LABORATOIRE PUBLIC D'ESSAIS ET D'ETUDES

DIRECTION DE LA LOGISTIQUE, DES ACHATS, DES APPROVISIONNEMENTS ET DE LA GESTION DU PATRIMOINE

CAHIER DE PRESCRIPTIONS SPECIALES
RELATIF À L'APPEL D'OFFRES OUVERT
SUR OFFRES DE PRIX N°80/2025

OBJET : FOURNITURE ET DÉPLOIEMENT D'UNE SOLUTION DE PROTECTION ANTIVIRALE AVEC EDR EN LOT UNIQUE

Etabli en application de l'alinéa 1 paragraphe 1 de l'article 21 du règlement des achats du LPEE RA/980/1, version 02 du 01 Juin 2025 fixant les conditions et les formes dans lesquelles sont passés les marchés pour le compte du Laboratoire Public d'Essais et d'Eudes ainsi que certaines règles relatives à leur gestion et à leur contrôle tel qu'il est publié sur le site www.lpee.ma.

Date limite de dépôt des plis : 30/12/2025 à 09H00

D.L.A.A.P
DV Achats

SOMMAIRE

OBJET : FOURNITURE ET DÉPLOIEMENT D'UNE SOLUTION DE PROTECTION ANTIVIRALE AVEC EDR EN LOT UNIQUE

ENTRE

Le Laboratoire Public d'Essais et D'Etudes (L.P.E.E), société anonyme au capital de 247 702 400,00 Dhs (Deux Cent Quarante Sept Millions Sept Cent Deux Mille Quatre Cent Dirhams), inscrit au registre de commerce de Casablanca sous le N° 32131, affilié à la Caisse Nationale de sécurité sous le n° 1066308, ICE N° 001527537000028, représenté par **Monsieur Hammou BENSAADOUT,** Directeur Général dudit laboratoire en vertu des pouvoirs qui lui sont conférés, faisant élection de domicile à Casablanca, 25 Rue d'Azilal.

Désigné ci-après par le terme « **Maître d'ouvrage** » ou « **LPEE** »,

D'UNE PART

ET

Cas d'une personne physique

..... *(Raison sociale et forme juridique),*

M.....qualité.....

Agissant en son nom et pour son propre compte.

Au capital social .....Patente n° .....

Registre de commerce de .....Sous le n°.....

Affilié à la CNSS sous n°.....

ICE n°.....

Faisant élection de domicile au.....

Compte bancaire RIB (24 positions).....

Ouvert auprès de.....

Désigné ci-après par le terme « **Prestataire de services** » ou « **Titulaire** »,

D'AUTRE PART

Cas d'une personne morale

..... *(Raison sociale et forme juridique),*

Représenté par M. .....qualité.....en vertu des pouvoirs qui lui sont conférés.

Au capital social ..... Patente n° .....

Registre de commerce de .....Sous le n°.....

Affilié à la CNSS sous n° .....

ICE n°.....

Faisant élection de domicile au .....

Compte bancaire RIB *(24 positions)*.....

Ouvert auprès de.....

Désigné ci-après par le terme « **Prestataire de services** » ou « **Titulaire** »,

D'AUTRE PART

Cas d'un groupement

Les membres du groupement soussignés constitués aux termes de la convention .....(les références de la convention)..... :

Membre 1 :

..... *(Raison sociale et forme juridique),*

Représenté par M. .....qualité .....en vertu des pouvoirs qui lui sont conférés.

Au capital social ..... Patente n° .....

Registre de commerce de .....Sous le n°.....

Affilié à la CNSS sous n° .....

ICE n°.....

Faisant élection de domicile au .....

Compte bancaire RIB *(24 positions)* .....

Ouvert auprès de.....

Membre 2 :

(Servir les renseignements le concernant)

.....

.....

Membre n :

(Servir les renseignements le concernant)

.....

.....

Nous nous obligeons (conjointement ou solidairement, selon la nature du groupement) ayant M..... (Prénom, nom et qualité) en tant que mandataire du groupement et coordonnateur de l'exécution des prestations, ayant un compte bancaire commun sous n° (RIB sur 24 positions) .....

Ouvert auprès de .....

Désigné ci-après par le terme **« Prestataire de services »** ou **« Titulaire »,**

D'AUTRE PART

IL A ETE ARRETE ET CONVENU CE QUI SUIT

CHAPITRE PREMIER : CAHIER DES CLAUSES ADMINISTRATIVES ET FINANCIERES

Article 1: Objet du marché

Le présent marché a pour objet **Fourniture et déploiement d'une solution de protection antivirale avec module EDR** pour l'ensemble du parc informatique du Laboratoire Public d'Essais et d'Etudes (LPEE) en un (01) lot unique, dont les détails figurent dans le cahier des prescriptions techniques et les quantités sont spécifiées dans le bordereau des prix-détail estimatif.

Article 2: Présentation du maître d'ouvrage

Autorité compétente : Le Directeur Général du LPEE.

Maître d'ouvrage : Le Laboratoire Public d'Essais et d'Etudes représenté par son Directeur Général.

La Direction de la Logistique, des Achats, des Approvisionnements et de la gestion du Patrimoine du LPEE (DLAAP) est chargée de la gestion administrative du présent marché.

La Direction d'organisation et des systèmes d'information (DOSI) est chargée, sur le plan technique, du suivi de l'exécution du présent marché.

Article 3: Consistance des prestations de services

Les prestations de services à réaliser au titre du présent marché font l'objet de la **Fourniture et déploiement d'une solution de protection antivirale avec module EDR en lot unique.**

Article 4: Documents constitutifs du marché

Les documents constitutifs du marché sont ceux énumérés ci-après :

a) Le bordereau des prix-détail estimatif ;
b) L'acte d'engagement ;
c) Le cahier des prescriptions spéciales (CPS) ;
d) Règlement de consultation (RC) ;
e) L'offre technique ;
f) La déclaration sur l'honneur ;
g) Le cahier des clauses générales applicables aux marchés de services exécutées pour le compte du LPEE (CCGS).

En cas de discordance ou de contradiction entre les documents constitutifs du marché, ceux-ci prévalent dans l'ordre où ils sont énumérés ci-dessus.

Article 5: Pièces contractuelles postérieures à la conclusion du marché

Les pièces contractuelles postérieures à la conclusion du marché comprennent :

- Les ordres de service ;
- Les avenants éventuels ;
- La décision prévue à l'article 33 du CCGS, relative à la résiliation du marché.

D.L.A.A.P
DV Achats

Les avenants et la décision susvisés sont soumis à l'approbation de l'autorité compétente.

Article 6: Référence aux textes généraux et spéciaux applicables au marché

Les parties contractantes du marché sont soumises aux dispositions des textes suivants :

- La loi n°69-00 relative au contrôle financier de l'état sur les entreprises publiques et autres organismes, promulguée par le Dahir n°1-03-195 du 16 ramadan 1424 (11 novembre 2003) ;
- La loi n 112.13 du 29 rabii II 1436 (19 février 2015) relative au nantissement des marchés publics ;
- Dahir n°1-00-91 du 15 février 2000 portant promulgation de la loi n °17-97 sur la protection de la propriété intellectuelle ;
- Le Règlement relatif aux conditions et formes de passation des marchés du LPEE RA/980/1, version 02 du 01 Juin 2025 ;
- Le Cahier des Clauses Générales applicables aux marchés de services passés pour le compte du LPEE (CCG/980/01) ;
- Tous les textes réglementaires rendus applicables au Maroc à la date de signature du marché et qui sont en rapport avec l'objet du présent marché.

