cyna
secure your future

PROJET B3 SRC

Table des matières

I. Introduction

GÉNÉRALITÉS :

La société **Cyna**, dans le cadre de son extension et déménagement vers de nouveaux locaux à Genève, prévoit de moderniser l'intégralité de ses infrastructures informatiques et de migrer vers des solutions technologiques avancées, en mettant l'accent sur la sécurité et l'optimisation des performances.

L'entreprise est structurée en deux pôles principaux : la distribution de solutions de sécurité aux entreprises (SOC, EDR, XDR) et le développement de services sur mesure via une **solution SaaS** pour la gestion des infrastructures de sécurité. Cette plateforme SaaS permet aux clients de gérer et surveiller leurs infrastructures en temps réel, offrant ainsi une solution flexible et accessible à distance, adaptée à leurs besoins spécifiques en matière de cybersécurité. Elle compte près de deux cents collaborateurs, répartis entre le siège et les bureaux régionaux. Tous les employés seront regroupés dans les nouveaux locaux à Genève, dotés d'infrastructures plus performantes et sécurisées.

Une nouvelle filiale à Paris sera également créée après le déménagement. Les équipements informatiques (matériels et logiciels) seront homogènes avec ceux du siège, tout en tenant compte des spécificités légales et technologiques locales. Les employés de cette filiale bénéficieront d'un accès sécurisé aux mêmes applications et ressources que ceux du siège via des systèmes de sécurité renforcés (EDR, XDR).

Le présent document a pour objet de décrire les prestations suivantes :

- La fourniture,
- L'installation,
- La mise en œuvre des matériels, logiciels de base, et des applications du système d'information de la société **Cyna**, spécialisée dans la vente de solutions de sécurité, notamment les SOC (Security Operations Center), EDR (Endpoint Detection and Response), et XDR (Extended Detection and Response).

Ce document comprend également les descriptifs techniques et financiers nécessaires à l'établissement d'une proposition solide, garantissant la sécurité des infrastructures grâce aux solutions avancées de Cyna.

L'évolution vers les nouvelles technologies sera marquée par l'intégration d'une plateforme e-commerce, visant à faciliter la distribution des produits de sécurité informatique via Internet. La transformation inclura la mise en place d'une veille technologique continue, axée sur les innovations en matière de cybersécurité, de SOC, et de surveillance automatisée, pour garantir que **Cyna** reste à la pointe des technologies de protection des infrastructures

II. DESCRIPTION DU PROJET

GÉNÉRALITÉS

La société **Cyna**, dans le cadre de son déménagement vers de nouveaux locaux à Genève, prévoit de moderniser l'intégralité de ses infrastructures informatiques et de migrer vers des solutions technologiques avancées, en mettant l'accent sur la sécurité et l'optimisation des performances. L'entreprise est structurée en deux pôles principaux : la distribution de solutions de sécurité aux entreprises (SOC, EDR, XDR) et le développement de services sur mesure via une **solution SaaS** pour la gestion des infrastructures de sécurité. Cette plateforme SaaS permet aux clients de gérer et surveiller leurs infrastructures en temps réel, offrant ainsi une solution flexible et accessible à distance, adaptée à leurs besoins spécifiques en matière de cybersécurité. Elle compte près de deux cents collaborateurs, répartis entre le siège et les bureaux régionaux. Tous les employés seront regroupés dans les nouveaux locaux à Genève, dotés d'infrastructures plus performantes et sécurisées.
Une nouvelle filiale à Paris sera également créée après le déménagement. Les équipements informatiques (matériels et logiciels) seront homogènes avec ceux du siège, tout en tenant compte des spécificités légales et technologiques locales. Les employés de cette filiale bénéficieront d'un accès sécurisé aux mêmes applications et ressources que ceux du siège via des systèmes de sécurité renforcés (EDR, XDR).
L'évolution vers les nouvelles technologies sera marquée par l'intégration d'une plateforme e-commerce, visant à faciliter la distribution des produits de sécurité informatique via Internet. La transformation inclura la mise en place d'une veille technologique continue, axée sur les innovations en matière de cybersécurité, de SOC, et de surveillance automatisée, pour garantir que **Cyna** reste à la pointe des technologies de protection des infrastructures.

