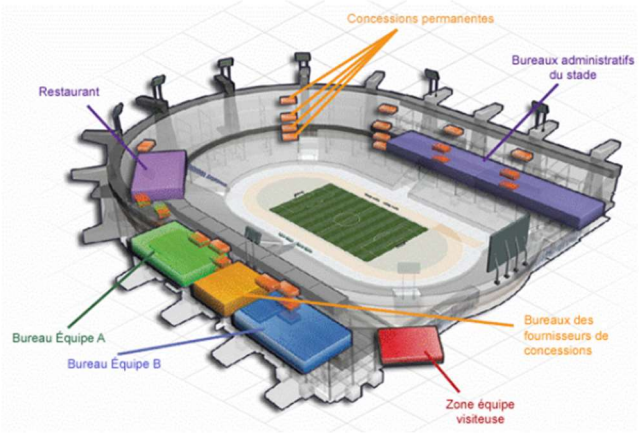
Stadium

Contexte Stadium

Stadium gère un grand stade et avait initialement mis en place un réseau de communication avancé lors de la construction. Cependant, au fil du temps, l'entreprise a ajouté de nouveaux équipements et augmenté les connexions sans tenir compte de ses objectifs commerciaux à long terme ni de la conception de son infrastructure réseau. Cela a conduit à des problèmes de bande passante et de gestion du trafic, limitant la capacité de la société à offrir des services de qualité.

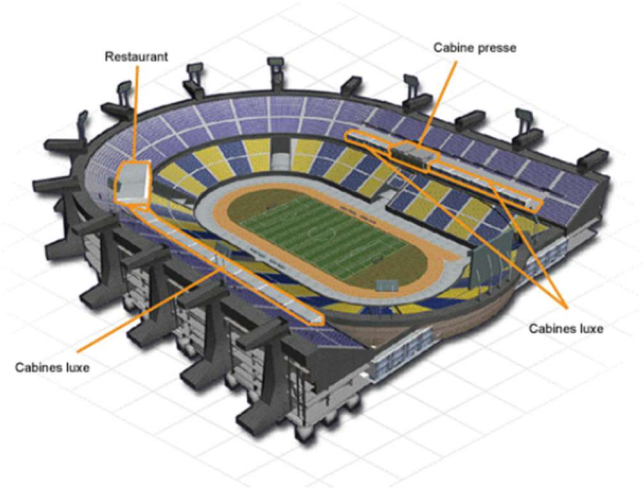
Maintenant, la direction de Stadium souhaite améliorer la satisfaction de ses clients en introduisant de nouvelles technologies et en permettant l'organisation de concerts, mais le réseau actuel ne le permet pas. Sachant qu'elle ne possède pas l'expertise nécessaire en matière de réseau, la direction a décidé de faire appel à des consultants réseau pour concevoir, gérer et mettre en œuvre ce projet en trois phases.

La première phase consiste à planifier le projet et à préparer une conception réseau de haut niveau. Pour cela, Stadium a engagé NetworkingCompany, une société spécialisée en conception de réseaux, qui a interrogé le personnel du stade pour comprendre l'organisation et les installations.

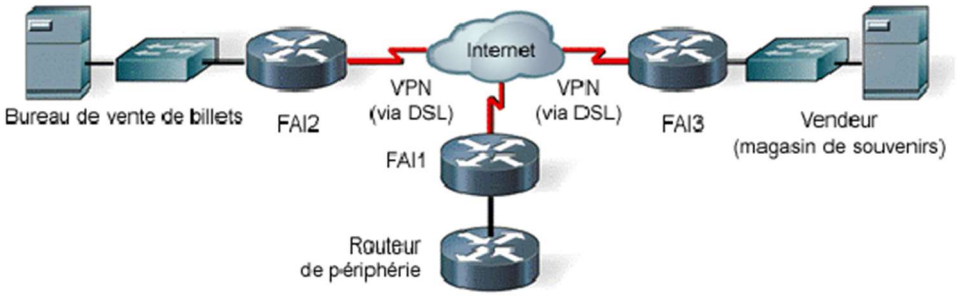


Stadium emploie 170 personnes à temps plein, dont 35 dirigeants et responsables, ainsi que 135 employés. Ils ont également recours à environ 80 intérimaires pour des événements spéciaux. Tous les employés, à l'exception des préposés au terrain et des gardiens, utilisent des PC et des téléphones connectés à un PABX vocal numérique

Stadium



Le stade propose des installations pour deux équipes sportives, une équipe visiteuse, un restaurant de luxe et un fournisseur de concessions. Il dispose également de deux sites distants, une billetterie en centre-ville et une boutique de souvenirs, connectés via DSL à un FAI local.



