ROYAUME DU MAROC

MINISTERE DE LA JUSTICE

DIRECTION PROVINCIAL DE LA JUSTICE

BENIMELLAL

Avis d'achat sur bon de commande N° : BC/48/2026

Le directeur provincial de la justice à Beni Mellal procède à l 'achat sur bons de commande des prestations objet du présent avis, en application des dispositions de I 'article 91 du décret N° 2-22-431 relatif aux marchés publics.

Objet de prestation : L'ACQUISITION, L'INSTALLATION ET LA MISE EN SERVICE D'UNE SOLUTION DE DETECTION ET REPONSE SUR LES TERMINAUX (EDR) POUR LE COMPTE DE LA DIRECTION PROVINCIALE DE JUSTICE A BENI MELLAL.

Délai d'exécution : **30 jours**

Date et heure limites de réception des devis des concurrents :

23/11/2026 à 10h00.

Garantie pécuniaire : Une attestation de référence et Une caution d'un montant de 2 000,00 DH (Deux mille Dirhams) doit être déposée au bureau des marchés à la direction provinciale de la justice Beni Mellal **au plus tard** avant le 23/11/2026 à 10h00 à défaut de l'écartement de l'offre.

Consistance de Ia prestation :

N°	Désignation	Spécifications techniques	Unité	Quantité
1	**L'ACQUISITION, L'INSTALLATION ET LA MISE EN SERVICE D'UNE SOLUTION DE DETECTION ET REPONSE SUR LES TERMINAUX (EDR) POUR LE COMPTE DE LA DIRECTION PROVINCIALE DE JUSTICE A BENI MELLAL**	La fourniture d'une solution de Détection et Réponse sur les Terminaux (EDR) permettant de renforcer la sécurité du système d'information contre les cybermenaces avancées. La solution devra assurer la prévention, la détection, l'investigation et la réponse aux incidents de sécurité touchant les postes de travail, les serveurs physiques et virtuels ainsi que les environnements Cloud. La solution devra intégrer une plateforme de protection des terminaux de nouvelle génération (NGAV) associée à des fonctionnalités EDR permettant : • la détection des attaques sophistiquées • l'investigation des incidents de sécurité • l'analyse des causes racines ; • la réponse automatique ou assistée aux	**U**	**320**

		incidents ; • la réduction de la surface d'attaque ; • la protection des ressources Cloud. • L'ensemble des fonctionnalités devra être administré depuis une console centralisée accessible en mode Cloud ou On-Premise. **Protection des terminaux** La solution devra assurer la protection des : • postes de travail Windows ; • serveurs Windows ; serveurs virtuels ; • infrastructures VDI ; • charges de travail hébergées dans le Cloud. • Elle devra assurer une protection continue contre : les virus ; les ransomwares ; les chevaux de Troie ; les spywares ; les attaques "fileless" ; les exploits ; les attaques utilisant des outils légitimes du système. **Détection avancée** La solution devra intégrer plusieurs technologies de détection, notamment : • Machine Learning ; • Analyse comportementale ; • Analyse heuristique ; • Détection des comportements anormaux ; • Détection des attaques avancées (APT) ; • Détection des ransomwares. • Les mécanismes de détection devront fonctionner en temps réel. **Fonctionnalités EDR** • Collecte de télémétrie : La solution devra enregistrer les événements de sécurité des terminaux afin de permettre leur analyse. • Analyse des incidents : l'analyse de la chaîne d'attaque ; la reconstitution chronologique des événements ; la visualisation graphique des processus ; l'identification de la cause racine. • Recherche des menaces : la recherche des (IoC) , l'import des (IoC) externes et le balayage automatique des terminaux. **Réponse aux incidents** La solution devra proposer des mécanismes de réponse permettant notamment : • l'isolation d'un poste compromis ; • la suppression d'un fichier malveillant ;		