FONCTIONNEMENT GÉNÉRAL

Le système d'information de l'entreprise **Cyna** intégrera toutes les applications nécessaires à la gestion complète des activités de l'entreprise (comptabilité, gestion de la paie, gestion commerciale, site marchand, etc.). Ces applications, bien que faisant l'objet d'une consultation séparée, devront être intégrées de manière fluide au système central via des API ou des services web standardisés pour garantir leur interopérabilité.
Le système informatique sera conçu comme une infrastructure adaptable et évolutive, avec pour objectif de favoriser le partage d'informations tout en réduisant considérablement l'utilisation de supports papier. Il devra être suffisamment flexible pour accueillir des technologies futures telles que l'**intelligence artificielle** (IA) pour l'analyse prédictive des données, l'**automatisation** des processus via des outils **RPA** (Robotic Process Automation), et l'intégration facile de nouveaux collaborateurs ou de nouveaux services à mesure que l'entreprise se développe.
Le nouveau réseau sera conçu avec des technologies de pointe en matière de sécurité, incluant la segmentation réseau par **SD-WAN** et des dispositifs de **firewall** nouvelle génération, garantissant un accès sécurisé et rapide à Internet, aussi bien pour les collaborateurs internes que pour les clients accédant aux services via la plateforme SaaS de gestion des infrastructures de sécurité.
Les équipements nécessaires devront être inclus dans une proposition technique détaillant les spécifications matérielles (serveurs, dispositifs de stockage, switches réseau) et logicielles (systèmes d'exploitation, solutions de virtualisation) ainsi qu'une estimation des coûts en fonction des quantités et des performances requises.
Les prestations couvriront également la création d'une maquette de l'infrastructure avec une intégration dans un environnement centralisé sécurisé. La mise en place vers une solution **cloud** ou

hybride sera envisagée pour centraliser les informations et le stockage local des messages et autres données sensibles.

FONCTIONS PRINCIPALES

Le système informatique de **Cyna** devra fournir un ensemble complet de fonctionnalités, en utilisant les technologies les plus récentes et performantes pour garantir la sécurité, la flexibilité, et l'évolutivité. Les principales fonctions attendues sont :