Le stade est construit sur deux niveaux, avec des locaux techniques reliés par des câbles à fibre optique en raison de sa grande taille. Les équipes sportives ont leurs bureaux et installations, tandis que le restaurant de luxe loue également des bureaux auprès de Stadium.

En résumé, Stadium souhaite moderniser son réseau pour répondre aux besoins actuels et futurs, et a fait appel à des experts pour le guider à travers ce processus de mise à niveau.

Stadium

Cahier des charges Stadium

Le Cahier des Charges de Stadium révèle votre intégration au sein de la division Systèmes d'Information (SI) de l'entreprise pour cette année. Votre mission centrale consistera à assumer la responsabilité de l'administration des systèmes et des réseaux informatiques. Stadium se compose de plusieurs sites distincts, chacun ayant un rôle spécifique :

1. Site 1 : Stade - Ce site est le cœur de l'entreprise, abritant l'hébergement informatique, le siège social et le centre administratif. Il est le pivot autour duquel s'articulent toutes les opérations et activités de l'entreprise.
2. Site 2 : Billetterie - Ce site est dédié à la gestion des ventes de billets, un élément essentiel pour les événements sportifs et les spectacles organisés au stade.
3. Site 3 : Magasin - Ce site est spécialement conçu pour la vente d'articles souvenirs, offrant aux fans et aux visiteurs la possibilité d'acheter des produits liés à l'équipe ou aux événements.

Le Cahier des Charges insiste sur la nécessité de documenter les différentes solutions retenues pour le projet en fonction de leur niveau de complexité. Cette approche méthodique garantira que chaque aspect de l'infrastructure informatique soit clairement spécifié et que les procédures soient consignées de manière exhaustive. Cela s'inscrit dans la vision globale adoptée par Stadium pour assurer une gestion efficace et cohérente de ses ressources informatiques.

Votre rôle au sein de cette mission sera d'une importance cruciale, car vous devrez contribuer à façonner et à maintenir l'infrastructure technologique qui soutient les opérations de 'entreprise et qui permet de répondre aux défis uniques posés par chaque site.

Mission 1 : Restructuration de l'Infrastructure de Stadium

Contexte : Cette mission vous amène à rejoindre l'équipe informatique du centre administratif de Stadium, situé au stade. Ce site occupe une position centrale dans l'entreprise, car il gère l'ensemble des opérations liées à la gestion du personnel et à l'administration du stade. Il se compose de sept services clés, chacun ayant un rôle vital dans les activités de l'entreprise :

1. Service Administration (170 collaborateurs) : En charge de la gestion administrative de l'entreprise.
2. Service Équipes (164 collaborateurs) : Impliqué dans la coordination des équipes opérationnelles.
3. Service WiFi (100 collaborateurs) : Responsable des réseaux sans fil.
4. Service Caméra IP (80 caméras) : Supervise le système de vidéosurveillance.
5. Service VIP-Presse (80 collaborateurs) : Gère les VIP et les relations avec la presse.
6. Service Fournisseurs (44 collaborateurs) : Responsable des relations avec les fournisseurs et les partenaires commerciaux.
7. Service Restaurant (14 collaborateurs) : En charge de la restauration interne de l'entreprise.

