DES ACCES ET DES PRIVILEGES
Mise en place d'une solution IAM, PAM et une infrastructure PKI

Désignations et Fonctions / caractéristiques minimales	Proposition du soumissionnaire	Appréciation de l'administration
<u>Item n°3.1 : Gestion des identités et des accès (IAM)</u>		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
La solution IAM, proposée doit permettre de centraliser la gestion des identités, garantir l'unicité des identifiants, et automatiser les processus de provisionnement et de dé provisionnement des comptes.		
Le prestataire doit assurer la mise en place d'une solution de gestion des identités et des accès notamment la configuration et le support, la solution doit répondre aux exigences techniques détaillées suivantes.		
Marque et référence à définir		
La solution proposée doit être d'un éditeur classé leader (1er rang de classement) dans les derniers Magic Quadrant de Gartner (ou équivalent) comme « Access Management » ou « Workforce Identity Platform » (ou équivalent)		
- La souscription des licences de la solution proposée est pour une durée de 3 ans pour un nombre minimum de 1000 utilisateurs		
Fonctionnalités		
La solution IAM doit offrir les fonctionnalités suivantes :		
<u>Gestion des identités :</u>		
- La création, la modification et la suppression des comptes utilisateurs		



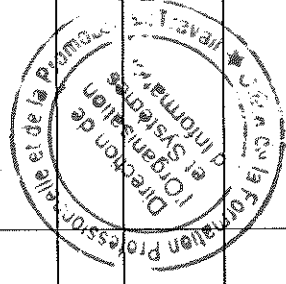


OFPPT/DOSSI

Dossier d'Appel d'Offres

AO. N° 98/2024

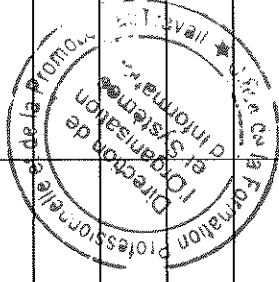
- la gestion des attributs d'identité standards tels que le nom, le prénom, l'adresse e-mail, etc		
- la gestion des attributs d'identité personnalisés et spécifiques à l'OFPPT		
- Stockage sécurisé et cryptage des informations d'identification des utilisateurs, avec des algorithmes avancés de hachage de mot de passe.		
- Application de la politique de mot de passe et exigences de sécurité pour garantir des contrôles d'accès sécurisés.		
- La synchronisation des identités avec Active directory locale (on prem) avec réécriture des changements de mot de passe.		
- Options de réinitialisation de mot de passe en libre-service.		
- Gestion centralisée du cycle de vie des identités pour un provisionnement et un déprovisionnement efficaces des utilisateurs.		
<u>L'authentification :</u>		
Authentification multifacteur (MFA) intégrant deux facteurs ou plus pour une vérification améliorée des utilisateurs.		
Méthodes d'authentification :		
- Mot de passe		
- SMS		
- Clé de sécurité FIDO2		
- Authentification basée sur des certificats		
- Application mobile d'authentification		





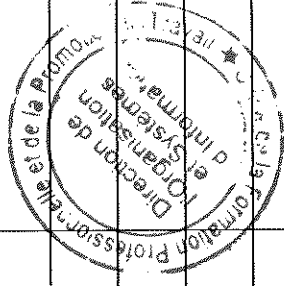
24

- Jetons logiciels OATH		
- Passe d'accès temporaire (TAP)		
- Windows Hello		
Authentification unique (SSO) :		
- Fonctionnalité SSO transparente permettant aux utilisateurs de se connecter une seule fois pour accéder à plusieurs systèmes ou applications sans avoir à saisir à chaque fois leurs identifiants		
- Support des protocoles d'authentification, tels que :		
• Open Authentification Oauth 2.0		
• OpenID Connect OIDC		
• Security Assertion Markup Language SAML		
• Authentification basée sur l'en-tête		
• Authentification Windows intégrée		
• Kerberos		
• LDAP		
• Active directory		
• RADIUS		
Authentification adaptative :		



2

<ul style="list-style-type: none"> - Authentification dynamique basée sur les risques pour ajuster les niveaux de sécurité en fonction des comportements des utilisateurs et de facteurs contextuels (adresse IP, appareil, version du système d'exploitation, ..). 			
<ul style="list-style-type: none"> - Analyse des menaces en temps réel pour détecter et répondre aux tentatives de connexion anormales et aux risques de sécurité potentiels. 			
<ul style="list-style-type: none"> - Capacités d'authentification continue pour la vérification continue des utilisateurs et la surveillance des sessions. 			
<u>Gestion des accès et des autorisations</u>			
<ul style="list-style-type: none"> - Mise en œuvre de contrôles d'accès et de privilèges basés sur les rôles pour appliquer les principes du moindre privilège. 			
<ul style="list-style-type: none"> - Gestion des groupes et des rôles 			
<ul style="list-style-type: none"> - Gestion des privilèges et des accès basés sur les rôles (RBAC) 			
<ul style="list-style-type: none"> - Attribution automatique d'utilisateurs/groupes auprès des applications cloud/locales 			
<ul style="list-style-type: none"> - Révisions d'accès 			
Gestion des cycles de vie des identités et des autorisations			
Analyse du comportement des utilisateurs pour la surveillance de l'activité des utilisateurs :			
<ul style="list-style-type: none"> - Surveillance et évaluation des interactions des utilisateurs avec les systèmes d'authentification pour l'identification des anomalies. 			
<ul style="list-style-type: none"> - Utilisation d'algorithmes d'apprentissage automatique pour la reconnaissance de formes et la détection d'anomalies. 			





OFPPT/DOSI

Dossier d'Appel d'Offres

AO. N° 98/2024

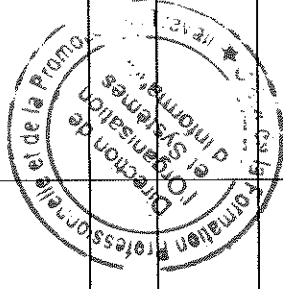
- Alertes et notifications en temps réel en cas de comportement suspect pour contrer de manière proactive les menaces de sécurité potentielles.