- **Messagerie Collaborative** : La messagerie collaborative sera assurée par des solutions telles que **Microsoft 365** ou **Google Workspace** qui incluent la gestion des emails, des calendriers partagés, et des documents collaboratifs en temps réel. Ces solutions devront être renforcées par des technologies de sécurité comme le chiffrement de bout en bout (TLS, S/MIME) et des filtres anti-spam et anti-phishing via des services tels que **Proofpoint** ou **Barracuda Email Security Gateway**.
- **Internet (Intranet, Extranet, Web)** : Une gestion efficace des flux Internet sera assurée par des solutions de **reverse proxy** telles que **NGINX** ou **HAProxy** pour équilibrer les charges et sécuriser les communications web. L'**Intranet** pourra être géré via des plateformes comme **SharePoint** ou **Confluence**, permettant une collaboration interne simplifiée, tandis que l'Extranet utilisera des solutions basées sur des **VPN sécurisés** et des **certificats SSL** délivrés par des autorités de confiance comme **Let's Encrypt** ou **DigiCert**.
- **Administration du Réseau et Gestion du Parc** : L'administration réseau utilisera des outils comme **Cisco Meraki**, **Palo Alto Panorama** ou **SolarWinds NPM** pour une gestion centralisée, incluant la supervision des performances réseau, la configuration des équipements (switches, routeurs) et la gestion des incidents. Des solutions de **Gestion Unifiée des Points d'Accès** (MDM) telles que **Jamf** pour les appareils Apple, ou **Microsoft Intune** pour la gestion multi-OS, seront implémentées pour gérer les appareils et assurer la mise à jour des correctifs de sécurité.
- **Gestion des Accès Distants** : L'accès à distance sera sécurisé par des technologies de **Zero Trust** comme **Zscaler** ou **Okta** pour un contrôle granulaire des identités et des accès. Un VPN moderne tel que **OpenVPN**, **Palo Alto GlobalProtect** ou **Fortinet** fournira une couche supplémentaire de sécurité pour les connexions externes. L'authentification multifacteur (MFA) sera rendue possible par des services comme **Duo Security** ou **Yubico**, garantissant un haut niveau de sécurité pour les employés travaillant à distance.
- **Télécommunications** : L'intégration des services de télécommunication reposera sur des plateformes **UCaaS** (Unified Communications as a Service) comme **Microsoft Teams**, **Zoom**, ou **Cisco Webex**, permettant une communication unifiée avec des fonctionnalités de VoIP, visioconférence, messagerie instantanée, et collaboration en temps réel. Ces solutions offriront une intégration transparente avec les autres outils métiers et systèmes de gestion documentaire.
- **Virtualisation** : La virtualisation des serveurs sera assurée par des solutions comme **VMware vSphere**, **Microsoft Hyper-V**, ou **KVM**. Ces hyperviseurs permettront la création et la gestion de multiples machines virtuelles (VMs) sur une seule infrastructure matérielle, optimisant ainsi l'utilisation des ressources. Pour la virtualisation des postes de travail, des technologies **VDI** (Virtual Desktop Infrastructure) comme **Citrix** ou **VMware Horizon** seront déployées, garantissant un environnement de travail virtualisé pour les utilisateurs finaux. Des outils d'orchestration tels que **Terraform** et **Ansible** automatiseront le déploiement des infrastructures virtualisées.
- **Analyse des Données** : L'analyse des données sera réalisée via des outils de **Business Intelligence** tels que **Microsoft Power BI**, **Tableau** ou **QlikView**, permettant l'extraction, la transformation, et l'analyse des données en temps réel. Pour les données volumineuses (Big Data), des plateformes comme **Apache Hadoop** ou **Spark** seront utilisées pour traiter et

analyser de grands volumes de données à haute vitesse. L'intégration de services de **machine learning** comme **Azure ML** ou **Google Cloud AI** permettra également l'analyse prédictive des données pour anticiper les tendances et améliorer la prise de décision.

- **Sécurité des Données et des Applications** : Des solutions **EDR** (Endpoint Detection and Response) comme **CrowdStrike Falcon** ou **SentinelOne** et **XDR** (Extended Detection and Response) telles que **Palo Alto Cortex XDR** seront mises en place pour assurer la sécurité des endpoints et des flux réseau. L'intégration d'un **SIEM** (Security Information and Event Management) comme **Splunk** ou **IBM QRadar** permettra de centraliser et corréler les logs, assurant une détection rapide des menaces potentielles. De plus, l'utilisation d'**outils de chiffrement** pour les données au repos et en transit, ainsi que la mise en place de **certificats SSL/TLS** pour sécuriser les communications web, sera primordiale.

Pour chacune de ces fonctions, un ensemble de matériels et logiciels sera sélectionné en respectant les critères de performance, sécurité, et évolutivité définis dans ce document. Chaque technologie sera choisie en fonction de sa capacité à s'adapter aux besoins actuels de **Cyna**, tout en offrant la flexibilité nécessaire pour intégrer des évolutions technologiques futures.

III. L'ORGANISATION DE LA SOCIÉTÉ

L'organigramme de la société **Cyna** présente une structure claire, avec des équipes spécialisées dans la gestion des opérations critiques, telles que la supervision du **Security Operations Center (SOC)** et la gestion du site **SaaS** pour les clients.