Le prestataire de services devra se procurer ces documents, s'il ne les possède pas, et ne pourra en aucun cas exciper de l'ignorance de ceux-ci, et se dérober aux obligations qui y sont contenues.

Article 7: Validité et date de notification de l'approbation du marché

Le présent marché ne sera valable et définitif qu'après son approbation par l'autorité compétente.

L'approbation du marché doit intervenir avant tout commencement d'exécution. Cette approbation sera notifiée dans un délai maximum de soixante-quinze (75) jours à compter de la date d'ouverture des plis.

L'approbation des marchés ne doit être apposée par l'autorité compétente qu'après l'expiration d'un délai d'attente d'une durée de quinze (15) jours à compter du jour suivant la date d'achèvement des travaux de la commission d'ouverture des plis.

Article 8: Pièces mises à la disposition du prestataire de services

Aussitôt après la notification de l'approbation du marché, le maître d'ouvrage remet gratuitement au prestataire de services, contre décharge, les documents constitutifs du marché en l'occurrence les pièces expressément désignées à l'article 4 du présent marché à l'exception du cahier des clauses générales applicables aux marchés de services, qui peut être téléchargé sur le site du LPEE : www.lpee.ma.

Le maître d'ouvrage ne peut délivrer ces documents qu'après constitution du cautionnement définitif.

Article 9: Election du domicile du prestataire de services

Toutes les correspondances relatives au présent marché sont valablement adressées au domicile du prestataire de services sis.....

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

Article 10: Nantissement

Dans l'éventualité d'une affectation en nantissement du présent marché, il est stipulé que :

1) La liquidation des sommes dues par, le maître d'ouvrage, en exécution du présent marché et leurs paiements seront opérés par les soins de Monsieur le Directeur Général du LPEE, seul qualifié pour recevoir les significations des créanciers du titulaire du marché ;

2) Au cours de l'exécution du marché, les documents cités à l'article 8 de la loi n°112-13 peuvent être requis du maître d'ouvrage, par le titulaire du marché ou le bénéficiaire du nantissement ou de la subrogation, et sont établis sous sa responsabilité ;

3) Lesdits documents sont transmis directement à la partie bénéficiaire du nantissement avec communication d'une copie au prestataire de services, dans les conditions prévues par l'article 8 de la loi n° 112-13.

Le maître d'ouvrage délivre sans frais, au prestataire de services, sur sa demande et contre récépissé, un exemplaire spécial du marché portant la mention "exemplaire unique" et destiné à former titre conformément aux dispositions législatives relatives au nantissement des marchés de l'état et des établissements publics tel que modifié et complété, et ce, en application du paragraphe 4 de l'article 11 du CCGS.

Article 11: Sous-traitance

Si le prestataire de services envisage de sous-traiter une partie du marché, il doit requérir l'accord préalable du maître d'ouvrage auquel il est notifié la nature des prestations de services à sous-traiter, la raison ou la dénomination sociale, l'adresse et l'identité des sous-traitants et une copie conforme du contrat de sous-traitance.

Les sous-traitants doivent satisfaire aux conditions requises aux concurrents à l'article 28 du règlement des achats du LPEE.

Le prestataire de services 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 reconnait aucun lien juridique avec les sous-traitants.

Article 12: Durée du marché

La durée du marché est de **douze (12) mois** n'excédant pas l'année en cours, et ce, à compter de la date prévue par l'ordre de service prescrivant le commencement de la réalisation de la prestation.

Le présent marché est reconduit, tacitement, d'année en année dans la limite d'une durée totale de trois (3) années.

La non-reconduction du marché est prise à l'initiative de l'une des deux parties moyennant un préavis de trois (3) mois, avant la fin de l'année en cours. Elle donne lieu à la résiliation du marché.

Article 13: **Délai d'exécution**

Le prestataire de services devra réaliser les prestations désignées en objet prescrits par ordre de service dans un délai de de vingt (20) jours.

Ce délai court à partir de la date prévue par l'ordre de service prescrivant le commencement de la prestation.

Le fournisseur devra réaliser les prestations de mise en œuvre et de paramétrage selon un programme préétabli en accord avec le maitre d'ouvrage.

Article 14: **Nature des prix**

Le présent marché est à prix unitaires.

Les sommes dues au prestataire de services sont calculées par application des prix unitaires portés au bordereau des prix-détail estimatif, joint au présent cahier des prescriptions spéciales, aux quantités 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 présent marché.

Article 15: **Caractère des prix**

Le présent marché est passé à prix fermes et non révisables et s'entendent comme suit :

Toutes taxes comprises, rendu au siège du LPEE, sis 25 rue d'Azilal, Casablanca- Maroc.

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 16: **Cautionnement provisoire et cautionnement définitif**

Le cautionnement provisoire, **ne comportant aucune date limite,** est fixé à : **Huit-mille** (8 000,00) DH

Le cautionnement provisoire reste acquis au LPEE, notamment dans les cas suivants :

- Si le soumissionnaire retire son offre ou se désiste pendant le délai de validité des offres ;
- Si l'offre du soumissionnaire ayant présenté l'offre la plus avantageuse est écartée pour les motifs suivants :
    - Ne fournit aucune réponse ;
    - Ne régularise pas les discordances constatées entre les diverses pièces de son dossier administratif, technique et additif ;
    - Ne confirme pas les rectifications des erreurs matérielles relevées ;
    - Fournit des justifications non convaincantes en ce qui concerne le ou les prix unitaires principaux jugés excessifs ou anormalement bas, le cas échéant.

- Dans le cas de la défaillance du groupement quel que soit le membre défaillant et ce, conformément aux dispositions de l'article 136 du règlement des achats du LPEE ;
- Si le titulaire refuse de signer le marché ;
- Si le titulaire ne dépose pas le cautionnement définitif dans les trente (30) jours suivant la notification de l'approbation du marché.

Le cautionnement provisoire ou la caution qui le remplace sera libéré conformément aux dispositions de l'article 26 du règlement des achats du LPEE.

Le montant du cautionnement définitif, **ne comportant aucune date limite**, est fixé à **trois pour cent (3%)** du montant initial du marché. Il doit être constitué dans les trente (30) jours qui suivent la notification de l'approbation du marché. Il reste affecté à la garantie des engagements contractuels de l'attributaire jusqu'à la réception définitive des prestations.

Le cautionnement définitif sera restitué ou la caution qui le remplace est libérée à la suite d'une mainlevée délivrée par le maître d'ouvrage dans un délai maximum de quatre-vingt-dix (90) jours suivant la date de la réception définitive des prestations et sous réserves des dispositions prévues par l'article 16 du CCGS.

Article 17: Retenue de garantie

Aucune retenue de garantie ne sera prélevée au titre du présent marché.

Article 18: Assurances – Responsabilité

Le prestataire de services doit adresser au maître d'ouvrage, avant tout commencement de réalisation des prestations de service, les copies des polices d'assurance qu'il doit souscrire et qui doivent couvrir tous les risques inhérents à la réalisation du marché, et ce, conformément aux dispositions de l'article 20 du CCGS. Il devra contracter dès le début d'exécution du marché, et pendant toute la durée de celui-ci, une assurance couvrant les risques suivants :

- La responsabilité découlant de l'utilisation des véhicules automobiles pour les besoins de l'exécution du marché conformément à la législation et à la réglementation en vigueur ;
- La responsabilité d'accident du travail survenant à ses agents conformément à la législation et à la réglementation en vigueur.