Concernant le réseau de Stadium, plusieurs exigences en matière de sécurité doivent être respectées pour garantir la solidité et la stabilité de l'infrastructure informatique. Ces exigences comprennent :

- L'utilisation d'une plage d'adresses IP spécifique (172.20.0.0/22) : Cette plage d'adresses simplifiera la gestion des noms et des ressources au sein du réseau.
- La mise en place d'un système de segmentation du réseau : Cette solution permettra de séparer différentes parties du réseau pour des raisons de sécurité et d'efficacité. Des commutateurs faciles à administrer seront utilisés pour permettre une configuration rapide et fluide de ces segments.
- La création d'une solution d'interconnexion efficace entre les différents sites : Cette solution garantira une communication optimale entre le stade, la billetterie et le magasin, favorisant ainsi une coordination sans faille des activités.
- La configuration uniforme des équipements réseau avec des équipements CISCO : Tous les commutateurs et le routeur seront configurés de manière cohérente à l'aide d'équipements réseau de la marque CISCO pour garantir une compatibilité et une gestion homogène.

Votre rôle au sein de cette mission est essentiel pour assurer le bon fonctionnement de l'infrastructure informatique de Stadium, ainsi que pour garantir la sécurité et la coordination efficace des opérations au sein de l'entreprise.

Mission 2 : Infrastructure, Configuration et Administration des Services Informatiques de Stadium

Au sein du site du stade de Stadium, l'infrastructure informatique revêt une importance cruciale pour soutenir les opérations de l'entreprise. Voici un aperçu des éléments clés en place :

1. Postes de Travail pour les Employés : Des postes de travail sont déployés pour les employés, fournissant ainsi l'accès aux ressources informatiques nécessaires à leurs activités quotidiennes.
2. Service Active Directory : Un service Active Directory est opérationnel pour gérer l'authentification des utilisateurs et la gestion des ressources du domaine **Stadium.com.** Cela permet une organisation efficace des utilisateurs par service au sein d'unités organisationnelles (UO).
3. Service DHCP : Un service DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer automatiquement des adresses IP aux postes de travail et autres périphériques du réseau.
4. Serveur DNS Primaire : Un serveur DNS primaire fonctionne sur une machine exécutant Windows Server 2022. Ce serveur est responsable de la résolution des noms de domaine au sein de l'entreprise, notamment pour le domaine Stadium.com.
5. Stockage des Fichiers Utilisateurs : La même machine hébergeant le DNS primaire est également utilisée pour le stockage des fichiers utilisateurs, facilitant ainsi l'accès aux données partagées.
6. Serveur RSync : Un serveur RSync est configuré pour la synchronisation de fichiers, garantissant la cohérence des données entre différentes ressources.
7. DNS Secondaire : Un DNS secondaire est en place, fonctionnant soit sous Linux Debian, soit sous Microsoft Server. Ce serveur agit comme une solution de secours en cas d'indisponibilité du DNS primaire, assurant ainsi la continuité des services DNS.

8. Gestion des Utilisateurs : Les utilisateurs sont regroupés par service au sein du service Active Directory, avec chaque service disposant d'un groupe d'utilisateurs au format G_xxxx. Les utilisateurs ayant des privilèges spécifiques, tels que les administrateurs de service (GP_Admin), sont également inclus. Des Objets de Stratégie de Groupe (GPO) sont utilisés pour appliquer des politiques de sécurité et d'autorisation spécifiques aux machines du réseau.
9. Authentification des Utilisateurs : Les utilisateurs sont identifiés par des logins construits à partir de la première lettre de leur prénom suivie de leur nom de famille. En cas de doublon, un chiffre de 1 à 10 est ajouté au login. Chaque utilisateur dispose d'un dossier personnel et d'un profil centralisé.
10. Politique de Complexité des Mots de Passe : Une politique de complexité des mots de passe est définie au niveau du domaine pour renforcer la sécurité des comptes.

En ce qui concerne la gestion du DNS, les serveurs sont configurés pour résoudre les zones directes (Stadium.local) et inverses (172.20.0.10). Le DNS primaire assure cette fonction sur Windows Server 2022, tandis que le DNS secondaire prend le relais en cas de besoin, garantissant ainsi la disponibilité continue du service DNS.

Pour le service DHCP, une plage d'adresses est réservée sur le réseau 172.20.0.10, avec des options de routeur et de serveurs DNS pour orienter les périphériques clients vers la passerelle/firewall et les serveurs DNS appropriés.

L'ensemble de ces configurations assure une infrastructure informatique robuste et bien organisée au site du stade de Stadium, permettant ainsi un fonctionnement efficace des services informatiques de l'entreprise.