- **Équipe SOC** : Cette équipe dédiée est responsable de la surveillance et de la gestion de la sécurité des infrastructures des clients en temps réel. Elle utilise des outils avancés de **SIEM** et des solutions **EDR/XDR** pour détecter, analyser, et répondre aux menaces potentielles. Le SOC fonctionne 24/7, avec une organisation en shifts pour garantir une couverture complète et une réactivité maximale face aux incidents de sécurité.
- **Équipe SaaS** : L'équipe de gestion du site **SaaS** est composée de **développeurs** et de **spécialistes DevOps**, responsables du déploiement, de la maintenance et de la mise à jour de la plateforme cloud utilisée par les clients pour la gestion de leurs infrastructures de sécurité. Cette équipe assure l'intégration continue (**CI/CD**), la supervision des performances du site et la gestion des incidents techniques via des outils comme **Kubernetes** pour l'orchestration des conteneurs et **Prometheus** pour le monitoring des services. Les développeurs sont chargés d'implémenter de nouvelles fonctionnalités, de maintenir le code source de la plateforme, et d'assurer la correction des bogues pour garantir la stabilité et l'évolutivité du service SaaS.

Après le déménagement prévu vers les nouveaux locaux à Genève, en Suisse, l'organisation sera restructurée pour maximiser l'efficacité et les synergies entre les différentes équipes.
La nouvelle implantation à Genève bénéficiera d'une infrastructure moderne, incluant des locaux techniques de pointe avec un câblage optimal et un courant secouru pour le data center, garantissant la résilience des opérations. Tous les systèmes critiques (**SOC** et **SaaS**) y seront hébergés dans un environnement sécurisé et redondant, conforme aux normes suisses et internationales.
En plus de l'équipe centrale basée à Genève, l'entreprise dispose également d'une filiale à Paris. Celle-ci regroupe 15 collaborateurs, répartis comme suit :

- **6 employés sédentaires** : responsables de la direction locale, des opérations commerciales, et de la gestion administrative.
- **9 commerciaux itinérants** : opérant à travers a France, ces collaborateurs sont responsables de l'acquisition de nouveaux clients et du suivi des comptes existants, en coordination avec les équipes techniques de Genève.

Cette organisation garantit une efficacité optimale dans la gestion des services à valeur ajoutée, tout en maintenant une proximité avec les clients sur plusieurs territoires clés.

IV. LES APPLICATIONS FONCTIONNELLES

Chaque application décrite ci-dessous sera structurée en tenant compte des technologies modernes, des exigences en matière de sécurité, et de l'organisation de **Cyna**, avec ses équipes spécialisées dans la gestion du **SOC**, du **SaaS**, et des solutions de sécurité **EDR/XDR**.

APPLICATIONS COMPTABLE

L'hébergement de l'application comptable se fera sur un serveur dédié dans le cloud (**IaaS**) où une base de données **Oracle** dernière version sera installée. Le serveur devra être surveillé en temps réel par le SOC de Cyna afin d'assurer une gestion proactive de la sécurité des données et des accès.
Configuration souhaitée :

- Mémoire : 32 Go
- Processeur : 4 cœurs
- Volumes SSD pour le système, les logs, et les données (total de 1150 Go en SSD)
- Carte réseau 1 Gbps dans une **DMZ**
- Intégration de la sécurité via les systèmes **EDR/XDR** de **Cyna** (ex. **CrowdStrike** ou **Palo Alto Cortex XDR**)

Le **SOC** surveillera l'intégrité des données comptables et la sécurité du serveur, grâce à une gestion continue des menaces par les solutions **EDR/XDR** et l'analyse des logs centralisée via le **SIEM**.

APPLICATIONS DE GESTION DE LA TRÉSORERIE

Cette application sera hébergée dans le cloud via un serveur dédié (**IaaS**) ou un service de base de données dans le cloud (**PaaS** ou **SaaS**). Les données financières sensibles seront protégées par les systèmes de détection d'intrusion et de réponse automatisée du SOC.
Configuration souhaitée :

- Mémoire : 64 Go
- Processeur : 8 cœurs
- Volumes SSD pour le système, les logs, et les données (total de 2150 Go)
- Subnet dédié au **Back End**
- Réseau sécurisé avec intégration d'un **firewall virtualisé** géré par le SOC pour garantir l'isolation des environnements

La solution devra inclure un monitoring 24/7 avec **Prometheus**, et la sécurité des bases de données sera assurée via des outils de gestion des menaces en temps réel (EDR/XDR).