Intégration et évolutivité :

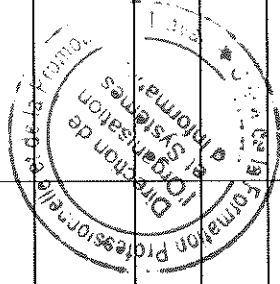
- Intégration transparente avec les applications de l'OFPPT, les services cloud et les systèmes existants pour une couverture complète.
- Évolutivité pour s'adapter à la croissance future et aux exigences d'authentification évolutives.
- Interopérabilité avec des solutions de sécurité tierces et des outils de gestion des terminaux pour des contrôles de sécurité améliorés
- La solution doit supporter en plus de la gestion des identités des collaborateurs de l'OFPPT, la gestion des identités des autres catégories comme partenaire, stagiaire, prestataire, infogérant

Conformité Audit et Journalisation :

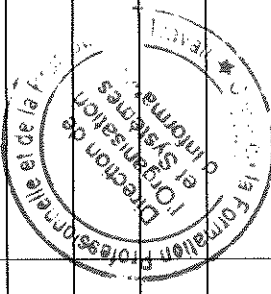
- Fonctionnalités de journalisation et de reporting des pistes d'audit pour les audits de conformité et les exigences réglementaires.
- Évaluations de sécurité régulières et examen des mécanismes d'authentification pour maintenir un environnement sécurisé.
- Vérifications de conformité automatisées et mécanismes d'application des politiques pour maintenir un environnement d'authentification sécurisé.
- Génération de journaux d'audit détaillés, de rapports de conformité et de politiques de contrôle d'accès pour les audits réglementaires
- Rapport sur l'état des accès

Item n°3.2 : Gestion des accès privilégiés (PAM)

Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée			
La solution proposée doit être d'un éditeur classé leader (1er rang de classement) dans les derniers Magic Quadrant de Gartner (ou équivalent) comme « Privileged Access Management » ou « Privileged Identity Management » (ou équivalent)			
<ul style="list-style-type: none"> - La souscription de licences pour une durée de 3 ans couvrant : <ul style="list-style-type: none"> o 20 administrateurs o Chaque administrateur doit pouvoir gérer 500 actifs minimum se trouvant sur 11 sites - La solution doit permettre de : - Protéger les administrateurs (administrateur Système, Administrateur réseau, Administrateur base de données, administrateur sécurité...) administrant les actifs avec une traçabilité de leur session. - Le nombre de comptes utilisateurs (compte root, administrateur local, compte du domaine, comptes de service,) pouvant être gérés par la solution doit être illimité. 			
Fonctionnalités du PAM :			
<u>Découverte des comptes privilégiés</u>			
<ul style="list-style-type: none"> - Découverte des comptes locaux, des comptes de domaine, des clés SSH - Découverte des services Windows et des tâches planifiées Windows qui utilisent les comptes privilégiés 			
<u>Gestion des comptes et des sessions à privilèges</u>			
<ul style="list-style-type: none"> - Stockage sécurisé des informations d'identification avec accès restreint basé sur les rôles. - Sauvegarde et protection des informations d'identification des comptes privilégiés dans un coffre-fort à savoir : <ul style="list-style-type: none"> • Les mots de passe 			



• clés SSH		
• Tokens		
• secrets d'accès à des API « clés API »		
- Le Coffre-fort doit être sécurisé, chiffré et hautement disponible		
- Rotation des mots de passe et des clés SSH		
o Selon une périodicité paramétrable		
o Après chaque connexion		
o Selon des politiques de mot de passe :		
▪ Longueur du mot de passe,		
▪ Nombre de caractère en minuscule/Majuscule, nombre de caractère spécial et nombre de chiffre,		
▪ Durée d'expiration		
▪ À détailler les autres possibilités		
- Rotation et gestion automatisées des identifiants pour les comptes privilégiés afin de réduire le risque de vol d'identifiants.		
- Etablissement automatique des sessions privilégiées via :		
o RDP,		
o SSH,		
o HTTP/HTTPS		



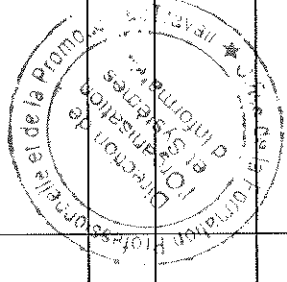


OFPPT/D05I

Dossier d'Appel d'Offres

AO. N° 98/2024

o MS SQL		
- Établissement de session privilégiée avec injection d'informations d'identification sans dévoiler les mots de passe cibles à l'utilisateur.		
- La consultation des sessions établies (qui est connecté à quoi et depuis quand)		
- Afficher des consignes qui doivent être explicitement acceptées par l'administrateur avant tout accès		
- Surveillance en temps réel des sessions		
- Surveillance en temps réel des sessions pour détecter les comportements anormaux et les menaces potentielles pour la sécurité, avec la possibilité de visualiser la session en temps réel avec la possibilité de sa résiliation immédiate		
- Surveiller les actions effectuées par les utilisateurs privilégiés		
- La solution doit permettre de déconnecter automatiquement un utilisateur si une commande ou un texte suspect apparaissent sur la ligne de commande ou à l'écran.		
Alertes et notifications pour les activités inhabituelles ou les violations de politique lors d'un accès privilégié		
- Enregistrement et audit des sessions des utilisateurs privilégiés (commandes et actions exécutées)		
- Enregistrement de session complet des activités des utilisateurs privilégiés pour les pistes d'audit		
- L'ensemble des activités de la session est enregistré, indexé et stocké dans des pistes d'audit inviolables à savoir :		
o fenêtre active		
o Frappes, Saisie de touches du clavier		
o Clic de souris,		



2



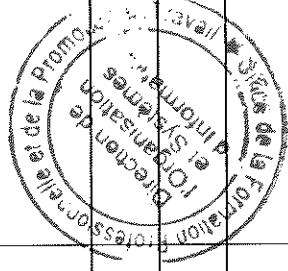
20

OFPPT/DOSI

Dossier d'Appel d'Offres

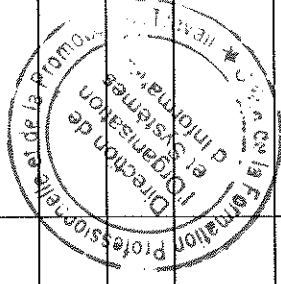
A0, N° 98/2024

o Changement de contenu		
o Échange de fichiers via le presse-papiers et les lecteurs locaux redirigés		
o Transfert de fichiers utilisant les différents protocoles, notamment sur les protocoles RDP et SSH.		
- Enregistrement au format vidéo des sessions établies		
- Transcription de l'enregistrement vidéo montrant toutes les métadonnées de session		
- Consultation des enregistrements avec possibilité :		
o De sélectionner directement les événements relatifs aux cliques de la souris ou de la saisie de certaines touches du clavier, ou l'ouverture de certaines fenêtres.		
o D'accélérer les vidéos		
o De prendre des captures de certaines manipulations effectuées lors d'une session.		
- Les enregistrements doivent être chiffrés et horodatés.		
- Recherche dans les enregistrements		
- La solution devrait fournir la fonction d'indexation et de recherche des métadonnées de session enregistrées qui permettent de détecter :		
o Le contenu de l'affichage complet de l'écran		
o Les commandes exécutées		
o Les titres des fenêtres		
- Recherche en fonction de commandes, noms d'utilisateurs, date et heure spécifiques exécutées dans une session privilégiée afin de déterminer qui les a exécutées et ce qui s'est passé avant et après		

