epsi®
l'école d'ingénierie informatique

Pro Alterna®

CERTIFICATION PROFESSIONNELLE EXPERT EN INFORMATIQUE ET SYSTEME D'INFORMATION

BLOC 5 – Concevoir et sécuriser des solutions d'infrastructures virtualisées et cloud

Cahier des Charges de la MSPR « Intégration et maintenance d'une architecture cloud et d'un système virtualisé - gestion & administration de la mobilité "

COMPÉTENCES ÉVALUÉES :

- Assurer une veille technologique afin de garantir l'optimisation des ressources de l'infrastructure du système d'information et préconiser des solutions innovantes au comité de direction / directions métiers.
- Assurer la migration de l'infrastructure vers une solution virtualisée dans le cloud afin de mettre à disposition des utilisateurs une plateforme de traitements à distance.
- Concevoir des procédures et des outils de surveillance permettant de garantir la haute disponibilité des infrastructures afin de renforcer la continuité et la reprise d'activité.
- Maintenir en condition opérationnelle les infrastructures virtualisées en diagnostiquant les pannes/dysfonctionnements afin de réduire ou supprimer les interruptions de services.
- Assurer une maintenance évolutive et corrective en fonction des évolutions technologiques (changements de versions)afin de réduire les dépenses d'investissements et d'exploitation.
- Mettre en place une plateforme de communication sécurisée entre les solutions cloud en utilisant des services d'authentification et d'identification afin de veiller à la sécurité des accès aux services.
- Administrer une plateforme workplace digitale de type EMM (gestion de la mobilité d'entreprise) afin de sécuriser et gérer l'utilisation des appareils mobiles appartenant à l'entreprise.

PHASE 1 : PRÉPARATION DE CETTE MISE EN SITUATION PROFESSIONNELLE RECONSTITUÉE

- Durée de préparation :
  - *24 heures*
- Mise en oeuvre :
  - *Travail d'équipe constituée de 4 apprenants-candidats (5 maximum si groupe impair)*
- Résultat attendu-Dossier à produire par équipe :
  - Produire un dossier de synthèse répondant aux différentes attentes de l'association of Tennis Professionals.

PHASE 2 : PRÉSENTATION ORALE COLLECTIVE + ENTRETIEN COLLECTIF

- **Durée totale par groupe** : 50 mn se décomposant comme suit :
  - 20 mn de soutenance orale par l'équipe.
  - 30 mn d'entretien collectif avec le jury (questionnement complémentaire), en français.
  - Objectif : mettre en avant et démontrer que les compétences visées par ce bloc sont bien acquises.

- **Jury d'évaluation** : 2 personnes (binôme d'évaluateurs) par jury – Ces évaluateurs ne sont pas intervenus durant la période de formation et ne connaissent pas les apprenants à évaluer.

I - CONTEXTE GLOBAL ET MÉTIER

Préambule : L'entreprise choisie pour cette MSPR est fictive, les prénoms sont fictifs, toute ressemblance à un cas réel serait purement fortuite.

L'association of Tennis Professionals (ATP) a été créée en 1972 par des joueurs de tennis professionnel dans le but de défendre leurs intérêts. Depuis 32 ans, l'association organise le circuit des tournois professionnels masculins de tennis au niveau mondial appelé ATP World Tour avec plus de 64 tournois dans 31 pays.

C'est l'ATP qui supervise les tournois au niveau sportif et financier et met en place un classement des joueurs nommé « classement ATP ».

Aujourd'hui, son siège social au niveau mondial se trouve à Londres avec environ 300 salariés. ATP Americas est basé en Floride aux USA avec 50 salariés, le siège européen ATP Europe se trouve à Monaco (150 salariés), et ATP International qui couvre l'Afrique, l'Asie et l'Australie est basée à Sidney (200 salariés).

II– CONTEXTE DU SYSTEMED'INFORMATION

À la suite des récents changements de gouvernance, le nouveau bureau exécutif a voté une uniformisation de son système d'information. En effet, chaque entité possède ses propres outils, ses propres méthodes de travail et il est difficile aujourd'hui d'unifier les outils du S.I.