SERVEURS WEB (SITE SaaS)

L'infrastructure hébergeant le site **SaaS** de Cyna, utilisé par les clients pour gérer leurs infrastructures de sécurité et l'achat de nouveaux services, sera optimisée pour la haute disponibilité, la scalabilité, et la sécurité via le SOC.
Configuration souhaitée :

- Subnet dédié **Front End**
- 4 serveurs VM **Linux** (16 Go de RAM, 4 cœurs, 50 Go SSD chacun)
- Intégration d'un **Load Balancer** pour répartir la charge et une publication sur Internet (nom de domaine : plateforme.Cyna.com)
- Sécurisation des accès par les systèmes **XDR** et par les pare-feux virtuels du SOC
- Orchestration des ressources via **Kubernetes** et surveillance des performances par **Prometheus**

Les équipes **DevOps** de Cyna géreront le déploiement continu du site **SaaS** avec des pipelines **CI/CD** automatisés et une surveillance proactive des incidents.

SERVEURS SOC (Security Operations Center)

Le **SOC** de Cyna sera l'épine dorsale de la sécurité des infrastructures des clients. Il devra être hébergé sur une infrastructure redondante et haute performance.

Configuration souhaitée :

- 2 serveurs physiques avec hyperviseurs
- Processeurs : 16 cœurs chacun
- Mémoire : 128 Go par serveur
- Stockage SSD : 5 To pour les logs et les données de sécurité
- Réseau : 2 cartes réseau 10 Gbps pour une connectivité rapide et redondante

Le **SOC** supervisera la sécurité à l'aide d'un **SIEM** centralisé (ex : **Splunk**, **IBM QRadar**), corrélant les événements pour détecter les incidents de sécurité et générer des alertes en temps réel.

SERVEURS EDR/XDR

Les serveurs pour les solutions **EDR** et **XDR** doivent garantir une surveillance complète des endpoints et une réponse automatisée aux menaces.

Configuration souhaitée :

- Serveurs VM dans le cloud avec des capacités de scalabilité
- Mémoire : 128 Go
- Processeur : 16 cœurs
- Stockage SSD : 2 To
- Connectivité sécurisée via **VPN**

Les systèmes **EDR** comme **CrowdStrike Falcon** ou **SentinelOne** assureront la détection des menaces sur les endpoints, tandis que **Palo Alto Cortex XDR** surveillera et analysera les menaces globales sur l'infrastructure.

MESSAGERIE COLLABORATIVE

Un service de messagerie sécurisé et résilient devra être fourni avec les fonctionnalités suivantes :

- Accès via client riche et client web
- Relayage SMTP sécurisé
- Partage d'agendas et filtre antispam
- Antivirus intégré avec mise à jour automatique

L'accès à la messagerie devra être possible depuis l'extérieur avec **MFA** et sécurisé via les systèmes de détection du **SOC**. Un **MDM** sera mis en place pour la gestion des appareils mobiles.

ADMINISTRATION DU RÉSEAU ET GESTION DU PARC

L'administration du réseau et la gestion du parc matériel et logiciel devront être centralisées et automatisées pour garantir une efficacité maximale et une sécurité accrue. Voici les outils recommandés pour ces fonctions :

- **Cisco Meraki** : Gestion complète du réseau incluant le WiFi, la sécurité, et le monitoring en temps réel de la qualité du service réseau.
- **SolarWinds NPM** (Network Performance Monitor) : Suivi et diagnostic des performances du réseau avec une détection automatique des pannes.
- **Microsoft Intune** ou **Jamf** pour la gestion des appareils mobiles (MDM), permettant le déploiement des mises à jour, la configuration des politiques de sécurité, et le suivi des appareils mobiles en temps réel.

- **PDQ Deploy** et **PDQ Inventory** : Outils de déploiement de logiciels et de gestion de l'inventaire des systèmes, permettant de suivre et déployer facilement les mises à jour logicielles.
- **Ansible Tower** : Solution de gestion automatisée pour la gestion des correctifs, le déploiement d'applications, et l'orchestration des tâches à grande échelle.
- **ServiceNow** : Gestion des incidents, du parc et des tickets de support en lien avec la surveillance des performances réseau et du parc informatique.