Le maître d'ouvrage ne peut être tenu pour responsable des dommages ou indemnités légales à payer en cas d'accidents survenus aux employés du prestataire de services ou ses sous-traitants.

A ce titre, le prestataire de services garantira le maître d'ouvrage contre toute demande de dommages-intérêts ou indemnités et contre toute réclamation, plainte, poursuite, frais, charge et dépense de toute nature relative à ces accidents.

Article 19: Propriété industrielle, commerciale ou intellectuelle

Le prestataire de services garantit formellement le maître d'ouvrage 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 prestataire de services le cas échéant, d'obtenir les cessions, licence d'exploitation ou autorisation nécessaires et de supporter la charge des frais et redevances y afférentes.

Article 20: Obligations de discrétion

Le prestataire de services qui, soit avant la notification du marché, soit au cours de son exécution, a reçu communication, à titre confidentiel, de renseignements, documents ou objets quelconques, est tenu de maintenir confidentielle cette communication. Ces renseignements, documents ou objets quelconques ne peuvent, sans autorisation, être communiqués à d'autres personnes que celles qui ont qualité pour en connaître. Le maître d'ouvrage s'engage à maintenir confidentielles les informations, signalées comme telles, qu'il aurait pu recevoir du prestataire de services.

Article 21: Délai de garantie

Le délai de garantie de la solution objet du présent Appel d'Offres est de **trois (3) ans** à partir de la date de la réception provisoire de la solution.

Pendant le délai de garantie, le prestataire de services est tenu, entre autres, de garantir la solution livrée contre toute non-conformité et écart par rapport aux spécifications du marché. Il doit aussi apporter toute son assistance technique pour le déblocage des problèmes qui pourraient survenir au niveau de la solution « Support éditeur », objet du présent marché.

Cette garantie concerne les licences et le support de la solution livrées par le prestataire de services. Dans le cadre de cette garantie, le prestataire de services maintiendra la solution en bon état de fonctionnement et procédera à toutes les interventions éventuelles qui s'avéreraient nécessaires. D'une manière générale, durant toute la durée de la garantie, les mises à jour sur la solution devront être effectuées par le prestataire de services.

Pendant cette période de garantie, le prestataire de services dispensera au LPEE le service de support logiciel comprenant :

- Installation et mise en état de bon fonctionnement de la solution sous licence ;

- Responsabilité du prestataire dans l'installation des nouvelles versions de la solution en cas de mise à jour ;

- Correction des anomalies détectées par le Maître d'Ouvrage ;

En cas d'un nouveau correctif de la part de l'éditeur de la solution proposée pour corriger une anomalie sur un système similaire à celui installé chez le LPEE, le prestataire doit informer ce dernier et doit mettre en œuvre, à titre préventif, les corrections définitives ou provisoires mises au point.

Article 22: Modalités de règlement

Pour l'établissement des ordres de paiement, le prestataire de services est tenu de fournir au maître d'ouvrage une facture appuyée par attachements signés et cachetés par le LPEE, et d'une copie de l'ordre de service signé et cacheté par le fournisseur, et doit être établie en trois (03) exemplaires décrivant les fournitures livrées et indiquant les quantités livrées, le montant total à payer ainsi que tous les éléments nécessaires à la détermination de ce montant.

La facture doit être établie et déposée contre accusé de réception, au plus tôt, à la date de fin de réalisation des prestations de services, et au plus tard, le dernier jour du mois de fin de réalisation des prestations de services. La facture doit également porter l'ensemble des mentions obligatoires conformément aux dispositions de l'article 145 du Code Général des Impôts.

Si le prestataire de services n'établit pas et/ou ne dépose pas la facture dans le délai précité, ou que la facture ne respecte pas les mentions obligatoires, toutes les sanctions pour infraction aux délais de paiement que le maître d'ouvrage devra verser au trésor conformément aux dispositions de la loi 69.21 publiée au Bulletin Officiel n°7204 du 15 juin 2023 seront déduites des sommes dues au fournisseur de plein droit et sans mise en demeure préalable.

Le règlement sera effectué sur la base desdits ordres de paiement en application des prix du bordereau des prix – détail estimatif aux quantités réellement livrées. Déduction faite de l'application des pénalités de retard le cas échéant.

Sur ordre du maître d'ouvrage, les sommes dues au prestataire de services seront versées au Compte bancaire RIB *(24 positions)*..... ouvert auprès de ..... *(la banque)* à quatre-vingt-dix (90) jours fin du mois de la date de facture.

Article 23: Réceptions provisoires et définitive

Le maître d'ouvrage se réserve le droit de s'assurer, dans les locaux du fournisseur, des quantités et des spécifications qualitatives indiquées dans la documentation technique, avant l'expédition des fournitures.

Les fournitures livrées sont soumises à des vérifications destinées à constater leur conformité, à tous égards, avec le descriptif des fournitures figurant au bordereau des prix détaillé estimatif, ou par comparaison avec les modèles décrits dans la documentation technique.

La réception ne peut être prononcée par le maître d'ouvrage, ou par ses représentants, qu'après un contrôle quantitatif, qualitatif et technique. Toutefois, cette réception ne dégage pas le fournisseur de sa responsabilité en cas de vices cachés ou de non-conformités des fournitures.

À l'issue de ces opérations, le maître d'ouvrage prononce la réception provisoire. La réception définitive sera prononcée après l'expiration du délai de garantie.

Les opérations susmentionnées sont sanctionnées, selon le cas, par un procès-verbal de réception provisoire ou définitive, signé par les membres de la commission de réception désignée à cet effet.

Article 24: Pénalités pour retard

A défaut d'avoir réalisé les prestations de services dans le délai prescrit à l'article 13 du présent marché, il sera appliqué au prestataire de services une pénalité par jour calendaire de retard **d'un pour mille (1‰)** du montant de la tranche considérée du marché modifiée ou complétée éventuellement par les avenants.

Ces pénalités seront appliquées de plein droit et sans mise en demeure sur toutes les sommes dues au prestataire de services.

L'application de ces pénalités ne libère en rien le prestataire de services de l'ensemble des autres obligations et responsabilités qu'il aura souscrites au titre du présent marché.

Toutefois, le montant cumulé de ces pénalités est plafonné à dix pour cent (10%) du montant initial du marché modifié ou complété éventuellement par des avenants, tel que stipulé dans l'article 42 du CCGS.

Lorsque le plafond des pénalités est atteint, l'autorité compétente est en droit de résilier d'office le marché et sans préjudice de l'application des mesures coercitives conformément aux dispositions de l'article 52 du CCGS applicable aux marchés de services.

Article 25: Droits de timbre et d'enregistrement

Conformément à l'article 6 du CCGS applicable aux marchés de services, le prestataire de services doit acquitter les droits auxquels peuvent donner lieu l'enregistrement et timbre du marché, tels qu'ils résultent des lois et règlements en vigueur.

Article 26: Lutte contre la fraude et la corruption

Le prestataire de services ne doit pas recourir par lui-même ou par personne interposée à des actes de corruption, à des manœuvres frauduleuses, et à des pratiques collusoires, à quelque titre que ce soit, dans les différentes procédures de passation, de gestion et d'exécution du marché.

Le prestataire de services 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 la réalisation du présent marché.