De plus, le nomadisme est le mode de travail numéro 1 dans la société car beaucoup de salariés sont dépêchés sur les tournois du monde entier. Aujourd'hui, il est difficile voire impossible pour ces nomades d'accéder aux outils informatiques et notamment l'application métier qui gère les résultats et les classements. De plus, concernant l'organisation des tournois, les processus de planification des matchs sont pour le moment propres à chaquetournoi : l'ATP souhaite opter pour un outil uniquehébergé à Londres.

Il est donc nécessaire pour la société de recentrer son système d'information au siège dans un premier temps, sachant qu'à moyen terme (entre 2 et 5 ans), elle souhaite externaliser dans le cloud l'essentiel de ses applications. Cependant, quelles que soient les ressources externalisées ou non, il est nécessaire de mettre en place des dispositifs techniques de continuité d'activité (PCA) ainsi qu'établir un plan de reprise d'activité (PRA).

III– EVOLUTION SOUHAITEE DU S.I ET BESOINS

À la suite des récents changements de gouvernance, le nouveau bureau exécutif a voté une uniformisation de son système d'information. En effet, chaque entité possède ses propres outils, ses propres méthodes de travail et il est difficile aujourd'hui d'unifier les outils du S.I.

De plus, le nomadisme est le mode de travail numéro 1 dans la société car beaucoup de salariés sont dépêchés sur les tournois du monde entier. Aujourd'hui, il est difficile voire impossible pour ces nomades d'accéder aux outils informatiques et notamment l'application métier qui gère les résultats et les classements. De plus, concernant l'organisation des tournois, les processus de planification des matchs sont pour le moment propres à chaquetournoi : l'ATP souhaite opter pour un outil uniquehébergé à Londres.

Il est donc nécessaire pour la société de recentrer son système d'information au siège dans un premier temps, sachant qu'à moyen terme (entre 2 et 5 ans), elle souhaite externaliser dans le cloud l'essentiel de ses applications. Cependant, quelles que soient les ressources externalisées ou non, il est nécessaire de mettre en place des dispositifs techniques de continuité d'activité (PCA) ainsi qu'établir un plan de reprise d'activité (PRA).

IV - MISSIONS ET COMPÉTENCES

Vous avez été engagés par l'ATP en tant que prestataire informatique pour réaliser dans un premier temps l'uniformisation du S.I puis pour présenter des solutions futures de migration et de délocalisation de la fonction informatique dans le cloud. Il est également indispensable de mettre en place un PCA puis un PRA sur les parties critiques du SI.

Voici les différentes composantes du projet :

Partie mise en place technique :

- Mise en place d'une infrastructure virtuelle au siège permettant d'héberger de nombreux serveurs virtuels – T1
- Mise en place d'un système d'identification uniformisé pour tous les salariésde l'ATP avec bureau virtuelreposant sur les mécanismes Active Directory et Bureau à distance – T2
- Mise en placed'une plateforme cloud de stockageet d'échanges de fichier pour le serviceinformatique avec réplication sur un site de l'ATP de votre choix pour PCA– T3
- Protection via firewall & Interconnexion réseau mondiale de tous les sites de l'ATP au moyen de tunnels VPN – T4
- Interconnexion des utilisateurs nomadesavec le siège – T5
- Mise en place d'un système de supervision et d'alerting que ce soit au niveauinfrastructure ou au niveau systèmes. – T6
- PRA : mise en place de serveurs de secours en cas d'incident majeur : serveurs A.D, DNS, plateforme de partage de fichiers, bureaux distants. – T7

Partie conseil, Veille et R&D :

- Choix du futur fournisseur de cloud et définition des procédures de migration – C1
- Choix d'une solutionde communications unifiéesUCaaS – C2
- Etude de la mise en place future d'une authentification des nomades reposant sur Azure AD ou tout autre mécanismede SSO en cloud – C3
- Rédaction d'une procédure de gestion d'incident critique et de déclenchement de PRA – C4

V - CAHIER DES CHARGES DÉTAILLÉ & LIVRABLES ATTENDUS:

A. Partie mise en place technique

Dans cette partie sont détaillés l'ensemble des éléments techniques attendus. Le livrable principal pour cette partie est une démonstration de tous les services mis en place qui aura lieu durant la soutenance.
La démonstration doit être organisée de façon que tous les points du présent cahier des charges soient validés / démontrés. Certaines missions ne nécessitent pas forcément de démonstration, le livrable attendu est alors précisé dans ce cas.

Un schéma récapitulatif est disponible en annexe de ce document.