Ces outils permettront de centraliser l'administration, d'automatiser la gestion des mises à jour des logiciels et des correctifs de sécurité, ainsi que de maintenir un inventaire précis et à jour du parc matériel et logiciel.

GESTION DES ACCÈS DISTANTS

La solution de gestion des accès distants permettra aux collaborateurs de travailler en toute sécurité, qu'ils soient en déplacement ou depuis leur domicile. Elle devra garantir une connexion sécurisée et des performances optimales tout en assurant une protection des données sensibles.

- **VPN Zero Trust** avec **Zscaler** ou **Palo Alto GlobalProtect** : Garantir un accès sécurisé aux ressources internes sans dépendre de périmètres réseau fixes, en accordant uniquement les accès requis en fonction des rôles et des besoins spécifiques des utilisateurs.
- **Multi-Factor Authentication (MFA)** via **Duo Security** ou **Microsoft Azure AD** : Utiliser l'authentification à deux facteurs pour sécuriser l'accès aux ressources sensibles. Cela inclura également une intégration avec les applications cloud.
- **Splunk Phantom** : Outil d'automatisation de la réponse aux incidents qui détecte les accès non autorisés et initie des actions automatiques comme le blocage d'accès ou la réinitialisation des accès.
- **Single Sign-On (SSO)** avec **Okta** : Simplifier la gestion des accès distants en permettant aux utilisateurs de se connecter à toutes leurs applications à l'aide d'un seul ensemble d'identifiants, avec une sécurité accrue.

Les collaborateurs auront la possibilité de se connecter aux ressources de l'entreprise (intranet, fichiers, messagerie, CRM, etc.) en toute sécurité et de manière transparente, avec un accès protégé par l'authentification forte.

GESTION DES LOGS

La gestion des logs est cruciale pour garantir la sécurité et le bon fonctionnement des infrastructures. Elle permettra de centraliser et corréler les événements générés par les différents systèmes pour anticiper et résoudre les incidents.

- **Splunk** ou **Elastic Stack (ELK)** : Solutions de gestion des logs pour la collecte, la mise en forme et l'analyse des données provenant des équipements réseau, machines virtuelles, serveurs, applications et solutions de sécurité (EDR/XDR).
- **Graylog** : Outil complémentaire pour l'analyse en temps réel des logs, avec des capacités avancées de création de tableaux de bord et d'alertes personnalisées.
- **SIEM (Security Information and Event Management)** comme **IBM QRadar** : Centralisation des logs et corrélation des événements de sécurité en temps réel pour identifier les menaces potentielles et générer des alertes automatiques.

Ces solutions fourniront des tableaux de bord interactifs et des rapports qui permettront une surveillance proactive et une capacité d'audit étendue. Elles permettront également une détection rapide des anomalies et des comportements suspects grâce à des alertes en temps réel.

VIRTUALISATION

La virtualisation de l'infrastructure est essentielle pour garantir une utilisation optimisée des ressources et une grande flexibilité dans la gestion des services.

- **VMware vSphere** ou **Microsoft Hyper-V** : Plateformes de virtualisation permettant de créer et de gérer plusieurs machines virtuelles (VM) sur des hôtes physiques, optimisant ainsi les ressources matérielles. Ces solutions permettront la répartition dynamique des charges de travail et le changement à chaud des VMs pour maintenir la disponibilité des services.
- **Proxmox** pour les environnements plus open source, offrant la virtualisation des serveurs ainsi que la gestion des containers.
- **Veeam** : Solution de sauvegarde et de restauration pour garantir la continuité des opérations et l'intégration avec les environnements **PRA** (Plan de Reprise d'Activité) et **PCA** (Plan de Continuité d'Activité).
- **vRealize Operations** ou **SolarWinds Virtualization Manager** : Solutions de gestion centralisée des ressources virtualisées, permettant une surveillance proactive des performances, des alertes en cas de dégradation et une optimisation continue des environnements virtualisés.