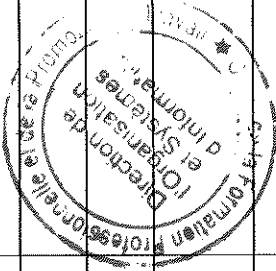


2

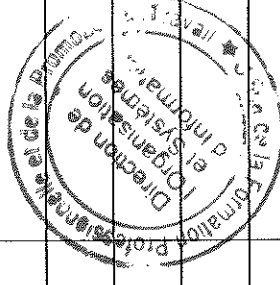
- Recherche rapide (ex : par mots clés, commandes,) des données indexées sur les protocoles en mode texte, en mode graphique.		
- Rechercher certains événements dans des sessions avec possibilité de lire l'enregistrement à partir du moment précis où le critère de recherche apparaît.		
- La solution doit permettre la gestion du processus de bout en bout de demande d'accès faites par des utilisateurs privilégiés avec des workflows d'approbation.		
Demands d'élévation de privilèges et d'accès :		
- Demandes d'accès contrôlées et flux de travail d'approbation pour les privilèges temporairement élevés.		
- Fourniture d'accès juste à temps avec autorisations limitées dans le temps et révocation automatique.		
- Processus d'authentification et de validation en plusieurs étapes pour les demandes d'élévation de privilèges.		
- de validation simple et convivial permettant aux enseignants et aux instructeurs d'accorder aux étudiants l'accès aux machines Labs		
Administration et gestion de la solution PAM :		
La solution doit fournir une console d'administration web intuitive et sécurisée en HTTPS		
- Prise en charge de l'administration basée sur les rôles (administrateur, utilisateur, auditeur)		
- Inventaire des utilisateurs, des ressources et des droits		
- La journalisation doit horodater les connexions, les tentatives de connexions, les enregistrements des sessions pour une visualisation ultérieure		
- Traçabilité de chaque action (accès aux informations d'identification, actions privilégiées, accès aux enregistrements et données associées (utilisateur, date et heure, type d'action, etc.) de façon exhaustive		



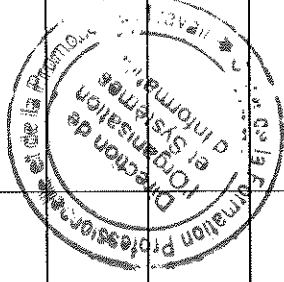
-	Outil de filtrage et recherche multicritère dans les journaux pour faciliter l'identification des incidents de sécurité.		
Rapports d'audit et de conformité :			
-	La solution proposée doit permettre :		
-	de créer manuellement ou automatiquement des rapports selon une fréquence journalière, hebdomadaire ou mensuelle.		
-	Envoyer les rapports par email.		
-	Génération de rapports de conformité - Reporting d'audit et de conformité :		
-	Création de rapports d'audit détaillés sur les activités d'accès privilégié pour les audits de conformité.		
-	Options de reporting personnalisables pour suivre les violations des politiques, les avis d'accès et l'activité des utilisateurs.		
-	Journaux d'audit et rapports sur l'utilisation des informations d'identification et les modifications apportées à des fins de conformité.		
-	La solution doit être capable de générer des alertes et de notifier automatiquement l'administrateur par message électronique, en cas d'événement spécifique :		
-	La solution doit être capable de synchroniser son horloge avec une source de temps NTP		
-	Permettre la remontée des événements vers une solution SIEM en syslog		
-	La solution doit fournir une fonctionnalité break glass qui permet de récupérer les mots de passe administrateurs locaux pour l'accès aux actifs en cas d'indisponibilité du PAM.		
Intégration et évolutivité :			



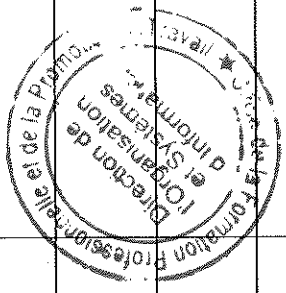
- Intégration transparente avec les solutions et outils de sécurité existants de gestion des identités et des accès (IAM).		
- Évolutivité pour s'adapter à une infrastructure croissante et à un nombre croissant d'utilisateurs privilégiés.		
- Prise en charge des intégrations API et de l'interopérabilité avec des applications tierces pour des fonctionnalités étendues.		
Les actifs à protéger par le PAM :		
- Active Directory		
- Windows (comptes administrateurs locaux)		
- Unix / Linux (Any Distribution)		
- Hyperviseurs (Hyper-V, VMware, AHV, KVM)		
- Out-of-Band Management Systems (Lenovo IMM , iDrac, HP iLO,)		
- Equipement réseau (ALCATEL CISCO HP)		
- Equipement sécurité (PALO ALTO, F5 BIG IP,)		
- Database (MySQL, MS SQL, SAP HANA, PostgreSQL)		
- Application web		
- Les actifs issus du présent CPS		
Item n° 3.3 : Infrastructure à clé publique (PKI)		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		



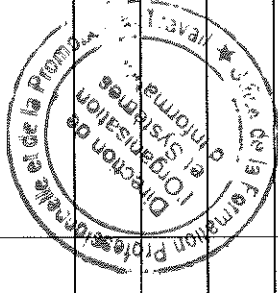
Le prestataire doit assurer la fourniture, la configuration et du support d'une solution PKI complète qui répond aux exigences techniques minimales détaillées suivantes :	
Marque et Modèle :	
La solution proposée doit être une solution reconnue	
- La souscription des licences proposée pour une durée de 3 ans	
- La solution doit offrir :	
- Un nombre de certificats : par user et par device :14 000	
- Type de certificat :	
- SSL/TLS pour les serveurs pour l'authentification serveurs Web, les chiffrements des connexions au serveurs base de données	
- Certificat client pour l'authentification (identité numérique), cryptage/signature des email, documents, pour remote network access, aussi chiffrement des données sur les postes nomades, supports amovibles	
Objectifs de la solution	
- Mettre en place une infrastructure robuste et sécurisée pour la gestion des certificats numériques.	
- Assurer la confidentialité, l'intégrité et l'authenticité des données échangées au sein de l'entreprise.	
- Faciliter l'émission, la révocation et le renouvellement des certificats numériques.	
- Permettre l'intégration avec les systèmes existants, tels que les annuaires LDAP et les applications web.	
Les fonctionnalités minimales de la solution :	
- Génération de certificats numériques X.509.	