Mission 3 : Mise en Place d'une Solution pour l'Administration à Distance Sécurisée et la Sécurisation des Interconnexions

Dans le cadre de la Mission 3, il est essentiel de mettre en place une solution robuste permettant une administration à distance sécurisée tout en renforçant la sécurité du système d'information entre les différents sites de Stadium. De plus, il est impératif de sécuriser les liaisons inter-sites, notamment entre le site du stade et les sites distants de la billetterie et du magasin. La solution sélectionnée doit permettre une administration à distance via un accès sécurisé basé sur le protocole SSH (Secure Shell).

Pour atteindre ces objectifs, voici les principales actions à entreprendre :

1. **Sécurisation du Système d'Information entre les Sites :** Il est primordial de mettre en place des mesures de sécurité appropriées pour protéger les données sensibles et les communications entre les différents sites de Stadium. Cela peut inclure la mise en œuvre de pare-feux, de mécanismes d'authentification renforcée, et la surveillance constante du trafic réseau pour détecter les activités suspectes.
2. **Sécurisation des Interconnexions :** Les liaisons réseau entre le site du stade et les sites de la billetterie et du magasin doivent être sécurisées en utilisant des technologies telles que les réseaux privés virtuels (VPN) ou des connexions chiffrées. Il est essentiel de garantir l'intégrité et la confidentialité des données transitant entre ces sites.
3. **Administration à Distance Sécurisée :** La possibilité d'administrer à distance les équipements réseau et les serveurs doit être mise en place de manière sécurisée. L'utilisation du protocole SSH pour l'accès à distance est une approche recommandée,

car il assure un chiffrement des communications et une authentification robuste. Les accès doivent être contrôlés par des mécanismes d'authentification à deux facteurs (2FA) lorsque cela est possible.

4. **Gestion des Certificats et des Identités :** Il est nécessaire de mettre en place une gestion efficace des certificats numériques et des identités pour garantir l'authenticité des connexions SSH. Les certificats doivent être régulièrement renouvelés et surveillés.
5. **Surveillance de la Sécurité :** Un système de surveillance de la sécurité doit être en place pour détecter et répondre rapidement à toute tentative d'intrusion ou d'attaque. Les journaux d'accès SSH et les alertes de sécurité doivent être suivis en temps réel.
6. **Formation du Personnel :** Il est important de former le personnel de l'entreprise à l'utilisation sécurisée des connexions SSH et à la gestion des accès à distance. La sensibilisation à la sécurité doit être une priorité.

En mettant en œuvre ces mesures, Stadium pourra bénéficier d'une infrastructure réseau plus sécurisée, d'interconnexions protégées, et d'une administration à distance fiable et sécurisée via SSH. Cela contribuera à renforcer la sécurité globale du système d'information de l'entreprise

Mission 4 : Mise en Place d'une Solution de Redondance, de Tolérance de Panne et d'Équilibrage de Charge pour les Éléments d'Interconnexion de Niveau 2 et 3

Dans le cadre de la Mission 4, l'objectif principal est de mettre en place une solution qui assure la redondance des services, la tolérance de panne et l'équilibrage de charge pour les éléments d'interconnexion de niveau 2 et 3 au sein de l'infrastructure de Stadium. Voici les principaux points à prendre en compte :

1. **Minimisation de l'Interruption de Service :** Il est impératif de réduire au maximum la durée de toute interruption de service. Cela peut être réalisé en mettant en place des mécanismes de basculement rapide (failover) en cas de panne, de manière à ce que les services restent disponibles en permanence, même en cas de défaillance d'un composant.
2. **Amélioration de la Continuité de Service en Cas de Panne :** La solution devra être conçue de manière à améliorer la continuité de service des services existants en cas de panne, que ce soit au niveau des commutateurs ou des liaisons d'accès fournies par les FAI (Fournisseurs d'Accès Internet). Cela pourrait impliquer la mise en place de chemins de secours, de configurations de basculement ou de redondance au niveau des équipements réseau.
3. **Agrégation des Liens et Augmentation de la Bande Passante :** Une partie essentielle de cette mission consiste à agréger les liens entre les commutateurs et à augmenter la bande passante globale du réseau. Cela permettra de mieux gérer la charge de trafic et d'éviter les goulets d'étranglement. Des technologies telles que le trunking Ethernet (agrégation de liens) et le routage dynamique peuvent être envisagées.
4. **Équilibrage de Charge :** Pour garantir une utilisation efficace des ressources réseau, il est nécessaire de mettre en place des mécanismes d'équilibrage de charge. Cela permet de répartir équitablement le trafic sur plusieurs liens, évitant ainsi la surcharge de certains équipements ou liaisons.