Article 27: Résiliation du marché

La résiliation du marché peut être prononcée conformément aux dispositions prévues aux articles 27 à 33 CCGS du LPEE applicable aux marchés de services.

La résiliation du marché ne fera pas obstacle à la mise en œuvre de l'action civile ou pénale qui pourrait être intentée au prestataire de services en raison de ses fautes ou infractions.

Si des actes frauduleux, des infractions réitérées aux conditions de travail ou des manquements graves aux engagements pris ont été relevés à la charge du prestataire de services, le maitre d'ouvrage, sans préjudice des poursuites judiciaires et des sanctions dont le prestataire de services est passible, peut par décision motivée, après avis de la Commission des Achats, et approbation de l'autorité compétente, l'exclure temporairement ou définitivement de la participation aux marchés du LPEE.

Article 28: Règlement des différends et litiges

Si au cours de la réalisation du marché, des différends et litiges surviennent avec le prestataire de services, les parties s'engagent à régler ceux-ci dans le cadre des stipulations des articles 52, 53 et 54 du CCGS du LPEE applicable aux marchés de services.

Les litiges entre le maître d'ouvrage et le prestataire de services sont soumis aux tribunaux compétents de Casablanca.

CHAPITRE II : CAHIER DES PRESCRIPTIONS TECHNIQUES

Article 29: Contexte

Le présent marché a pour objet de fourniture, et déploiement d'une solution de protection antivirale avec module EDR (Endpoint Detection And Response) centralisée pour le compte de LPEE. Cette solution centralisée EDR devra permettre de remplacer la solution actuelle et de répondre aux enjeux stratégiques suivants :

• La licence de la solution actuellement utilisée par LPEE, et qui est destinée à être remplacée, expirera le 28 janvier 2026

• Assurer une protection avancée, proactive et en temps réel contre un large spectre de cybermenaces visant les terminaux fixes et mobiles.

• Mettre en place une gestion centralisée, efficace et sécurisée de l'ensemble du parc des Endpoints (déploiement de politiques, gestion des configurations, contrôle des accès, etc.).

• Améliorer significativement la visibilité sur les activités suspectes ou malveillantes au niveau des terminaux, et renforcer nos capacités de détection, d'analyse et de réponse rapide aux incidents

• Garantir la conformité de notre gestion des terminaux avec les standards de sécurité pertinents et les réglementations en vigueur.

Article 30: Périmètre

Le maître d'ouvrage dispose d'un siège à Casablanca et de plusieurs sites distants répartis à travers le royaume. Tous ces sites sont interconnectés via un réseau SD-WAN et VPN.

Systèmes d'exploitation :

Le périmètre concerné comprend environ 1 200 postes de travail et 30 serveurs répartis sur l'ensemble du parc informatique.

- Postes de travail : Environnements Microsoft Windows, toutes versions confondues.
- Serveurs : Environnements Microsoft Windows Server (toutes versions) et Linux (distributions Enterprise).

Il est impérativement exigible que la console d'administration centrale de la solution soit déployée et hébergée en mode **on-premise**, au sein de l'infrastructure technique de LPEE. L'intégration transparente avec l'environnement existant de LPEE (notamment Active Directory, SIEM, Mail, etc.) est également requise.

Article 31: Fonctionnalités et télémétrie de la solution

- Être parmi les leaders dans la protection antiviral et Endpoint Protection and response ;

- Offrir une solution combinant EDR et EPP (incluant anti-malware, réputation web, contrôle des périphériques, Data Loss Prevention DLP, ML, analyse comportementale, Sandbox, patching virtuel, Device Access Control, contrôle applications, etc) en un seul agent.
- Protéger et sécuriser les environnements virtuels basés sur Nutanix AHV et VMware.
- Fournit une détection et une réponse automatisées avancées des menaces contre diverses menaces de logiciels malveillants avancés, y compris les attaques sans fichier, le cryptomining et les ransomwares.
- Capable de fournir en un seul agent les fonctionnalités suivantes : Data Loss Prevention (DLP), Virtual Patching, Application Control, Device Access Control, etc.
- Fournir à la fois des fonctionnalités de plate-forme de protection des Endpoint (EPP) et de détection et de réponse des endpoints (EDR) dans un seul agent.
- Effectuer une investigation sur les menaces grâce à l'EDR intégré.
- Doit avoir un système de prévention d'intrusion basé sur l'hôte (HIPS) pour corriger virtuellement les vulnérabilités connues et inconnues avant qu'un correctif ne soit disponible ou déployable.
- La solution doit pouvoir utiliser les services Threat Intelligence basés sur le cloud du fournisseur pour obtenir la réputation des objets, des noms d'hôte et des adresses IP distantes. Vérifier les informations des certificats des objets binaires et plus.
- La solution doit effectuer une enquête sur les menaces grâce à l'EDR intégré.
- Capable de prendre en charge l'installation de l'agent sur Windows et MAC OS ainsi que dans l'environnement de bureau virtuel.
- Doit être en mesure de présenter une solution de sécurité holistique offrant une protection des endpoints et une visibilité centrale sur le paysage des menaces.
- Prend en charge le cryptage basé sur SSL pour un accès sécurisé au navigateur.
- Surveillez les statistiques de santé du système pour fournir la preuve de la disponibilité des agents et de la conformité aux politiques.
- La solution doit être capable de supprimer (réinitialiser) les modifications des logiciels malveillants dans le registre Windows, de supprimer les fichiers déposés et de mettre fin à l'exécution des processus malveillants.
- Capable d'effectuer différentes actions d'analyse en fonction de divers types de logiciels malveillants (cheval de Troie / ver, virus, etc.).
- La solution doit avoir une capacité de surveillance du comportement pour détecter le comportement des programmes malveillants qui est courant pour exploiter les attaques.
- Capable de détecter et de supprimer les logiciels espions et publicitaires même après leur installation et leur exécution sur l'ordinateur.
- Doit fournir une protection continue contre les logiciels malveillants et être capable d'effectuer des mises à jour, que le client soit ou non connecté au serveur de gestion.
- Doit fournir une protection continue contre les logiciels malveillants, que le terminal soit connecté à Internet ou non.
- La solution doit être capable de bloquer l'accès aux sites Web et URL malveillants avec un algorithme de notation précis et complet.
- Doit pouvoir prendre en charge la liste des URL approuvées (liste blanche) et bloquées (liste noire).
- Doit pouvoir bloquer les tentatives de connexion pour commander et contrôler les serveurs (C&C).
- Doit être en mesure de prendre en charge les listes d'adresses IP approuvées (liste blanche) et bloquées (liste noire).
- Capable de protéger l'ordinateur contre le cryptage et la modification non autorisés.
- Capable de bloquer les processus généralement associés aux ransomwares.
- Capable de sauvegarder et de restaurer automatiquement le fichier modifié par un ransomware.
- Doit avoir une capacité de surveillance du comportement pour surveiller en permanence les points finaux pour des modifications inhabituelles du système d'exploitation, des documents liés au travail ou sur l'application installée.