1) Mise en place d'une infrastructure virtuelle au siège permettant d'héberger de nombreux serveurs virtuels T1

Cette mission consiste à mettre en place un hyperviseur permettant d'exécuter l'ensemble des machines virtuelles du projet.
Cet hyperviseur doit être également configuré pour simuler les différents réseaux du projet : U.K, U.S, Monaco, Australie.
Il est nécessaire que l'hyperviseur ait accès à Internet. Aucun éditeur imposé mais l'on conseille ici la suite VMware VSphere avec son hyperviseur VMWare ESXi et au besoin l'appliance VMWare VCENTER.
Le découpage de chaque site en un ou plusieurs VLANS est à réfléchir et mettre en place.
A noter qu'il est nécessaire de rajouter un site appelé « datacenter » qui simulera l'hébergeur cloud hébergeant la solution de partage de fichiers (cf mission T3)

==> Livrable attendu : point validé lors de la démonstration de la soutenance. Document écrit : schéma d'infrastructure systèmes et réseaux.

2) Mise en place d'un système d'identification uniformise pour tous les salariés de l'ATP avec bureau virtuel reposant sur les mécanismes active directory et bureau à distance T2

Chaque salarié doit s'identifier auprès d'un service d'annuaire centralisé de type Active directory. A la suite de son identification, il doit retrouver son espacede travail.
Les utilisateurs nomades (qui se connectent à partir d'un réseau extérieur à la société) ne doivent pas pouvoir récupérer leur environnement de travail sur leur poste nomade directement mais passer par un service de bureau virtuel intermédiaire : d'où la nécessité de mettre en place une solution de bureau à distance.
On conseillera ici la mise en place d'un service de bureau à distance (RDP) mais on peut partir au choix sur d'autres solutions.

Il est clair que ce service d'identification et de bureau distant se doit d'être hautement disponible.
En principe on prévoit la mise en place des serveurs A.D au siège mais le site américain désire fonctionner également avec un contrôleur de domaine local en supplément des contrôleurs existants.
Enfin, dans le cadre de la mise en place d'un PRA, l'ATP souhaite mettre en place sur le site de votre choix un serveur AD qui sera prêt à prendre le relai en cas de sinistre sur Londres.
Un service DNS doit également être mis en place, il sera lui aussi redondant.

==> Livrable attendu : point validé lors de la démonstration de la soutenance.
Haute disponibilité à démontrer pendant la démonstration notamment.

3) Mise en place d'une plateforme cloud de stockage et d'échanges de fichier pour le service informatique T3

L'équipe informatique comprend des ingénieurs ou techniciens DevOps, développeurs, administrateurs réseaux, administrateurs systèmes ainsi qu'une nouvelle équipe cybersécurité.
Le comité exécutif de l'ATP a décidé de renforcer les liens au sein du service informatique et de concevoir les nouveaux projets en y incluant chacun des corps de métier même s'il n'est pas directement concerné. C'est particulièrement le cas de l'équipe cybersécurité.

Il n'existe aucun moyen d'échanger des fichiers actuellement au sein du service si ce n'est via des répertoires de partage Windows classiques. Il est donc demandé de choisir et de mettre en place une plate-forme répondant aux besoins suivants :

- Partage de fichiers via un lien WEB
- Consultation d'un fichier en ligne via un navigateur
- Création de groupes de partage contenant des utilisateurs autorisés à s'échanger des fichiers et ayant accès à des répertoires communs
- Possibilité de consulter les fichiers en local et de les mettre à jour via un client de synchronisation.

La plate-forme est à mettre en place au sein d'un cloud. Vous simulerez ce Cloud sur votre maquette en ajoutant un réseau « datacenter » indépendant. (cf schéma annexe).

Dans le cadre du PCA, il est demandé que les fichiers soient synchronisés à intervalle de temps régulier sur le site de Londres.
On souhaite également une copie du système complet prête à être démarré sur le site PRA. (cf mission PRA T7)

==> Livrable attendu : point validé lors de la démonstration de la soutenance.

4) Protection via firewall & interconnexion réseau mondiale de tous les sites de l'atp au moyen de tunnels VPN T4

Chaque site de l'ATP doit être protégé de l'extérieur au moyen d'un firewall virtualisé qui assurera un filtrage entre le LAN et les autres sites distants ainsi qu'Internet. Vous devez mettre en place ce firewall que vous choisirez sur chacun des sites. Vous devez mettre en place les règles de firewall qui vous semblent les mieux appropriées et qui ne laissent passer que le trafic nécessaire au bon fonctionnement des applications et à la navigation Internet.