- Gestion des demandes de certificats (CSR).		
- Révocation des certificats compromis ou expirés.		
- Renouvellement automatique des certificats.		
- Intégration avec les annuaires LDAP pour l'authentification des utilisateurs.		
- Gestion des politiques de sécurité et des profils de certificats.		
- Audit et journalisation des opérations effectuées.		
- Compatible avec divers systèmes d'exploitation de type Unix, y compris Linux et FreeBSD.		
- Bibliothèques cryptographiques pour les opérations cryptographiques.		
- Configuration des Politiques : Les administrateurs peuvent définir des politiques pour l'émission et la gestion des certificats en fonction des exigences organisationnelles.		
- Application des Politiques : application des politiques pour garantir la conformité aux normes de sécurité et aux exigences réglementaires.		
- Scalabilité Horizontale : peut être déployé dans une configuration en grappe pour s'adapter à des charges accrues.		
- Haute Disponibilité : Des mécanismes de redondance et de basculement sont pris en charge pour assurer une haute disponibilité des services de certificats.		
Déploiement et intégration :		
L'OFPPT dispose de plusieurs systèmes existants, le prestataire doit assurer que le serveur PLI devra être capable de s'intégrer avec ces systèmes, notamment :		
- Les annuaires LDAP pour l'authentification des utilisateurs.		



<ul style="list-style-type: none"> - Les applications web nécessitant des certificats pour l'authentification SSL/TLS. 	<p>Le déploiement du serveur PKI devra être réalisé de manière planifiée et documentée. Des procédures de sauvegarde régulières devront être mises en place pour assurer la disponibilité et l'intégrité des données. Des mises à jour de sécurité devront être appliquées régulièrement pour corriger les vulnérabilités identifiées.</p>	<p>La solution proposée doit assurer au minimum les éléments d'intégration suivants :</p>	<ul style="list-style-type: none"> - Exposer une API RESTful pour un accès programmable aux fonctionnalités de gestion de certificats. 	<ul style="list-style-type: none"> - Des bibliothèques d'intégration et des SDK sont disponibles pour les langages de programmation populaires (par exemple Python, Java) pour faciliter l'intégration système. 	<p>Le prestataire doit impérativement assurer un déploiement de la solution proposée au sein de l'infrastructure de l'établissement.</p>	<ul style="list-style-type: none"> - Les mesures de sécurité suivantes devront être mises en place par le prestataire : 	<ul style="list-style-type: none"> - Utilisation d'algorithmes cryptographiques robustes pour la génération et la gestion des clés. 	<ul style="list-style-type: none"> - Protection des clés privées avec des mécanismes de stockage sécurisés. 	<ul style="list-style-type: none"> - Contrôles d'accès basés sur les rôles pour limiter l'accès aux fonctionnalités sensibles. 	<ul style="list-style-type: none"> - Intégration avec des mécanismes d'authentification forte, tels que les certificats client ou les jetons d'authentification. 	<ul style="list-style-type: none"> - Utilisation des mécanismes de stockage sécurisé des clés pour protéger les clés privées contre 	<p>Support et Formation</p>	<p>Une formation doit être dispensée aux administrateurs chargés de la gestion du serveur PKI avec un support technique disponible après la mise en place de la solution pour la résolution des problèmes rencontrés lors de l'utilisation du serveur PKI.</p>
---	--	---	---	--	--	--	--	--	---	---	--	------------------------------------	--



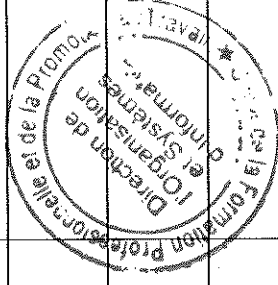


20

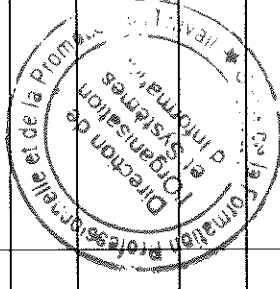
Dossier d'Appel d'Offres

AO. N° 98/2024

Le prestataire doit assurer une formation des administrateurs chargés de la gestion de l'infrastructure PKI (5 personnes minimum)		
Item n°3.4 : Industrialisation du déploiement des postes de travail		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
Le prestataire doit mettre en place une solution de déploiement des postes de travail sous Windows, qui consiste à automatiser les tâches quotidiennes répétitives, libérant ainsi l'équipe informatique. Il s'agit de :		
<ul style="list-style-type: none">- Mettre en place les outils nécessaires pour le déploiement automatisé des postes connecté au réseau de l'OFPPT et les postes de travail hors réseau- La "masterisation" des postes de travail : création d'une image système standardisée et préconfigurée en personnalisant les configurations et les logiciels selon les besoins de chaque groupe d'utilisateurs- Durcissement de l'image master « hardening », il s'agit de renforcer la sécurité en appliquant diverses mesures pour réduire les risques d'exploitation par des logiciels malveillants ou des attaquants.- Automatiser le processus de déploiement des images en utilisant des scripts, des tâches planifiées et des outils de déploiement.- Maintenance et mise à jour des images ;- Autonomie utilisateur lors de la réinstallation et restauration en self-serviceo Stratégie de reconstruction de postes en cas de réinstallation de zéro ou de changement de poste de travailo Organisation des opérations de réparation des postes de travail et récupération des données utilisateurs		
Item n° 3.5 : Solution cryptage des terminaux		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		



<ul style="list-style-type: none"> - Mise en œuvre d'algorithmes de chiffrement puissants pour protéger les données au repos sur les appareils, notamment les ordinateurs portables, les appareils mobiles et les supports amovibles. 		
<ul style="list-style-type: none"> - Les fonctionnalités suivantes devront être respecter au minimum : <ul style="list-style-type: none"> o Chiffrement complet du disque dur o Authentification TPM avec connexion automatique pour protéger contre les modifications de l'état du système. o Compatibilité avec la norme FIPS 140-2. o Prise en charge de l'authentification multifactorielle o Prise en charge avancée du déploiement en masse o Gestion centralisée pour, la configuration et la gestion du chiffrement sur un grand nombre de postes de travail. o Gestion des clés de récupération centralisée pour pouvoir assurer le rollback en cas de panne. o Fonctionnalités de reporting avancées pour surveiller l'état de chiffrement des postes de travail, générer des rapports de conformité et effectuer des audits pour s'assurer que toutes les politiques de sécurité sont correctement appliquées. 		
<p>Prestation de service</p> <p>Le prestataire doit assister l'OFPPT à mettre en place des processus solides, une structure organisationnelle efficace et une politique de sécurité et de conformité pour la gestion des identités, des accès et des privilèges, et ce pour renforcer sa posture de sécurité et garantir un accès sécurisé et autorisé à ses ressources numériques. Il s'agit de repenser et simplifier son organisation, ses processus et sa politique notamment :</p>		
<ul style="list-style-type: none"> - Les politiques définissant les règles et les normes de sécurité relatives à l'authentification, à l'autorisation et à la gestion des accès 		