- La solution doit être en mesure d'empêcher l'accès aux fichiers malveillants avec un algorithme précis et complet correspondant à la valeur de hachage de la somme de contrôle MD5 basée sur l'intelligence des menaces.
- Doit être en mesure de prendre en charge l'exclusion de scan pour les fichiers approuvés (liste blanche), l'extension de fichier et le répertoire.
- La solution doit disposer d'une technologie d'apprentissage automatique qui fournit une protection multicouche pour la pré-exécution et l'exécution (exécution) des logiciels malveillants.
- Capable de bloquer les tentatives de résiliation des processus et services associés à l'agent du fournisseur.
- Capable de bloquer les tentatives de modification, de suppression ou d'ajout de nouveaux registres associés à l'agent du fournisseur.
- Doit prendre en charge la prévention automatisée des épidémies virales avec les capacités suivantes :
    - Reçoit des recommandations de politique spécifiques aux attaques de la console de gestion d'entreprise et distribue la politique aux autres serveurs gérés.
    - Capable d'annuler le partage de dossiers.
    - Capable de configurer l'accès à " lecture seule ".
    - Capable de bloquer certains ports TCP / UDP ou une plage de ports.
    - Capable de bloquer l'accès par nom (s) de fichier.
- Capable d'empêcher d'autres programmes ou utilisateurs de désinstaller, de modifier ou de supprimer les fichiers du fournisseur.
- La solution doit protéger les terminaux contre les vulnérabilités exploitables du réseau ciblant le système d'exploitation des terminaux.
- Doit réduire l'exposition aux risques dus aux patchs manquants.
- La solution proposée est capable de fournir des fonctionnalités de correctif virtuel sans empreinte d'agent supplémentaire ni intégration tierce.
- La solution doit fournir au client une option de priorité de performance et de sécurité qui convient à ses exigences et à son environnement de sécurité.
- Sera capable de bloquer les exploits de vulnérabilité connus et inconnus.
- La solution proposée est capable de fournir des fonctionnalités DLP sans empreinte d'agent supplémentaire ni intégration tierce.
- Le DLP intégré assure la protection des données du client, qui comprend les fonctions suivantes :
    - Protège les données privées - sur ou hors réseau ;
    - La capacité de contrôle avancé des appareils protège contre les fuites de données via des clés USB et d'autres supports ;
    - Couvre la plus large gamme d'appareils, d'applications et de types de fichiers ;
    - Aide à la conformité avec une plus grande visibilité et application. Par exemple : GDPR, PCI / DSS, PII, GLBA, HIPAA, PDPA, ISMS, etc. ;
    - Le DLP intégré sera en mesure de prendre en charge la même politique sur différentes solutions de sécurité telles que la passerelle Web / Mail, l'Exchange, les points de terminaison, etc.
- Doit prendre en charge l'option de justification de l'utilisateur en cas de violation des stratégies DLP.
- Doit avoir des modèles DLP personnalisables, une option pour importer et exporter des identificateurs de données et ajouter une expression DLP.
- La configuration du contrôle d'accès aux périphériques doit être effectuée de manière centralisée à partir de la console de gestion.
- Capable d'afficher un message de notification sur l'ordinateur client en cas de violation.
- Capable de consigner la violation du contrôle des périphériques.
- Autoriser l'ajout d'appareils de confiance.

- Doit pouvoir restreindre l'accès aux terminaux sur les terminaux en attribuant des droits d'accès en lecture, en lecture / écriture, en écriture et en refus. Les équipements pouvant être restreints doivent inclure les éléments suivants :
  - Périphériques de stockage USB (également capable de désactiver l'exécution automatique) ;
  - Partages réseau ;
  - CD / DVD ;
- Capable d'isoler le point de terminaison lorsque la prévention des épidémies est invoquée.
- La solution doit prendre en charge le chiffrement de fichiers et de bureau complet.
- Doit prendre en charge le cryptage complet du disque End Point avec la capacité d'authentification pré-démarrage.
- La possibilité pour l'utilisateur de crypter des fichiers ou des dossiers spécifiques à l'aide de divers types de clés (locale, partagée, basée sur un mot de passe ou un certificat).
- Possibilité d'appliquer le cryptage sur les données qui correspondent aux règles DLP.
- Possibilité d'appliquer le cryptage sur les données écrites sur USB.
- Capable de bloquer l'exécution de logiciels malveillants à l'aide de politiques de verrouillage, de liste blanche et de liste noire personnalisables.
- La solution proposée est capable de fournir des fonctionnalités de contrôle des applications sans empreinte d'agent supplémentaire ni intégration tierce.
- Doit être capable de corréler les données de millions d'événements d'application pour identifier les menaces et maintenir une base de données à jour des applications validées.
- Doit prendre en charge le système d'exploitation suivants :
  - Windows client (32-bit / 64-bit) et Windows Server
  - Linux
- Les données de télémétrie des endpoints doivent contenir des informations sur les activités du compte, les communications réseau, les modifications du système de fichiers, les modifications du registre, entre autres types de données.
- La solution doit prendre en charge les règles de l'IOC et de YARA qui permettent la création, le partage et la réutilisation des informations sur les menaces existantes.
- La solution doit pouvoir exécuter une analyse IOC dans une base de données de télémétrie des endpoints collectée centralisée.
- La solution doit pouvoir forcer l'exécution de l'analyse IOC sur tous les hôtes avec des agents installés.
- La solution EDR doit utiliser les technologies Machine Learning sur le site pour détecter les comportements très suspects.
- La solution doit pouvoir mettre fin à un processus (ou fichier) en cours ou isoler un point de terminaison comme action de réponse à une enquête d'attaque en cours.
- La solution EDR doit permettre d'isoler la machine du reste du réseau en cas d'urgence, tout en préservant une communication contrôlée avec les serveurs d'administration et de contrôle des agents.
- La solution EDR doit fournir un moyen de résolution des incidents à distance via un agent (suppression de fichiers, suppression des processus, prévention de l'ouverture de fichiers particuliers, etc.).
- Roll-Back: Remédier les attaques et revenir à l'état précédent de confiance, Exemple : restauration des fichiers qui ont été cryptés suite à une attaque CryptoLocker.
- Visualisation de l'historique de l'attaque : cartographier depuis le point d'origine jusqu'à l'évolution de l'attaque.
- La solution doit offrir à la fois EDR et une plate-forme de protection des points de terminaison (anti-malware, réputation de sites Web, contrôle des périphériques, DLP intégré, apprentissage automatique, analyse du comportement, soumission Endpoint Cloud Sandbox, patching virtuel pour les points de terminaison via HIP et contrôle des applications, Endpoint FW) en un seul agent.