Les connexions inter-sites doivent être rendues possibles et se faire de manière sécurisée au moyen de VPN de type IPsec.

Pour le moment, la liaison avec l'hébergeur Cloud utilisera Internet (simulation d'Internet), pas besoin de mettre en place un tunnel VPN. On prévoit cependant un routeur/firewall au niveau du site datacenter.

Le site choisit pour le PRA se verra ajouter un réseau supplémentaire destiné à accueillir les copies de serveurs/les ressources qui seront mises en service en cas de déclenchement du PRA et donc d'incident majeur. (cf mission PRA T7)

==> Livrable attendu : point validé lors de la démonstration de la soutenance.

5) Interconnexion des utilisateurs nomades avec le siège T5

Un utilisateur nomade doit pouvoir être capabled'initier une connexionréseau avec le siège à partir d'Internet afin d'accéder à un bureau virtuel (mission T2).
Vous devez mettre en place une solution VPN destinée à accueillir ces connexions nomades.

==> Livrable attendu : point validé lors de la démonstration de la soutenance.

6) Mise en place d'un système de supervision et d'alerting que ce soit au niveau infrastructure ou au niveau systèmes T6

Tout serveur ou service mis en place pour chaque mission se doit d'être supervisé. Ainsi vous devez choisir et mettre en place un ou plusieurs outils de supervision et de gestion d'alertes obéissant notamment aux critères suivants :

- Supervision de la disponibilité de l'infrastructure et des serviceset dispositif d'alerte
- Métrologie du réseau
- Supervision des espacesdisques, utilisation CPU et RAM
- Centralisation des journauxd'évènements et alertesen cas d'évènement majeur ou inattendu
- Paramétrage des seuils d'alertes
- Mise en place d'un tableaude bord récapitulatif destiné au service informatique

==> Livrable attendu : point validé lors de la démonstration de la soutenance.

7) PRA : mise en place de serveurs de secours en cas d'incident majeur : serveurs A.D, DNS, bureaux distants T7

Malgré les dispositifs de continuité d'activité que vous avez mis en place : serveurs A.D Londres et USA, serveur DNS éventuel, bureaux distants, etc… La DSI souhaite mettre en place un PRA global dont le périmètre technique vous concernant consiste à prévoir la reprise d'activité via des serveurs « dormant » qui prendraient le relai sur l'existant en cas d'incident critique avéré.
Ainsi, sur un site distant que vous choisirez (sur le schéma annexe on a choisi le site de Monaco), seront mis en place des copies de données/serveurs/systèmes prêts à être mis en production en cas de déclenchement du PRA (sans un réseau isole). Il est nécessaire qu'en cas de déclenchement du PRA, il n'y ait aucun paramètres réseaux à modifier sur les serveurs/les postes de travail. Vous pouvez donc gérer la bascule au niveau du DNS et par la mise en place d'un tunnel VPN de niveau 2 entre le réseau de production de Londres et le réseau utilisé sur le site dédié au PRA. UN tunnel de niveau 2 permet de conserver le même plan d'adressage entre 2 réseaux reliés via le WAN/Internet.
On souhaite atteindre un RPO maximum de 36H et un RTO de 48H.

==> Livrable attendu : point validé lors de la démonstration de la soutenance. Déclenchement du PRA selon la procédure décrite dans la mission C4.

B. Partie conseil, Veille et R&D

1) Choix du futurfournisseur de cloud et définition des procédures de migration C1

A moyen terme, l'ATP souhaite migrer l'infrastructure du siège vers un prestataire CLOUD.
On attend ici de votre part le choix d'un prestataire cloud, des conseils permettant de peser le pour et le contre d'une telle migration pour chacun des services ainsi qu'une documentation expliquant les différentes étapes de la migration que vous prévoyez.
Vous devez prendre en compte les impératifs de haute disponibilité et de sécurité dans votre réflexion ainsi qu'une approximation globale du budget nécessaire à une telle migration, budget élaboré en différenciant CAPEXet OPEX et en incluant les coûts en main d'œuvre.
Sont à prendre en compte dans la migration, uniquement les services que vous avez mis en place.