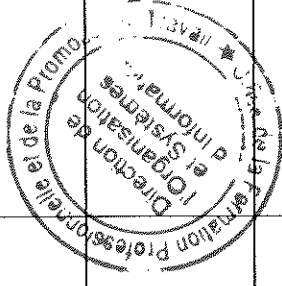


OFPPT/DOSI

Dossier d'Appel d'Offres

AO_N° 98/2024

- Structure organisationnelle		
- Les processus et les procédures pour la gestion des identités (collaborateur, un partenaire, un stagiaire, un prestataire, un infogérant) et leur cycle de vie complet, y compris la création, la modification, la désactivation/désinscription et la suppression des comptes d'utilisateurs, ainsi que la gestion des attributs d'identification des utilisateurs		
- Le Processus d'Identification et d'authentification pour vérifier l'identité des utilisateurs lorsqu'ils accèdent aux systèmes ou aux applications. Cela inclut la définition de la méthode d'authentification selon la criticité du système ou de la donnée à savoir simple authentification par mots de passe, ou d'autres méthodes d'authentification multi-facteurs par de jetons, de certificats...		
- Le Processus de Gestion des certificats numériques utilisés pour l'authentification et le chiffrement des données, y compris la création, la distribution, le renouvellement et la révocation des certificats.		
- Le Processus de Suivi et de gestion des droits d'accès des utilisateurs tout au long de leur cycle de vie, y compris la revue périodique des droits d'accès pour assurer leur pertinence et leur conformité aux politiques de sécurité. Il inclut le modèle d'attribution des droits d'accès : en fonction des rôles d'utilisateurs dans l'organisation RBAC, en fonction des attributs de l'utilisateur.		
- Les processus de surveillance et d'audit des activités d'identification et d'accès pour détecter les anomalies et les comportements suspects.		
- Les processus de demande des utilisateurs concernant la création de compte, la demande d'accès, la demande de réinitialisation de mot de passe, de renouvellement de certificat.		
- Processus de gestion du cycle de vie des certificats ainsi que les règles de conformité concernant l'usage des certificats électroniques recouvrant ainsi toutes les opérations d'enregistrement ou d'affectation d'une clé dans un système en y incluant aussi la vérification de l'identité de son possesseur, la gestion de ses équipements, des révocations...		
Le prestataire doit également assurer la mise en place des solutions IAM, PKI, et PAM qui répondent aux spécifications techniques demandées, le déploiement de ces solutions, ainsi que l'intégration de ces solutions entre elles et avec les systèmes informatiques existants.		



20

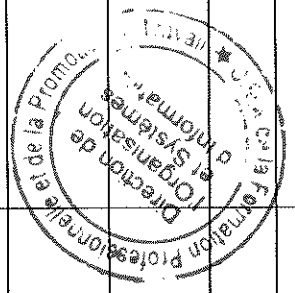


OFPPT/D.O.S.I

Dossier d'Appel d'Offres

A.O. N° 98/2024

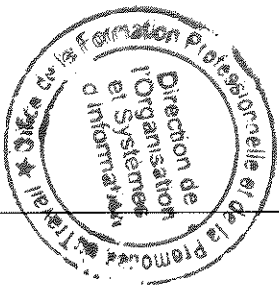
Le prestataire doit assurer aussi		
- Sécurisation de l'active directory local pour minimiser la compromission des comptes		
- Synchronisation Active directory local et Microsoft Entra		
Le prestataire doit fournir une conception pour la mise en œuvre des solutions objet de la partie 3 sur mesure en fonction des besoins de sécurité de l'OFPPT. Il doit assurer entre autre		
- Le déploiement de ces solutions avec un impact minimal sur les systèmes existants ;		
- L'accompagnement des utilisateurs, et leur support pour la conduite de changement et à la mise en œuvre de cas d'usage ;		
- Document d'Architecture : Une conception architecturale décrivant les composants des différentes solutions, leur interconnexion et leur intégration avec les systèmes existants de l'organisation		
- Documentation des processus		
- La formation pour sensibiliser les utilisateurs finaux et les administrateurs aux bonnes pratiques en matière de gestion des identités et des accès		



2



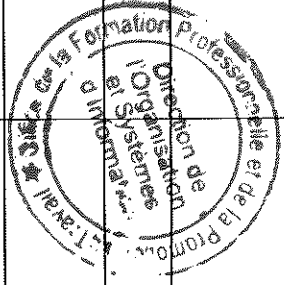
PARTIE N°4 : RÉORGANISATION DE LA GESTION DES SERVICES IT SELON LE RÉFÉRENTIEL ITIL OU EQUIVALENT

Désignations et Fonctions / caractéristiques minimales	Proposition du soumissionnaire	Appréciation de l'administration
Item N°4.1 : Mise en œuvre des pratiques ITIL ou équivalent		
La mission portera sur la formalisation des processus et pratiques ITIL v4 ou équivalent notamment : <ul style="list-style-type: none">- Gestion des incidents- Gestion des demandes de service- Gestion du changement- Gestion des problèmes- Gestion de Centre de service- Gestion des actifs- Gestion de configuration des services- Gestion du catalogue de services- Gestion des niveaux des services :- Gestion de la disponibilité- Gestion des capacités et des performances- Gestion de la continuité des services- Gestion du déploiement- Développement et gestion des logiciels- Gestion de l'infrastructure et des plates-formes- Gestion des fournisseurs		