- La solution doit être en mesure de mettre fin à un processus (ou fichier) en cours d'exécution ou d'isoler un point de terminaison comme action de réponse à une enquête d'attaque en cours.
- La solution doit effectuer l'enregistrement des vecteurs couramment associés aux attaques ciblées, aux exécutions de fichiers, aux modifications de registre, etc.
- La solution doit enregistrer les métadonnées EDR dans la base de données centralisée de tous les fichiers, activités et ressources systèmes importants, et met à jour en permanence cette base de données pour enregistrer l'arrivée et l'exécution d'objets suspects.
- La solution doit fournir des capacités d'enquête sur les menaces.
- La solution doit fournir une investigation personnalisée des terminaux. La solution doit prendre en charge les règles IOC et YARA qui permettent la création, le partage et la réutilisation des informations existantes sur les menaces.
- La solution doit prendre en charge la surveillance des fichiers et des comportements. Les utilisateurs peuvent définir et télécharger leurs propres règles IOC pour spécifier les fichiers et les événements à surveiller.
- La solution doit pouvoir s'intégrer et faire partie de la stratégie de défense contre les menaces connectée à la solution existante.
- La solution devrait tirer parti du réseau mondial de renseignements sur les menaces grâce à l'utilisation de règles du IOC régulièrement mises à jour pour fournir une protection contre les dernières menaces.
- La solution doit pouvoir effectuer des recherches à plusieurs niveaux et des investigations peuvent être menées en fonction de chacun, des paramètres ou objets IOC, des fichiers OpenIOC et des fichiers YARA. Les paramètres de recherche doivent inclure :
  - Communications : IP, port, domaine, DNS
  - Logiciel malveillant ou tout fichier par : hachage Sha1, nom de fichier, chemin de fichier, type de fichier
  - Activité du registre
  - Activité du compte utilisateur
- La solution doit pouvoir obtenir des informations sur les menaces à partir des flux de menaces publics.
- La solution doit être en mesure de partager les informations sur les menaces entre les produits ou appareils gérés.
- La solution doit être capable de partager des informations sur les menaces avec des produits ou services tiers intégrés tels que les systèmes SIEM.
- Les renseignements partagés sur les menaces doivent être compatibles avec la norme publique STIX.
- La solution doit pouvoir se connecter au serveur TAXII pour obtenir des renseignements sur les menaces.
- La solution doit pouvoir agir comme un serveur TAXII et partager des informations sur les menaces avec les clients TAXII abonnés.
- La solution doit être en mesure de fournir une API Web telle que l'API Restful pour le partage de renseignements sur les menaces et l'intégration avec les automatisations des opérations de sécurité.
- Les renseignements sur les menaces partageables doivent inclure au moins 4 types : IP, URL, domaine et somme de contrôle de fichier.
- La solution doit permettre aux utilisateurs de définir des renseignements personnalisés sur les menaces, y compris l'IP, l'URL, le domaine et la somme de contrôle des fichiers, et de les déployer sur des produits / appareils gérés.
- La solution doit permettre aux utilisateurs de définir des renseignements personnalisés sur les menaces en important / exportant des règles YARA.
- La solution doit permettre aux utilisateurs de définir des informations personnalisées sur les menaces en important / exportant STIX.
- La solution doit permettre aux utilisateurs de définir une liste d'exceptions globale à exclure.

- La solution doit pouvoir exporter des informations sur les menaces vers un serveur Syslog externe.
- La solution doit produire une détection des menaces haute-fidélité et aider le SOC à prioriser la réponse aux menaces.
- Capacité à remonter le temps en analysant les données historiques et en identifiant le patient Zero.
- Identifiez facilement le point d'entrée d'une attaque.
- Possibilité d'identifier tous les hôtes infectés par la même menace.
- Possibilité d'identifier tous les hôtes qui se sont connectés au serveur C&C malveillant.
- La solution proposée doit être hautement disponible pour une protection continue des endpoints.

Logs et reporting :

- La solution doit fournir des filtres de recherche granulaires dans les journaux pour que les utilisateurs définissent leurs propres critères de recherche.
- Les fonctions d'investigation doivent inclure des données historiques d'au moins un mois de tous les évènements de point de terminaison principal (télémétrie) pour déterminer les changements survenus.
- Possibilité d'afficher dans une seule vue l'ensemble du cycle de vie des attaques par menaces.
- La solution doit avoir un rapport d'analyse des causes profondes (RCA) visualisé et une explication des objets suspects.
- La solution doit disposer de tableaux de bord interactifs pour afficher et analyser les activités du système au fil du temps, évaluer les calendriers d'activité à l'échelle de l'entreprise et exporter les résultats des enquêtes.

Administration :

- La solution EDR doit pouvoir être géré à partir d'une console d'administration on-premise.
- La solution doit fournir une console de gestion unique et centralisée pour une gestion plus efficace de tous les composants de protection dans le paysage des menaces en constante évolution.
- La solution doit fournir des fonctions de gestion centralisée des journaux collectés à partir des produits / appareils gérés.
- Panneau de verre unique pour tous les contrôles et produits de sécurité de la suite.
- La solution doit être gérée via une console Web.

Intégration :

- Capable de s'intégrer aux solutions de supervisons SIEM.
- Permettre aux programmes tiers de s'intégrer à la solution via une interface de programmation d'application (API).

Déploiement :

- La solution doit supporter le mode de déploiement on-premise.
- Déploiement facile de l'agent à l'aide de diverses procédures prises en charge (par exemple, installation Web, script de connexion, package d'installation de l'agent, installation à distance de Windows, disque client, Microsoft System Center Configuration Manager, etc.).

Fonctionnalités protection des serveurs :

- La solution doit avoir une console de gestion centralisé pour l'ensemble de ces agents.

- La solution doit accélérer et simplifier la préparation des audits et accompagne les initiatives internes de mise en conformité pour améliorer la visibilité sur l'activité du réseau interne.
- La solution doit intégrer la sécurité au processus DevSecOps grâce à des API pour améliorer les cycles de développement et réduire les risques et les interactions humaines.
- La solution devrait fournir un contrôle anti-malware amélioré et un scanning des ransomwares avec une surveillance du comportement.
- La solution devrait contenir des fonctionnalités de sécurité complètes, y compris des logiciels anti-malveillants avec une réputation sur le Web, un pare-feu basé sur l'hôte, une détection / prévention des intrusions, une surveillance de l'intégrité, une inspection du journal et des certificats SSL globalement fiables.
- La solution devrait protéger des vulnérabilités connues et inconnues dans les applications et les systèmes d'exploitation.
- La solution doit envoyer des alertes et déclencher une prévention proactive lors de la détection d'activités suspectes ou malveillantes.
- La solution devrait suivre la crédibilité du site Web et protéger les utilisateurs des sites infectés par l'intelligence de la menace de réputation sur le Web à partir de la base de données de réputation de domaine global.
- La solution devrait identifier et bloquer les botnets, attaques ciblées et communications Command & Control en utilisant la base de données de réputation de domaine global de l'intelligence de menace unifiée.
- La solution devrait assurer une efficacité opérationnelle améliorée avec un agent intelligent plus léger et plus dynamique qui facilite le déploiement afin de maximiser l'allocation des ressources.
- La solution devrait simplifier l'administration avec une gestion centralisée à travers les produits de sécurité des fournisseurs. Le reporting centralisé des contrôles de sécurité multiples réduit le défi de créer des rapports pour des produits individuels.
- La solution devrait fournir des rapports d'audit qui documentent les attaques empêchées et le statut de la politique de conformité.
- La solution devrait être en mesure d'effectuer une évaluation de la vulnérabilité du serveur qu'elle protège en utilisant des fonctions d'analyse de recommandation qui identifient les vulnérabilités connues, puis applique automatiquement les règles de protection appropriées.
- La solution doit supporter le mode de déploiement on-premise.
- La solution doit prendre en charge des évènements de sécurité détaillée au niveau du serveur qui seront fournis à un système SIEM.

<u>Anti-malware avec web réputation :</u>

- Fournir un agent anti-malware pour étendre la protection aux serveurs.
- Protéger des attaques sophistiquées dans des environnements en isolant les logiciels malveillants des composants critiques du système d'exploitation ainsi que ceux de sécurité.
- S'intégrer au réseau global de renseignement de menaces pour les capacités de réputation Web qui renforcent la protection des serveurs.
- La possibilité de décharger le traitement de protection de sécurité sur un serveur dédié et sécurisé.
- Une protection Anti-malware complète est requise qui doit assurer au minimum :
  - Toutes les actions standard, par exemple : pass, repair, quarantine, delete/remove, ...
  - Real-time scanning, on-demand et scheduled scan.
  - Possibilité de fournir des exceptions pour des emplacements spécifiques à l'intérieur du serveur ou des exceptions générales de type de fichier / dossier.
  - Détection pour virus, spywares, chevaux de Troie, ...