Les systèmes seront administrés via une interface centralisée, avec des outils de monitoring pour analyser les performances en temps réel et garantir une répartition efficace des charges de travail.

HYBRIDATION, ÉLASTICITÉ ET AUTOMATISATION

L'hybridation permettra d'intégrer des ressources on-premises avec le cloud pour absorber les pics d'activité et offrir une élasticité en fonction de la demande.

- **VMware Cloud on AWS** ou **Microsoft Azure Arc** : Ces solutions permettent d'étendre les infrastructures locales au cloud public, tout en maintenant une cohérence dans la gestion des ressources et des politiques de sécurité.
- **Terraform** et **Ansible** pour l'**Infrastructure as Code** (IaC) : Automatiser le provisionnement des infrastructures, tant on-premises que dans le cloud, en utilisant des fichiers de configuration pour garantir une infrastructure reproductible, sécurisée, et facilement scalable.
- **Autoscaling** via **AWS Auto Scaling** ou **Google Cloud Compute Engine** : Mettre en place des mécanismes d'élasticité automatique pour allouer ou retirer des ressources en fonction de la charge de travail, assurant ainsi une utilisation optimale des ressources.
- **Fortinet ou Palo Alto Firewalls virtualisés** : Protéger les interconnexions entre les infrastructures cloud et locales, avec des politiques de sécurité adaptées à chaque segment de réseau et une gestion des flux entrants et sortants.

ACTIVE DIRECTORY

La société **Cyna** a choisi comme élément central de son système d'information la solution **Microsoft Active Directory** (AD), avec une configuration optimisée pour garantir la haute disponibilité, la sécurité, et l'évolutivité.

Les principales fonctionnalités d'Active Directory incluront :

- **Gestion des droits utilisateurs** : Les accès aux ressources seront gérés de manière centralisée via des **Group Policies (GPO)**, permettant une gestion granulaire des droits en fonction des rôles au sein de l'organisation.
- **Gestion des certificats** : L'**Active Directory Certificate Services (AD CS)** sera utilisé pour gérer les certificats de sécurité, garantissant une connexion sécurisée au réseau **Wi-Fi** et aux **VPN** via des certificats numériques. Cela permettra également de sécuriser les communications internes avec des **certificats SSL/TLS**.
- **Authentification unique (Single Sign-On)** : La solution **SSO** permettra aux utilisateurs de se connecter à toutes les applications et services internes avec un seul ensemble d'identifiants, réduisant ainsi la complexité et renforçant la sécurité des accès.
- **Service d'annuaire** : L'AD fournira un service d'annuaire pour l'enregistrement, la recherche et la gestion des objets du réseau (utilisateurs, groupes, ordinateurs, périphériques).

- **Réplication** : La réplication des données sera assurée à travers plusieurs sites, garantissant une continuité de service et une protection contre les pannes. L'utilisation de **contrôleurs de domaine** secondaires permettra de garantir que les informations critiques sont toujours disponibles, même en cas de défaillance d'un site.
- **Sécurité renforcée** : L'AD sera intégré avec des solutions **EDR/XDR** (ex. **CrowdStrike**, **SentinelOne**) pour surveiller en temps réel les comportements anormaux des utilisateurs ou des terminaux et réagir immédiatement en cas de tentative de compromission.
- **Résilience et haute disponibilité** : La configuration physique de l'Active Directory devra inclure des **contrôleurs de domaine** redondants, hébergés à la fois localement et dans des infrastructures cloud. La réplication sera assurée entre les sites via des connexions sécurisées, garantissant que toutes les informations soient synchronisées en temps réel.
- **Reprise après sinistre (PRA/PCA)** : Une solution de **Plan de Reprise d'Activité (PRA)** sera mise en place pour assurer la restauration rapide du service en cas d'incident majeur. L'AD devra être restauré en priorité pour garantir l'accès aux ressources critiques. Des copies de sauvegarde automatiques seront effectuées régulièrement, avec des solutions de **sauvegarde dans le cloud** (ex. **Veeam**, **Azure Backup**).