Handwritten signature or mark



<ul style="list-style-type: none">- Gestion des connaissances- Mesures et Rapports			
Le prestataire doit proposer une documentation de tous les aspects du projet fournissant ainsi des guides détaillés et des références pour assurer une gestion transparente et une évolution future harmonieuse des processus IT, notamment les documents suivants :			
- Document de terminologie ;			
- Description détaillée de chaque processus ;			
- Procédures opérationnelles d'exécution de chaque processus ;			
- Matrice de responsabilité (RACI) : qui définit les responsabilités de chaque acteur impliqué dans les processus ITIL ou équivalent, y compris les responsables, les contributeurs, les approbateurs, etc.			
- Mesures de performance et indicateurs de performance clés (KPI) : pour évaluer l'efficacité des processus ITIL ou équivalent mis en place, comme le temps moyen de résolution des incidents, le taux de réussite des changements, etc.			
- Plan de communication : pour informer et impliquer les parties prenantes sur l'implémentation des bonnes pratiques ITIL ou équivalent.			
- Recommandations en terme d'améliorations organisationnelles.			
Le prestataire doit prévoir des séances d'accompagnement et de support pour l'équipe DOSI sur la mise en place des pratiques clé du référentiel ITIL v4 ou équivalent citées ci-dessus..			
Item N°4.2 : Formation et certification sur les bases fondamentals ITIL V4 ou équivalent			
Le prestataire doit assurer la formation ITIL Fondation avec certification pour le personnel de la DOSI (8 personnes minimum), garantissant une compréhension complète des nouveaux processus et une maîtrise des bonnes pratiques.			



220



PARTIE 5 : Sécurité des Terminals & Cybersurveillance

Désignations et Fonctions / caractéristiques minimales	Proposition du soumissionnaire	Appréciation de l'administration
Item n°5.1 : NOC (Network Operations Center) managé		
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée		
Le Network Operations Center (NOC) ou Centre d'Opérations Réseau, a pour objectif le maintien de la disponibilité, de la performance et de la sécurité des infrastructures informatiques de l'OFPPT, contribuant ainsi au bon fonctionnement des activités de l'office.		
Le NOC gère et supervise en continu les performances et la santé d'un réseau, notamment les infrastructures, les réseaux, les systèmes et les services et les équipements.		
Le NOC doit assurer la gestion, la supervision, la maintenance, l'assistance et la résolution des problèmes en arrière-plan à travers des services individualisés en fonction des besoins spécifiques à savoir :		
- Gestion des actifs :		
o Inventaire complet actifs (ordinateurs portables, des postes de travail et des serveurs), des applications logicielles, des services .		
o Fonctions de suivi, de catégorisation et de gestion du cycle de vie des actifs afin d'optimiser leur utilisation et d'améliorer la visibilité.		
o Cartographie de l'infrastructure et production des rapports spécifiques		
o Intégration avec les systèmes de help desk et les plateformes de gestion des services pour une résolution rationalisée des incidents et un suivi des actifs.		



- Gestion des correctifs

Le NOC doit assurer la gestion des correctifs qui consiste à mettre à jour tous les logiciels et périphériques avec des correctifs importants, sans nécessiter de maintenance individuelle. Il s'agit de principalement de :

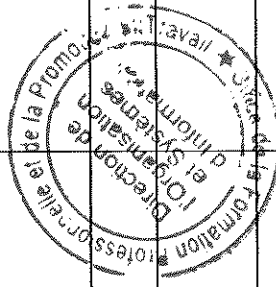
- Déploiement automatisé de correctifs pour les systèmes d'exploitation (Windows/Linux, Mac), les logiciels bureautiques, les applications, les navigateurs (Edge, Chrome, Firefox) et les dispositifs de réseau afin de remédier aux vulnérabilités et d'assurer la sécurité du système.
- Analyses programmées des correctifs, tests et fonctionnalités de rapport pour suivre l'état et la conformité des correctifs sur l'ensemble du réseau.
- Capacités de retour en arrière des correctifs et tests de compatibilité pour atténuer les risques potentiels et garantir la stabilité du système.
- Intégration avec des outils d'évaluation des vulnérabilités et des flux de renseignements sur les menaces pour une application proactive des correctifs.

- Supervision :

- Surveillance en temps réel des performances, de la disponibilité et de l'état des actifs pour détecter de manière proactive les problèmes et garantir un fonctionnement optimal
- Mécanismes d'alerte en cas de défaillance du système, de dégradation des performances, d'incidents de sécurité et de comportement anormal des actifs.
- Seuils, notifications et escalades configurables pour une réponse et une résolution rapide des alertes.

- Génération de rapports en temps réel

Le NOC génère des rapports réguliers sur les performances et la disponibilité des réseaux et des services. Il effectue également des analyses post-mortem des incidents pour identifier les causes profondes, proposer des solutions d'amélioration et prévenir les problèmes futurs.



**Le prestataire est tenu à assurer les services suivants :**

- Surveillance de la santé de chaque appareil.
- Surveillance et alerte des bases de données antivirus.
- Fourniture de l'inventaire logiciel de chaque appareil.
- Mises à jour hebdomadaires des correctifs (cela garantit que l'appareil est protégé contre les vulnérabilités).
- Installation ou de désinstallation des logiciels selon les besoins.
- Vérifications et suivi quotidiens des journaux.
- Vérifications antivirus quotidiennes.
- Vérification des sauvegardes et actions correctives si nécessaire.
- Inclus les fonctionnalités d'assistance à distance des utilisateurs

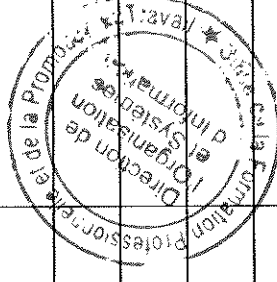
Item n°5.2 : Solution EDR managé

Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée

Le NOC doit assurer le monitoring des agents de l'Endpoint Detection Response EDR.

La solution EDR proposée doit permettre la :

- Protection antivirus
 - o Protection en temps réel contre les virus, les logiciels malveillants, les ransomwares, les chevaux de Troie et d'autres menaces en analysant les fichiers et les activités en cours d'exécution sur l'ordinateur.