- La détection doit reposer non seulement sur les signatures conventionnelles, mais aussi sur la réputation et les technologies de détections multiples.

Patch virtuel :

- Fournir un correctif virtuel qui protège les systèmes vulnérables qui attendent un patch de sécurité.
- Avoir des règles de vulnérabilité pour protéger les vulnérabilités connues d'un nombre illimité d'exploits.
- Bloquer automatiquement les vulnérabilités récemment découvertes en quelques heures.
- La solution proposée doit être en mesure d'effectuer une évaluation des vulnérabilités du serveur qu'elle protège en utilisant des fonctionnalités d'analyse de recommandation qui identifient les vulnérabilités connues, puis applique automatiquement les règles de protection appropriées.
- La solution doit supporter la protection des vulnérabilités pour les OS end of support et OS end of life.

Prévention des intrusions :

- Examiner tout trafic entrant et sortant pour les écarts de protocole, les violations de la politique ou le contenu qui signale une attaque.
- Assurer une protection automatique contre les vulnérabilités connues mais non corrigées en les protégeant virtuellement d'un nombre illimité d'exploits, en poussant la protection à des milliers de serveurs en quelques minutes sans redémarrer le système.
- Assurer la défense contre l'injection SQL, les scripts entre sites et d'autres vulnérabilités d'applications Web.
- Fournir une protection de vulnérabilité prête à l'emploi pour tous les principaux systèmes d'exploitation et plus de 100 applications, y compris la base de données, le Web, le courrier électronique et les serveurs FTP.
- Fournir une visibilité et un contrôle accrus sur les applications qui accèdent au réseau.
- Offrir la possibilité de fournir une inspection des paquets en profondeur.
- Fournir un ensemble recommandé de règles IPS en fonction des correctifs de sécurité manquants (par hôte) et en fonction des services installés et actifs.
- Les règles IPS doivent être autorisées dans un mode de détection plutôt que comme un comportement exclusif.

Pare-feu hôte bidirectionnel :

- Inclure un firewall stateful bidirectionnel d'entreprise offrant une gestion centralisée de la stratégie de pare-feu, y compris des modèles prédéfinis.
- Assurer l'isolation des serveurs.
- Filtrage (adresses IP et MAC, ports).
- Couverture de tous les protocoles basés sur IP (TCP, UDP, ICMP, GGP, IGMP, etc.) et tous les types de trames (IP, ARP, etc.).
- Empêche les attaques de déni de service et détecte les scans de reconnaissance.
- Politique de conception par interface réseau.
- Diminuer la surface d'attaque des serveurs avec un filtrage granulaire, des règles par réseau et la géolocalisation, pour tous les protocoles IP et les types de trames.

- Fournir une gestion centralisée des pares-feux du serveur, y compris des modèles pour les types de serveurs courants.
- La solution doit fournir des fonctionnalités de pare-feu basées sur l'hôte pour contrôler les services réseau entre les serveurs du même VLAN, et il est nécessaire d'avoir des capacités de pare-feu détachées.
- Loguer les évènements du pare-feu, facilitant ainsi le reporting de conformité et d'audit.

Contrôle d'intégrité :

- Être capable de fournir la surveillance de l'intégrité des fichiers, des systèmes et des applications.
- Surveiller le système d'exploitation critique et les fichiers d'application, tels que les répertoires, les clés de registre et les valeurs, pour détecter et signaler les changements malveillants et inattendus en temps réel.
- La solution proposée devrait fournir une surveillance de l'intégrité du fichier et des capacités de surveillance de l'intégrité du système, par exemple surveiller les changements du système, des fichiers et des dossiers.
- Le système a la possibilité de créer des règles personnalisées pour la surveillance de l'intégrité du système / fichier.
- La solution proposée devrait prendre en charge les plateformes OS suivantes pour la surveillance de l'intégrité :
  - Oracle Solaris.
  - Linux Enterprise Servers (Red Hat, Ubuntu).
  - Microsoft Windows.
- Prise en charge de la surveillance de l'intégrité en temps réel ainsi que l'intégrité planifiée et les balayages à la demande.
- Alertes / notifications pour violation de la politique.
- La solution devrait comporter un ensemble prédéfini de règles de surveillance de l'intégrité "meilleures pratiques" mises à jour périodiquement.
- Possède une capacité intégrée pour marquer automatiquement les évènements d'intégrité connus afin de réduire les faux positifs, par exemple évènements d'intégrité générés par les déploiements de correctifs de sécurité.
- Réduire les charges d'exploitation avec la définition d'évènements de confiance, qui entrainent une exécution automatique d'actions prédéfinies sur l'ensemble du data center.
- Proposer un système de liste blanche automatique d'évènements de confiance.

Inspection des logs :

- Recueillir et analyser les logs applicatifs et du système d'exploitation dans plus de 100 formats de logs, pour identifier les comportements suspects, ainsi que les évènements de sécurité et d'administration sur l'ensemble du data center.
- Transmettre les évènements vers des systèmes SIEM à des fins de corrélation, de reporting et d'archivage.
- Avoir la possibilité de fournir l'inspection du journal.
- Supporter des pistes d'audit, par exemple les modifications effectuées par les administrateurs sur la solution de sécurité et le serveur lui-même.

- Permettre de créer des rôles de sécurité à accès multiples (pour les administrateurs, les auditeurs, les ingénieurs de sécurité informatique, ...).
- Le système doit disposer d'une fonction de journalisation et d'enregistrement intégrée.
- La solution proposée devrait prendre en charge plusieurs bases de données pour stocker des configurations / logs / évènements / rapports (Oracle Database, Microsoft SQL ...).
- Le gestionnaire de système (Console de gestion) doit prendre en charge le déploiement dans un environnement Microsoft Windows ou Linux.
- Fournir un tableau de bord interactif.
- Avoir la possibilité d'automatiser la recherche de recommandations pour toutes les couches de protection (par exemple IPS, Integrated Integrity Monitoring, Log Inspection ...).

Console de management :

- La solution proposée doit avoir un tableau de bord pour afficher plusieurs informations.
- Le tableau de bord doit être configuré par l'administrateur pour afficher les informations requises uniquement.
- La solution proposée doit disposer d'un système de gestion basé sur le Web permettant aux administrateurs d'accéder à l'aide de navigateurs Web. La Solution devrait offrir une gestion complète pour tous les serveurs.
- Le console de gestion doit fournir une section "Alertes" pour afficher les notifications à destination des administrateurs de la solution concernant les évènements système et de sécurité.
- Assurer un mécanisme d'envoi d'alertes et de notifications en temps réel par mail.
- Fournir des évènements de pare-feu pour afficher les activités sur les serveurs protégés avec le pare-feu activé (généralement inclus les paquets abandonnés ou enregistrés).
- Fournir l'accès aux évènements DPI (Deep Packet Inspection) pour voir les activités DPI liées à la sécurité. La section devrait afficher les exploits détectés, soit entrainant un trafic abandonné (Mode Prévention), soit la consignation des évènements (Mode Détection).
- Fournir des évènements système pour afficher un résumé des évènements liés à la sécurité, principalement pour le serveur de gestion et incluant également les évènements du système des agents. Toutes les actions administratives devraient être vérifiées dans les évènements du système.