==> Livrable attendu : document écrit professionnel dans le formalisme de votre choix

2) Choix d'une solution de communications unifiées UCaaS C2

L'ATP souhaite se d'outils facilitant le télétravail et la communication en interne. Elle souhaite acquérir ou louer un service lui permettant d'assurer les besoins suivants en termes de communication :

- Téléphonie IP via softphone
- Chat entre collaborateurs
- Visioconférence

Après avoir recensé quelques offres du marché qui pourraient correspondre à ces besoins, faites une proposition d'une solution qui répondrait au cahier des charges en mettant en avant le bien fondé d'un tel choix. Vous pouvez proposer plusieurs produits afin de couvrir l'ensemble des besoins si nécessaire.

==> Livrable attendu : document écrit professionnel dans le formalisme de votre choix. Présentation de la solution choisie lors de la soutenance oral.

3) Étude de la mise en place d'une authentification reposant sur azure ad ou tout autre mécanisme de SSO en cloud C3

L'ATP souhaite peu à peu délocaliser la fonction d'authentification chez un prestataire externe pour des raisons de sécurité et de haute disponibilité. La direction vous demande votre avis sur un tel choix et la faisabilité d'un tel projet notamment en mettant en place un mécanisme de SSO en cloud tel qu'AZURE A.D.
La direction n'est cependantpas bloquée sur le choix d'AZURE, ni sur le choix d'un prestataire exclusif qui assumerait à la fois l'hébergement, l'administration et le fonctionnement de la solution..

==> Livrable attendu : document écrit professionnel dans le formalisme de votre choix contenant notamment les prérequis et la faisabilité technique d'un tel projet. L'aspect financier n'est pas ici à prendre en compte.

4) Rédaction d'une procédure de gestion d'incident critique et de déclenchement de PRA C4

Dans la mission T7, vous êtes amenés à mettre en place un PRA concernant le cœur de l'infrastructure du SI que vous avez mis en place. Après avoir effectué une étude des principaux risques menant au déclenchement du PRA (une dizaine de risques attendus) et en les évaluant, vous rédigerez une procédure décrivant le déclenchement du PRA contenant les principales étapes techniques nécessaires pour le basculement en mode dégradé.

==> Livrable attendu : document écrit contenant un tableau des risques et leur évaluation en termes de criticité. Procédure décrivant les différentes étapes de la bascule vers le site de secours en cas de déclenchement du PRA. Cette procédure devra être suivie lors de la démonstration pour valider la mission T7

VI– CONTRAINTES

A. Matériel

La principale contrainte est de mettre en place la maquetteà l'aide d'un unique hyperviseur qui hébergera l'ensemble des machines virtuelles. Tout sera donc virtuel.
Au besoin, on pourra faire l'usagede matériels physiques comme des firewalls.

B. Logiciels

Le choix des systèmes d'exploitation pour les machines virtuelles à mettre en place est libre s'il n'est pas explicitement demandé.
La suite logicielle pour la virtualisation n'est pas imposée, cependant, nous conseillons vivement la suite VMWareVSphere.