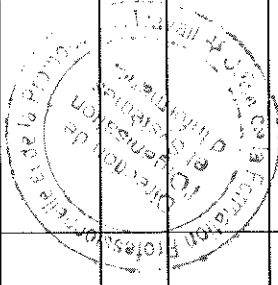


OFPPT/DOSI

Dossier d'Appel d'Offres

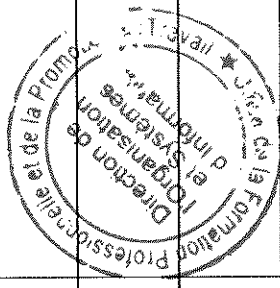
AO_N° 98/2024

<ul style="list-style-type: none">o Analyse des fichiers téléchargés, les pièces jointes d'e-mails et les périphériques de stockage amovibles pour détecter les menaces potentielles et les isoler avant qu'elles n'endommagent le système.		
<ul style="list-style-type: none">o Protection contre les ransomwares pour protéger les fichiers contre le chiffrement non autorisé et les demandes de rançon avec possibilité de restauration après une attaque.		
<ul style="list-style-type: none">o Filtrage des sites web malveillants connus pour distribuer des logiciels malveillants, du phishing ou d'autres menaces en ligne.		
<ul style="list-style-type: none">o Analyse personnalisée et planifiée pour vérifier les fichiers, les dossiers ou les disques selon un calendrier prédéfini.		
<ul style="list-style-type: none">o Mises à jour automatiques des bases de données de signatures de virus et des moteurs de détection pour garantir une protection contre les nouvelles menaces.		
<ul style="list-style-type: none">o Gestion à distance qui permettent aux administrateurs de surveiller et de gérer les solutions antivirus installées sur plusieurs ordinateurs depuis une console centralisée.		
<ul style="list-style-type: none">- Détection et prévention des menaces :		
<ul style="list-style-type: none">o Surveillance en temps réel des activités des terminaux, du trafic réseau et du comportement des utilisateurs pour détecter et prévenir les menaces avancées, les logiciels malveillants et les activités suspectes.		
<ul style="list-style-type: none">o Analyse comportementale, apprentissage automatique et intégration des renseignements sur les menaces pour une détection et une prévention proactives des menaces.		
<ul style="list-style-type: none">o Contrôles de sécurité des terminaux, liste blanche des applications pour une protection contre les activités malveillantes.		
<ul style="list-style-type: none">- Réponse aux incidents et criminalistique :		
<ul style="list-style-type: none">o Capacités rapides de réponse aux incidents, de confinement et de récupération pour atténuer les incidents de sécurité et les cyberattaques sur les terminaux.		





<ul style="list-style-type: none">o Outils d'analyse médico-légale, de recherche de menaces et d'enquête sur les incidents pour identifier les causes profondes et l'attribution des menaces.o Actions correctives, fonctionnalités de quarantaine et d'isolation pour contenir et atténuer les failles de sécurité des terminaux.			
Item N°5.3 : Solution SOC managé			
Préciser ici le nom de la Marque/ Modèle /Référence de la solution proposée			
Le Security Operations Center (SOC) ou le Centre Opérationnel de Sécurité, a pour objectif de surveiller et d'analyser en temps réel la posture de sécurité de l'OFPPT afin d'anticiper les cyberattaques.			
Le SOC est chargée de surveiller en continu les systèmes informatiques, les réseaux, les applications et les données afin de détecter, d'analyser et de répondre aux menaces de sécurité			
Le SOC analyse l'incident pour comprendre sa nature, son impact potentiel et les techniques utilisées par les attaquants.			
Le SOC met en œuvre des mesures de réponse pour contenir et éradiquer la menace. Cela peut inclure l'isolation des systèmes infectés, le blocage des adresses IP malveillantes, la désactivation des comptes compromis, etc.			
Le SOC effectue une analyse approfondie des tendances et des modèles d'attaques pour identifier les vulnérabilités potentielles et les faiblesses de sécurité.			
Le SOC doit fournir des rapports de remédiation priorités en fonction des risques pour aider à concentrer les efforts là où le meilleur retour sera obtenu, ainsi que des rapports de tendance et des rapports exécutifs à l'intention de la direction (les activités de sécurité, les incidents détectés, les mesures prises et les recommandations d'amélioration).			
Le SOC doit permettre une amélioration continue de la posture de sécurité de l'OFPPT à travers l'utilisation des technologies de sécurité de pointe, l'ajustement des stratégies de détection et de réponse, et l'adoption des meilleures pratiques de sécurité.			



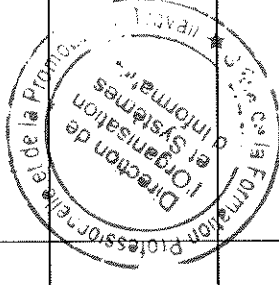


OFPPT/DOSI

Dossier d'Appel d'Offres

AO_N° 98/2024

La plateforme SOC doit permettre de déployer des capteurs physiques et/ou software. Ces capteurs doivent être en mesure de collecter les journaux locaux des dispositifs et de signaler les alertes pour remédiation. Les agents doivent pouvoir être installés sur n'importe quel appareil Windows, MAC, Linux.		
La plateforme SOC doit fournir un ensemble de méthodes d'alerte et de détection, y compris, mais sans s'y limiter, les intrusions dans le réseau, le comportement du réseau, les résumés de détection, les menaces émergentes et les événements de suivi.		
La plateforme SOC doit pouvoir s'intégrer à l'Active Directory de l'OFPPT et à l'environnement "Microsoft Entra" le plus récent.		
La plateforme SOC doit être en mesure de fournir une vue complète de tous les services basés sur le cloud : Entra ID & O365, Azure, AWS...		
La plateforme doit être capable d'ingérer tous les types de formats de journaux, l'ingestion doit pouvoir prendre n'importe quel "format" de journal et, s'il n'est pas disponible, la plateforme doit être capable de configurer un processus d'ingestion de journaux. Les types de journaux doivent être (au moins) les suivants : pare-feu, AV & EDR, applications et services.		
La plateforme SOC doit également comprendre une "section de renseignement" qui fournit au moins les données de renseignement suivantes : recherches et analyses sur le Dark Web, renseignements sur les menaces, analyse des vulnérabilités, évaluations de la réputation et un fil d'actualité sur la sécurité.		
La plateforme doit être gérée par le fournisseur 24 heures sur 24, 7 jours sur 7 et 365 jours par an.		
Le SOC doit disposer des outils et des services avancés à savoir :		
Détection d'intrusion		
La plateforme SOC doit pouvoir s'intégrer avec les solutions existantes et les solutions déployées dans le présent marché pour la détection d'intrusion en se basant sur les IoC et en intégrant IA dans le processus de détection.		
Il est nécessaire de disposer d'une sonde de détection qui dispose au minimum des fonctionnalités suivantes :		