Article 32: Protection des données personnelles de LPEE

Conformément aux dispositions de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, le prestataire de services s'engage à prendre les mesures adéquates concernant la protection des données personnelles dont il a accès, eu égard aux obligations de sécurité et de confidentialité imposées à LPEE désigné par ladite loi comme responsable de traitement, incombant également au Prestataire , en suivants la loi n" 09-08 précitée.

LPEE conserve la propriété pleine et entière des informations mises à disposition ou accessibles au Prestataire. En aucun cas le présent contrat n'emporte transfert du droit d'utiliser, de publier ou de reproduire, au profit du Prestataire les informations qui lui auront été communiquées par le Responsable de traitement.

Le Prestataire et son personnel s'engagent à considérer comme « confidentielles », et entrant dans le champ d'application du secret professionnel auquel ils seront tenus, les informations de toute nature,

écrites ou orales, qu'ils seraient amenés à connaître durant l'exécution du contrat. L'obligation de confidentialité du Prestataire continuera après expiration des présentes, aussi longtemps que lesdites informations n'auront pas été rendues publiques par le Responsable de traitement.

Article 33: Etude et architecture

Le prestataire devra réaliser une étude de l'environnement à sécuriser afin de concevoir une architecture cible répondant aux exigences. Cette phase comprendra :

- L'analyse des besoins en matière de protection des Endpoint (postes de travail, serveurs, postes nomades, etc.) ;
- La définition des prérequis techniques (OS supportés, intégration avec AD, SIEM, Mail, etc.) ;
- La conception de l'architecture cible, incluant :
  - Positionnement adéquat des composants dans l'architecture globale ;
  - Les flux réseau requis pour la communication entre les différents composants de la solution (agent-console, mises à jour, etc.) ;
  - Le scénario de déploiement on-premise.
- La définition des stratégies de protection, de détection et de réponse à mettre en place par type d'Endpoint ;
- La rédaction et la remise des livrables suivants :
  - Document d'architecture et d'ingénierie
  - Plan de recette qui définit les scénarios de tests à réaliser ainsi que les critères de réussite.

Ces livrables devront être soumis pour validation au LPEE avant la phase d'installation, et serviront de base pour la configuration effective.

Article 34: Installation et configuration de l'environnement

Le prestataire de services procédera à l'installation complète des composants de la solution EDR et sa configuration selon les bonnes pratiques de sécurité et conformément à la conception définie en phase d'étude et architecture. Cette prestation inclura au minimum :

- L'installation et paramétrage complet de la solution centralisée EDR
- Installation du serveur de gestion/console d'administration en mode local (on-premise) au sein de l'infrastructure de LPEE.
- Déploiement des agents EDR sur les terminaux cibles (postes de travail et serveurs).
- La configuration des politiques de protection et de détection ;
- La mise en place des réponses automatiques (isolement, blocage, remédiation, etc) ;
- La configuration des mises à jour de signatures et moteurs de détection ;
- Le paramétrage des logs, alertes, notifications et intégration avec les outils existants (SIEM, AD, messagerie, etc.).
- La mise en œuvre de la haute disponibilité (HA) ;
- La création des comptes utilisateurs pour d'administration et la supervision en fonction de la matrice d'habilitation arrêtée ;
- La sauvegarde des configurations finales validées ;
- La documentation complète pour l'administration et l'exploitation de la solution EDR.

Article 35: Tests et recette

Une phase de validation complète devra être menée, incluant au minimum :

- Les tests de détection d'événements (fichiers malveillants, comportements anormaux, tentatives d'exploitation) ;
- La simulation de scénarios de compromission pour valider la réactivité de la solution et vérifier la bonne exécution des réponses automatiques (blocage, alerte, isolement, etc.) ;
- Les tests d'intégration avec les composants existants (SIEM, AD, Mail, etc.),
- Les scénarios de basculement HA ;

Article 36: Maintenance et Support

Le prestataire de services assure la maintenance corrective, évolutive, et le support technique de la solution EDR durant la durée du marché.

Le prestataire s'engage à fournir les mises à jour des logiciels et correctifs durant la durée du marché.

Article 37: Formation et transfert de compétences

- L'attributaire doit proposer une formation d'une durée minimale, portant sur l'administration et l'utilisation de la solution, basée sur le cours officiel de l'éditeur, pour un groupe ne dépassant pas 5 personnes.
- Le soumissionnaire doit fournir toutes les informations concernant la prestation de formation : lieu, durée, modules dispensés, les supports de formation, les LABs, etc.
- Le soumissionnaire doit fournir le CV ainsi que la certification relative au produit de la personne chargée de dispenser la formation.
- Le soumissionnaire doit prévoir un transfert de compétences tout au long de l'installation, afin d'assurer l'autonomie des équipes internes dans l'exploitation et la gestion de l'infrastructure déployée.

Article 38: Documents à remettre au maître d'ouvrage

Le prestataire de services doit fournir la documentation technique requise pour l'utilisation de la solution fournis. De plus, le prestataire devra remettre les livrables suivants dans le cadre du projet :

- Un document relatif à l'étude de déploiement de la solution.
- Un document d'installation et de configuration.
- Un document d'ingénierie détaillant le scénario de déploiement.
- Un document d'administration et d'exploitation de la technologie déployée.
- Un document de recette présentant les tests réalisés.
- Support de formation.

Article 39: **Définition des prix**

Prix N° 1 : FORNITURE ET DEPLOIEMENT D'UNE SOLUTION DE PROTECTION ANTIVERALE AVEC MODULE DE EDR

Ce prix rémunère la fourniture et le déploiement de la solution de protection antivirale avec module EDR, Selon les spécifications du présent marché y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....*(F)*

Prix N° 2 : FORMATION ET TRANSFERT DE COMPETENCE

Ce prix rémunère la Formation et transfert de compétences selon les spécifications du présent marché, y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....(F)

BORDEREAU DES PRIX – DETAIL ESTIMATIF

LOT 1 : FORNITURE ET DEPLOIEMENT D'UNE SOLUTION DE PROTECTION ANTIVERALE AVEC MODULE DE EDR EN LOT UNIQUE

N° de prix	Désignation	Unité	Quantité	Prix unitaire en DH/HT	Prix total en DH/HT
1	Fourniture et déploiement d'une solution de protection antivirale avec EDR	F	1		
2	Formation et transfert de compétences	F	1		
MONTANT TOTAL HT					
TVA (20%)					
MONTANT TOTAL TTC					

Fait à ……, le …….

(Signature et cachet du prestataire de services)

DERNIERE PAGE

APPEL D'OFFRES OUVERT SUR OFFRES DE PRIX N°80/2025

OBJET : FOURNITURE, ET DEPLOIEMENTS D'UNE SOLUTION DE PROTECTION ANTIVIRALE AVEC MODULE EDR EN LOT UNIQUE

POUR UN MONTANT DE (*en chiffres et en lettres*) : .....

Le Prestataire de services	Le Maître d'ouvrage
Nom et qualité du signataire Lu et approuvé *(mention manuscrite)* Cachet et signature	**DOSI** **N. BENHACHEM** Directeur de l'Organisation et Systèmes d'Information **DLAAP** **PRESENTE PAR : F. OUTERGA** **VERIFIE PAR : H. SARJANE** **VALIDE PAR : A. ABOUFARISS** **LA DIRECTION GENERALE DU LPEE**

L.P.E.E - Casablanca - Tél: 05 22.54.75.00 Fax: 05 22.30.15.50 - 25, Rue d'Azilal - 1986

D.L.A.A.P Achats