5. **Tests et Validation :** Avant la mise en production de cette solution, il est essentiel de réaliser des tests approfondis pour s'assurer qu'elle fonctionne conformément aux attentes. Les scénarios de panne doivent être simulés et évalués pour garantir la tolérance de panne souhaitée.
6. **Documentation et Formation :** Une documentation complète de la nouvelle architecture doit être élaborée. De plus, le personnel responsable de l'administration et de la maintenance du réseau devra être formé à la gestion de cette solution de redondance, de tolérance de panne et d'équilibrage de charge.

En mettant en œuvre cette solution, Stadium pourra garantir une disponibilité élevée de ses services, minimiser les interruptions de service et assurer une utilisation efficace de ses ressources réseau, tout en améliorant la résilience de son infrastructure en cas de panne.

Mission 5 : Sécurisation de l'Interconnexion du Réseau de Stadium avec Internet

Contexte : Après avoir mis en place l'architecture réseau interne du site du stade, le Directeur des Systèmes d'Information (DSI) de Stadium souhaite désormais interconnecter le réseau de l'entreprise avec Internet. Cette expansion vers Internet offre de nombreux avantages, mais elle expose également l'entreprise à de nouvelles menaces en matière de sécurité. Il est donc essentiel d'intégrer la sécurité au sein de l'architecture réseau pour réduire ces risques.

Définition du besoin : Le DSI de Stadium souhaite réaliser une étude complète des risques liés à l'accès à Internet, en prenant en compte les éléments de sécurité suivants :

1. **Mise en place d'une DMZ :** Création d'une zone démilitarisée (DMZ) contenant un ensemble de serveurs accessibles depuis l'extérieur, en particulier le serveur web.
2. **Restriction de l'accès au réseau interne :** L'environnement du réseau interne du stade doit être accessible uniquement aux acteurs de l'entreprise.
3. **Hébergement en interne des serveurs :** Les serveurs exécutant les applications et les besoins de Stadium sont hébergés en interne.
4. **Accès Internet pour les collaborateurs :** Les employés de l'entreprise sont autorisés à accéder à Internet à partir du réseau interne.
5. **Accès Internet restreint pour les utilisateurs du réseau Wi-Fi Visiteurs :** Les utilisateurs du réseau Wi-Fi Visiteurs ont un accès limité, uniquement à Internet.

Travail à réaliser : Pour répondre à ces besoins, les tâches suivantes doivent être accomplies :

1. **Identification des Risques :** Il est essentiel d'identifier les risques potentiels associés à l'interconnexion avec Internet. Cela comprend la menace de cyberattaques, d'intrusions, de fuites de données, etc.
2. **Détermination de la Démarche de Sécurité :** Élaboration d'une démarche visant à réduire ces risques. Cela inclut la mise en place de pare-feux, de systèmes de détection d'intrusions, de systèmes de prévention des intrusions, et d'autres mesures de sécurité.
3. **Définition de la Problématique de l'Accès à Internet :** Élaboration d'une stratégie de sécurité pour gérer l'accès au réseau Internet à partir d'un réseau privé, en garantissant la confidentialité, l'intégrité et la disponibilité des données.
4. **Conception de la Politique de Filtrage :** Définition d'une politique de filtrage des flux de données conformément aux exigences du cahier des charges. Cette politique devrait déterminer quels types de trafic sont autorisés ou bloqués.

5. **Adaptation de la Maquette :** Mise à jour de l'architecture réseau actuelle en fonction de la solution proposée, en intégrant les éléments de sécurité nécessaires pour garantir la protection du réseau et des données.