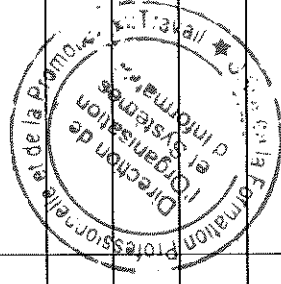
20

Dossier d'Appel d'Offres

AO_N° 98/2024

OFPPT/DOSI

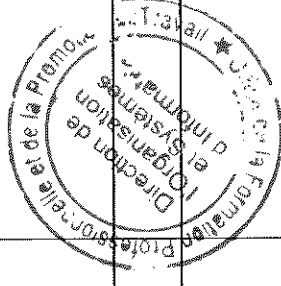
- Fonctionnement offline (maîtrise des données, etc)			
- Analyse avec plusieurs			
- Analyse statique et heuristique			
- Retro-analyse de fichiers dans le temps			
- Détection de communications C&C inconnus			
- Interfaçage avec des outils avec des outils de Threat Intelligence			
- Possibilité de dropped du flux en se basant sur IP/port/Vlan			
- Possibilité de faire de l'agrégation de flux (si TAP branché en direct sur la sonde)			
- Interface pour soumettre un fichier et l'analyser avec des moteurs AV			
- Pouvoir identifier un flux par IP/port/Vlan / sonde de capture / interface de capture			
Il doit permettre également:			
- Détection de compromission de fichiers (contrôle d'intégrité)			
- Analyse de la base de registre (windows) ou des LKMs (Linux)			
- Analyse et corrélation de logs en provenance de firewalls hétérogènes			
- Analyse des flux cryptés			
- Vérification de l'intégrité des systèmes			
Gestion des vulnérabilités :			



2



Pour détecter les nouvelles vulnérabilités signalées via l'utilisation d'outils de scan de vulnérabilités, l'analyse des bulletins de sécurité et la surveillance des flux de Threat Intelligence			
SIEM			
Le Security Information and Event Management SIEM pour la collecte, l'analyse et la gestion des informations sur les événements de sécurité informatique à partir de différentes sources (applications, appareils, réseau, serveurs utilisateurs			
Le SIEM doit offrir les fonctions de base suivantes :			
<ul style="list-style-type: none">- Gestion des journaux : Les systèmes SIEM centralisent de grandes quantités de données qu'ils organisent en vue de déterminer si celles-ci présentent des signes de menace, d'attaque ou de violation.			
<ul style="list-style-type: none">- Corrélation entre les événements : afin de détecter rapidement les menaces potentielles et d'y répondre.			
<ul style="list-style-type: none">- Surveillance et réponse aux incidents : Les technologies SIEM surveillent les incidents liés à la sécurité sur le réseau d'une organisation, et fournissent des alertes et des audits pour toutes les activités en lien avec ces incidents.			
Plateformes de Threat Intelligence :			
Pour agréger les données provenant de diverses sources, telles que des flux de renseignements sur les menaces TIF, des rapports de sécurité, des analyses de vulnérabilités, IDS, SIEM, Firewall, etc. Elles fournissent des fonctionnalités avancées d'analyse et de corrélation pour identifier les schémas et les tendances des menaces			
Services de veille sur les menaces :			
Ces services fournissent des rapports et des analyses détaillées sur les tendances actuelles des menaces, les groupes de cybercriminels, les vulnérabilités exploitées, etc.			
Services de Threat Hunting :			



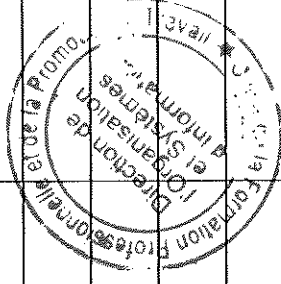


OFPPT/DOSI

Dossier d'Appel d'Offres

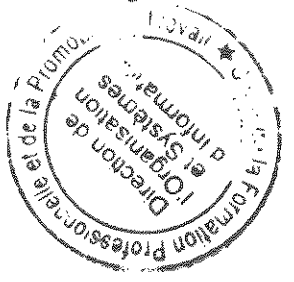
AO, N° 98/2024

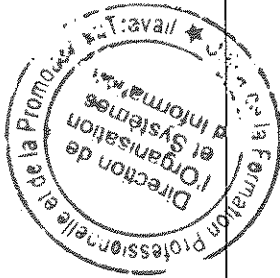
Le Threat Hunting consiste à rechercher activement des indicateurs de compromission (IOC) et des comportements anormaux qui pourraient échapper à la détection automatisée			
Le prestataire est tenu à assurer les services suivants :			
- Surveillance 24/7 :			
o Surveillance continue des systèmes, des réseaux et des terminaux pour détecter et répondre aux incidents de sécurité en temps réel.			
- Détection et Analyse des Menaces :			
o Utilisation d'outils de détection des menaces, d'analyses comportementales et de technologies avancées pour identifier les activités suspectes et les anomalies.			
o Analyse des alertes pour déterminer leur gravité et leur pertinence.			
- Réponse aux Incidents :			
o Gestion des incidents de sécurité, y compris l'investigation, la réponse et la résolution des problèmes.			
- Gestion des Alertes :			
o Gestion des alertes de sécurité.			
o Priorisation des alertes en fonction de leur impact potentiel et de leur urgence.			
- Analyse Forensique :			
o Réalisation d'analyses approfondies pour comprendre les incidents de sécurité, reconstituer les événements et collecter des preuves pour les enquêtes.			
- Gestion des Journaux et des Événements :			





o Collecte, centralisation et analyse des journaux système, des journaux d'application et des événements de sécurité.		
- Gestion des Vulnérabilités :		
o Identification et évaluation des vulnérabilités dans les systèmes et les applications.		
- Rapports et Documentation :		
o Génération de rapports réguliers sur la sécurité, les incidents et les activités du SOC.		
o Documentation des incidents, des actions entreprises et des leçons apprises.		
- Conseil et Optimisation :		
o Fourniture de recommandations pour améliorer la posture de sécurité globale.		
- Formation et Sensibilisation :		
o Formation sur les meilleures pratiques en matière de sécurité.		
o Sensibilisation aux menaces émergentes et aux nouvelles vulnérabilités.		



**ANNEXE II****Tableau de répartition des équipements par site**

	Siège	Annexe Casablanca Sidi Maarouf	Annexe Casablanca Ain Borja	Casablanca	Béni-Mellal	Laayoune	Errachidia	Agadir	Fes	Oujda	Tanger	Rabat	Marrakech
Item 2.1 FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (siège)	2												
Item 2.2 FIREWALL NOUVELLE GÉNÉRATION NGFW / SDWAN (régions et annexes siège)			1	1	1	1	1	1	1	1	1	1	1
Item 2.3 Switch Fédérateur	2												
Item 2.4 Switch multi Giga (avec PoE+)	7												
Item 2.5 Switch 48 ports (avec PoE+)	33	1	1	1	0	0	0	1	1	2	0	0	1
Item 2.6 Switch 24 ports (avec PoE+)	11	2	2	3	1	3	3	2	0	0	2	3	1
Item 2.7 Points d'accès Wifi	70	6	16	10	2	6	3	4	4	4	4	6	4