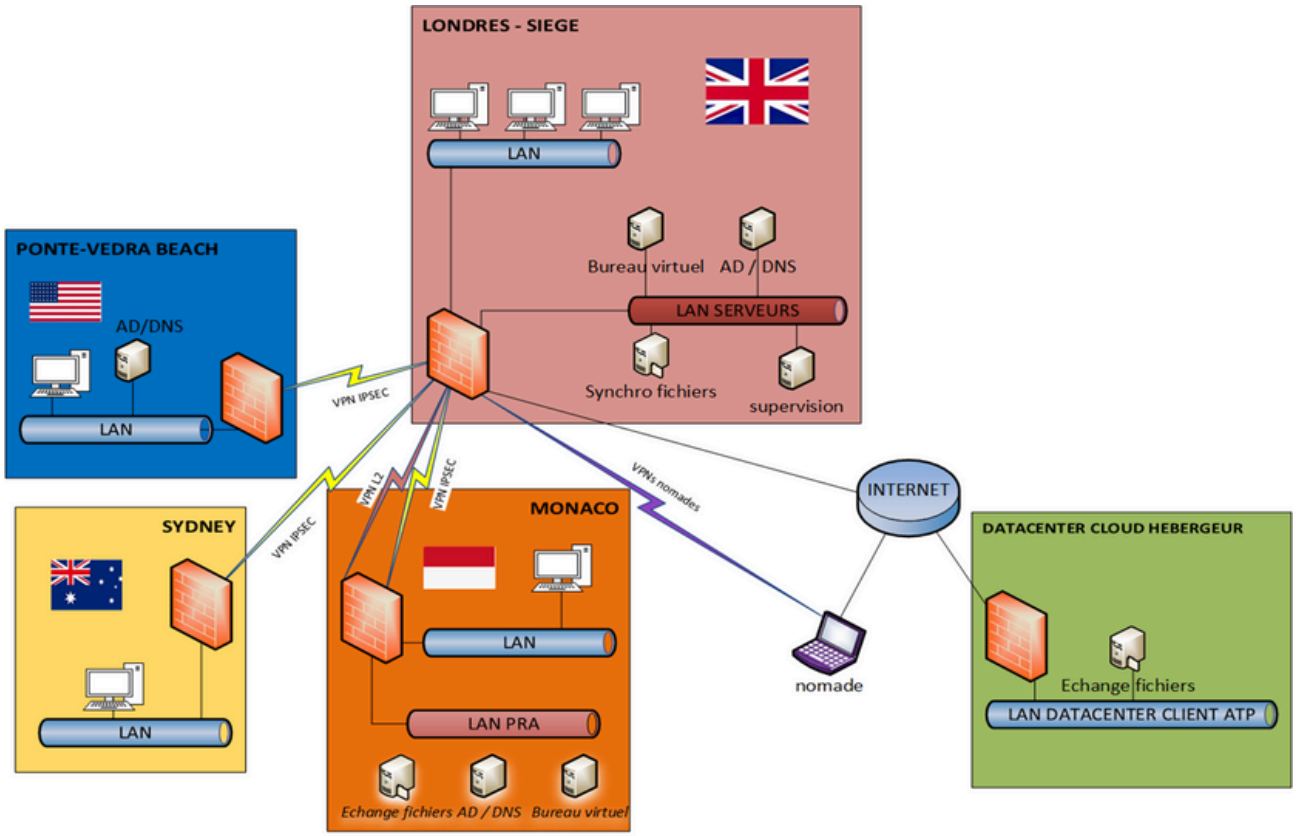
C . Temps et Organisation

La MSPR est à préparer à plusieurs au sein d'un groupe de 4 personnes maximum.
Un planning prévisionnel avec découpage en tâches et affectation de ces dernières doit être établi **le jour de la présentation du sujet ou dans la séance qui suit.**

D. Livrables

Le livrable principal attendu est une démonstration de tous les services mis en place dans le cadre de la soutenance orale. Cette dernière peut s'accompagner d'une présentation type powerpoint si c'est nécessaire notamment pour les missions C1, C2,C3 et C4, mais ce n'esten rien obligatoire.
Le livrable écrit est constitué de l'ensemble des documents rédigés tel qu'énoncé dans les missions concernées.

VII– SCHÉMA ANNEXE



Les compétences évaluées durant cette MSPR :

- Assurer une veille technologique afin de garantir l'optimisation des ressources de l'infrastructure du système d'information et préconiser des solutions innovantes au comité de direction / directions métiers.
- Assurer la migration de l'infrastructure vers une solution virtualisée dans le cloud afin de mettre à disposition des utilisateurs une plateforme de traitements à distance.
- Concevoir des procédures et des outils de surveillance permettant de garantir la haute disponibilité des infrastructures afin de renforcer la continuité et la reprise d'activité.
- Maintenir en condition opérationnelle les infrastructures virtualisées en diagnostiquant les pannes/dysfonctionnements afin de réduire ou supprimer les interruptions de services.
- Assurer une maintenance évolutive et corrective en fonction des évolutions technologiques (changements de versions)afin de réduire les dépenses d'investissements et d'exploitation.
- Mettre en place une plateforme de communication sécurisée entre les solutions cloud en utilisant des services d'authentification et d'identification afin de veiller à la sécurité des accès aux services.
- Administrer une plateforme workplace digitale de type EMM (gestion de la mobilité d'entreprise) afin de sécuriser et gérer l'utilisation des appareils mobiles appartenant à l'entreprise.