La réalisation de cette mission est cruciale pour assurer la sécurité de l'entreprise dans un environnement connecté à Internet, en réduisant les risques potentiels et en mettant en place les contrôles de sécurité adéquats.

Mission 6 : Implémentation d'un Réseau Wi-Fi pour les Employés et les Visiteurs au Stade

La mission consiste à mettre en place une solution d'accès Wi-Fi pour les employés du stade de Stadium, ainsi que pour les visiteurs. Les visiteurs auront un accès limité à Internet, conformément aux obligations légales.

Voici les éléments du cahier des charges concernant les accès Wi-Fi :

1. **Point d'accès par Service :** Chaque service dispose d'un point d'accès 802.11 b/g/n compatible PoE (Power over Ethernet). Un SSID non diffusé est attribué à chaque service, sauf pour le VLAN visiteur.
2. **Sécurité par WPA2, WPA3 Enterprise :** La sécurité des réseaux Wi-Fi sera assurée par la norme WPA2 Enterprise. Cela garantit une authentification robuste pour les employés.

Prérequis :

- Le système d'information d'Authentification et d'Autorisation (AAA) tel que le protocole RADIUS est opérationnel.

Modifications à effectuer :

1. **Solution d'accès Wi-Fi pour le VLAN Wi-Fi (stade-wifi) :** Pour répondre à cette exigence, vous devrez configurer les points d'accès Wi-Fi pour émettre le SSID correspondant au VLAN Wi-Fi. Les employés pourront se connecter en utilisant leurs identifiants de réseau.
2. **Solution d'accès Wi-Fi pour les Visiteurs :** Vous devrez également configurer un réseau Wi-Fi distinct pour les visiteurs. Cela peut être fait en configurant un SSID spécifique pour les visiteurs. Ils auront un accès limité à Internet uniquement.
3. **Intégration et Configuration des Switchs PoE :** Les switchs compatibles PoE doivent être intégrés dans l'infrastructure réseau. Ils devront être configurés pour alimenter les points d'accès Wi-Fi via Power over Ethernet.
4. **Intégration et Configuration des Points d'Accès Wi-Fi :** Les points d'accès Cisco compatibles devront être intégrés à l'infrastructure et configurés pour émettre les SSID appropriés et appliquer la sécurité WPA2 Enterprise.
5. **Authentification des Salariés via le Réseau Wi-Fi :** L'authentification des employés sur le réseau Wi-Fi se fera via le protocole RADIUS. Vous devrez configurer les serveurs RADIUS pour gérer cette authentification.
6. **Accès Internet pour les Visiteurs :** L'accès à Internet pour les visiteurs doit être configuré de manière sécurisée. Il peut être nécessaire de mettre en place un portail captif pour les visiteurs, où ils devront accepter les conditions d'utilisation avant d'accéder à Internet.

7. **Renforcement de l'Authentification (Phase 2) :** Comme indiqué, dans un deuxième temps, vous devrez renforcer l'authentification pour le dernier VLAN. Cela peut inclure des méthodes d'authentification supplémentaires telles que le certificat client ou des protocoles d'authentification plus avancés.

La réalisation de cette mission permettra aux employés du stade d'accéder de manière sécurisée au réseau sans fil, tandis que les visiteurs auront un accès contrôlé à Internet, garantissant la conformité aux obligations légales en matière de sécurité

Mission 7: Mise en Place d'une Solution de Gestion du Parc Informatique avec Synchronisation Active Directory, Notification des Tickets et Collecteurs d'E-mails

L'objectif de cette mission est toujours la mise en place d'une solution automatisée de gestion du parc informatique de Stadium, mais avec des fonctionnalités supplémentaires, notamment l'intégration de collecteurs d'e-mails. Voici les objectifs mis à jour :

1. **Inventaire à Jour :** Fournir aux administrateurs du parc un inventaire à jour de tous les postes de travail des services du stade.
2. **Outil d'Helpdesk :** Mettre en place un outil d'helpdesk pour la gestion des pannes et des incidents.
3. **Synchronisation avec Active Directory :** Assurer une synchronisation entre l'outil de gestion du parc informatique et l'Active Directory de Windows Server 2022 pour garantir la cohérence des données.
4. **Notifications des Tickets :** Configurer des notifications automatiques pour informer les administrateurs et les utilisateurs en cas de création de ticket d'incident.
5. **Collecteurs d'E-mails :** Intégrer des collecteurs d'e-mails dans l'outil pour permettre la création automatique de tickets à partir des e-mails envoyés à l'adresse support@Stadium.local. Les collecteurs récupéreront les e-mails dans la boîte de réception et créeront des tickets dans le helpdesk.