		• le blocage d'un exécutable ; • la mise en quarantaine ; • l'arrêt d'un processus malveillant ; • l'application automatique de mesures correctives ; • la propagation automatique des actions de réponse à plusieurs postes. **Gestion de la surface d'attaque** La solution devra contribuer à réduire la surface d'attaque grâce notamment à : • la gestion des vulnérabilités ; • la gestion des correctifs logiciels (Patch Management) ; • le contrôle des applications ; • le contrôle des périphériques ; • le contrôle des accès aux ressources Cloud. **Sécurité Cloud** La solution devra intégrer des fonctionnalités permettant : • la découverte des services Cloud ; • le contrôle des applications SaaS ; • le blocage des services non autorisés ; • la visibilité sur Microsoft 365 ; • la protection de SharePoint Online ; • la protection de OneDrive ; • la protection de Microsoft Teams. **Console d'administration** La solution devra disposer d'une console unique permettant : • l'administration centralisée ; • le déploiement des agents ; • la gestion des politiques de sécurité ; • le suivi des alertes ; • la génération de rapports ; • la gestion des mises à jour. • La console devra être disponible : • en mode Cloud ; • en mode On-Premise. **Automatisation** La solution devra intégrer des mécanismes d'automatisation permettant : • la réponse automatique aux incidents ; • le déploiement automatique des correctifs ; • l'automatisation des tâches récurrentes ; • la gestion centralisée des politiques.		

Investigation

La solution devra permettre à l'administrateur :

- de consulter les alertes détaillées ;
- d'analyser les événements associés ;
- d'accéder aux recommandations de remédiation ;
- d'identifier rapidement le vecteur d'attaque ;
- de suivre la propagation de la menace.

Licence

- La licence doit être d'une durée de 3 (trois) ans et au nom de DPJ de Beni Mellal
- Attestation d'authenticité et de garantie éditeur au nom de DPJ de Beni Mellal
- Chaque tribunal doit avoir sa propre clé d'activation selon la distribution mentionnée dans le tableau.
- Licence pour trois (3) ans (fichiers : clé de licence et code d'activation) Clé USB 64 GO)
- Le titulaire devra assurer l'installation, la configuration et la mise en service de l'ensemble de la solution proposée.

À ce titre, le titulaire devra notamment :

- Installer et configurer la plateforme Kaspersky Security Center (KSC) dans sa version compatible avec la solution EDR proposée.
- Réaliser le déploiement et le paramétrage de la console d'administration KSC.
- Procéder à l'ajout, à l'activation et à la gestion des licences Kaspersky Next EDR Optimum au sein de la console KSC.
- Déployer les agents de sécurité (Network Agent et Endpoint Agent) sur les postes de travail et les serveurs concernés.
- Configurer les politiques de sécurité, les tâches d'administration ainsi que les profils de protection conformément aux bonnes pratiques de l'éditeur.
- Vérifier le bon fonctionnement de la communication entre les terminaux protégés et la console d'administration.
- Effectuer les tests de validation permettant de s'assurer du bon fonctionnement de la solution, notamment la remontée des événements, la détection des menaces, les

		fonctionnalités EDR et les mécanismes de réponse aux incidents. • Remettre un rapport de mise en service détaillant les opérations réalisées, les configurations appliquées ainsi que les résultats des tests de validation. Le titulaire remettra, au minimum, les documents suivants : • Les licences logicielles et les clés d'activation ; • Les certificats ou preuves d'enregistrement des licences ; • Les guides d'installation et d'administration ; • Les documents de configuration ; • Les rapports d'installation et de mise en service ; • Les rapports des essais et des tests de validation ; • Le support technique.		

Lieu d'exécution

Le titulaire est tenu de livrer 4 clés d'activation selon le tableau suivant :

Tribunal	Quantité
Tribunal de 1ère instance de Béni Mellal	210
Direction Provinciale de la justice à Béni Mellal	60
Tribunal de Commerce Béni Mellal	50

Date et heure limites de réception des devis des concurrents :
23/11/2026 à 10h00.

Délai d'exécution de la prestation : 30 jours à compter de la date prévue par l'ordre de service prescrivant le commencement de l'exécution des prestations.

Les plis des concurrents sont déposés par voie électronique dans le portail des marchés publics accessible à l'adresse www.marchespublics.gov.ma