Contraintes Techniques :

- L'outil doit être gratuit, bien établi et avoir une communauté d'utilisateurs importante pour faciliter son installation et sa gestion.
- L'authentification doit être gérée par l'annuaire LDAP de Stadium, en synchronisation avec l'Active Directory Windows Server 2022.
- Différents niveaux d'autorisation doivent être configurés pour l'outil.
- L'administration de l'outil doit se faire via une interface web.
- L'outil doit être compatible avec les systèmes d'exploitation Windows et Linux, qui composent le parc informatique.
- L'outil sera installé sur un serveur virtuel au sein du réseau du stade.
- Un guide utilisateur destiné à tous les employés de l'entreprise sera créé pour expliquer clairement les étapes de connexion, la génération de tickets d'incidents, le suivi de la gestion des tickets, ainsi que la synchronisation avec l'Active Directory, les notifications et l'utilisation des collecteurs d'e-mails.

Gestion du Projet :

1. **Choix de l'Outil :** Un dossier présentant les différentes solutions envisagées, y compris celles prenant en charge la synchronisation avec l'Active Directory, les

notifications et les collecteurs d'e-mails, sera soumis à Stadium pour prendre la décision finale.

2. **Étude du Logiciel et Planification du Projet :** Une étude prévisionnelle des différentes phases du projet sera réalisée, incluant l'installation de l'outil, la configuration du service, le déploiement du logiciel client sur les postes de travail, la configuration de l'helpdesk, la synchronisation avec l'Active Directory, la configuration des notifications et l'intégration des collecteurs d'e-mails.
3. **Installation du Logiciel Serveur :** Un rapport détaillé de l'installation et du paramétrage de l'outil serveur, y compris la synchronisation avec l'Active Directory, sera rédigé.
4. **Déploiement du Logiciel Client :** Le logiciel client sera déployé sur l'ensemble des postes de travail, et les informations d'inventaire seront remontées. La configuration des notifications et des collecteurs d'e-mails sera également mise en place.
5. **Configuration de l'Helpdesk :** L'helpdesk sera configuré pour la gestion des pannes et des incidents, en incluant les notifications automatiques. Les collecteurs d'e-mails seront configurés pour la création automatique de tickets.

La mise en place de cette solution de gestion du parc informatique, avec la synchronisation Active Directory, les notifications et les collecteurs d'e-mails, permettra à Stadium de maintenir un inventaire à jour, de gérer efficacement les incidents, tout en offrant une interface pratique pour la création de tickets à partir d'e-mails, améliorant ainsi la réactivité de l'assistance technique.

Mission 8 : Mise en Place d'un Système de Supervision Open Source

Contexte : Stadium recherche l'implémentation et la configuration d'une solution Open Source pour la supervision à distance des différents éléments actifs de son infrastructure systèmes et réseaux au stade, avec la gestion des alertes.

Plan de Travail : Le principal objectif du projet est de sélectionner et mettre en place une solution de surveillance des serveurs, routeurs, commutateurs, etc., qui réponde aux critères suivants :

1. **Coûts Minimaux :** Rechercher une solution open source qui limite au maximum les coûts financiers associés.
2. **Collecte d'Informations :** Mettre en place un système de collecte d'informations permettant la détection des pannes, la surveillance de la disponibilité des serveurs (Windows, Linux), des routeurs, des commutateurs, des états des imprimantes réseau, et de leurs services.
3. **Monitoring Avancé :** Configurer des fonctionnalités avancées de monitoring, telles que la surveillance de la charge CPU, de l'espace disque, de la mémoire disponible, des entrées/sorties, des processus en cours d'exécution, du taux de paquets perdus, du temps de parcours moyen, des informations d'état SNMP, du trafic réseau, de la bande passante consommée, etc.
4. **Monitoring des Services :** Surveiller les services essentiels tels que DNS, DHCP, HTTP, SMTP, POP, IMAP, FTP, etc.
5. **Gestion des Alertes :** Mettre en place un système de gestion des alertes qui notifie automatiquement par e-mail ou SMS en cas de problème ou de défaillance d'un élément du réseau.

6. **Rapports Mensuels :** Générer des rapports mensuels sur le fonctionnement des serveurs, y compris les statistiques de disponibilité et de performance.
7. **Création de Graphes :** Créer des graphiques et une cartographie du réseau pour une visualisation claire de l'infrastructure supervisée.
8. **Interface Utilisateur Conviviale :** Mettre à disposition une interface utilisateur graphique conviviale pour permettre aux utilisateurs d'interagir avec le logiciel de supervision.

Cette mission vise à garantir la surveillance proactive de l'infrastructure informatique du stade, à améliorer la réactivité en cas de problèmes, et à fournir des données exploitables pour une gestion optimale des systèmes et des réseaux. La solution open source sélectionnée doit être efficace, économique et répondre aux besoins spécifiques de Stadium.

Mission 9 : Mise en Place d'un Système de Gestion des Informations et des Événements de Sécurité (SIEM)

Contexte : Stadium reconnaît l'importance cruciale de la sécurité de son infrastructure informatique et souhaite mettre en place un Système de Gestion des Informations et des Événements de Sécurité (SIEM) pour surveiller, détecter et répondre aux menaces potentielles.

Plan de Travail : L'objectif de cette mission est de sélectionner, mettre en place et configurer un SIEM qui permettra de gérer les informations et les événements de sécurité de manière efficace. Voici les étapes clés :

1. **Évaluation des Besoins de Sécurité :** Comprendre les besoins spécifiques de sécurité de Stadium, y compris les types de menaces potentiels, les actifs critiques à protéger et les objectifs de sécurité.
2. **Sélection du SIEM :** Identifier et sélectionner un SIEM approprié en fonction des besoins de sécurité de l'entreprise. Le choix peut se porter sur des solutions telles que Splunk, ELK Stack, ArcSight, QRadar, etc.
3. **Mise en Place de l'Infrastructure SIEM :** Mettre en place l'infrastructure nécessaire pour le SIEM, y compris les serveurs dédiés, les capacités de stockage, la connectivité réseau et les dispositifs de collecte de données.
4. **Collecte de Données :** Configurer le SIEM pour collecter des données de sécurité à partir de diverses sources, notamment les journaux système, les équipements réseau, les applications, les bases de données, les pare-feu, etc.
5. **Analyse et Corrélation :** Mettre en place des règles d'analyse et de corrélation pour détecter les anomalies, les incidents de sécurité potentiels et les attaques.
6. **Alertes et Notifications :** Configurer le SIEM pour générer des alertes et des notifications en temps réel lorsqu'un événement de sécurité critique est détecté.
7. **Investigation et Réponse :** Mettre en place des procédures d'investigation et de réponse aux incidents en fonction des alertes générées par le SIEM.
8. **Rapports de Sécurité :** Générer des rapports de sécurité réguliers pour suivre l'état de la sécurité, les tendances des incidents et les mesures prises pour atténuer les menaces.

9. **Formation du Personnel :** Former le personnel de sécurité et les équipes d'intervention aux procédures et à l'utilisation du SIEM.
10. **Maintenance et Mise à Jour :** Assurer la maintenance continue du SIEM, y compris les mises à jour logicielles, la gestion des règles de détection et la gestion des dispositifs de collecte de données.
11. **Conformité Réglementaire :** S'assurer que le SIEM est configuré pour répondre aux exigences de conformité réglementaire, le cas échéant.

La mise en place d'un SIEM permettra à Stadium de renforcer sa posture de sécurité, de détecter rapidement les menaces potentielles, de prendre des mesures préventives et d'améliorer la gestion globale de la sécurité de son infrastructure informatique. Cette mission est essentielle pour protéger les actifs de l'entreprise contre les cybermenaces.