SERVICE DE FICHIERS

La société **Cyna** souhaite mettre en place un **nouveau système de fichiers** performant et sécurisé, intégrant les fonctionnalités suivantes pour répondre aux besoins d'une gestion optimisée des données :

- **Performance** : Le système de fichiers devra offrir des performances élevées pour les opérations d'E/S, en particulier pour les accès simultanés de nombreux utilisateurs. L'utilisation de **SSD NVMe** et de **RAID** pour la redondance des données assurera une haute performance et une faible latence.
- **Redondance** : Les données devront être stockées dans une infrastructure redondante, avec des solutions de **réplication automatique** entre plusieurs sites pour garantir la disponibilité des fichiers, même en cas de panne d'un serveur ou d'un site.
- **Déduplication** : L'intégration d'une fonctionnalité de **déduplication** permettra de réduire la quantité d'espace de stockage nécessaire en évitant le stockage de copies inutiles des fichiers. Cela sera particulièrement utile pour les environnements de stockage volumineux, comme les archives ou les backups.
- **Sécurité (gestion des accès)** : Le contrôle des accès aux fichiers sera géré de manière granulaire en fonction des services, via des politiques de sécurité intégrées à l'Active Directory (ex. **ACL**, **NTFS permissions**). Les accès aux fichiers sensibles seront surveillés en temps réel, avec des solutions de **DLP (Data Loss Prevention)** pour éviter toute fuite de données.
- **Sauvegarde et intégration dans le PRA/PCA** : Le système de fichiers devra être intégré dans le **Plan de Reprise d'Activité** et le **Plan de Continuité d'Activité**, avec des sauvegardes régulières effectuées via des solutions comme **Veeam** ou **Commvault**. Des sauvegardes incrémentielles et complètes seront réalisées automatiquement et stockées dans des infrastructures locales et distantes (cloud).

Solutions envisagées pour le système de fichiers :

- **NetApp** ou **Dell EMC Isilon** : Solutions de stockage réseau (NAS) offrant des performances élevées, une redondance intégrée, et des fonctionnalités avancées de gestion de données (déduplication, compression).
- **ZFS** ou **Microsoft Storage Spaces Direct** : Systèmes de fichiers offrant une résilience avancée, la gestion des snapshots, la redondance des données et des capacités de mise à l'échelle en fonction des besoins de stockage.

Résumé des fonctionnalités principales : L'objectif est de fournir à **Cyna** une solution de fichiers performante et sécurisée, capable de gérer des volumes de données importants tout en assurant la sécurité et la disponibilité des fichiers en toute circonstance.

V. LA SOLUTION TECHNIQUE

Une grande latitude de proposition est laissée aux fournisseurs concernant le choix des technologies à installer. Toutefois, les solutions proposées devront garantir le bon fonctionnement, la sécurité et la scalabilité, en accord avec les spécifications techniques et les exigences de sécurité de **Cyna**.
Toute solution facilitant l'exploitation du système informatique, assurant une gestion centralisée et garantissant une sécurité maximale peut être proposée. Les fournisseurs devront s'assurer que les propositions tiennent compte des éléments suivants :

Sécurité :

- **Zero Trust Architecture** : Les solutions proposées devront respecter les principes d'une **architecture Zero Trust**, assurant que chaque utilisateur et chaque appareil est vérifié à chaque accès au réseau. Une gestion granulaire des accès (via **Zscaler** ou **Palo Alto Prisma Access**) devra être intégrée pour protéger les environnements. Le **PRA/PCA** pour cette architecture garantira la continuité des accès en cas de compromission, avec des redirections automatiques vers des environnements sécurisés de secours.
- **EDR/XDR** : L'intégration des solutions **EDR** et **XDR** (ex. **CrowdStrike Falcon**, **SentinelOne**, **Palo Alto Cortex XDR**) est impérative pour garantir une surveillance continue des menaces et une réponse automatisée aux incidents sur les postes utilisateurs, serveurs, et applications critiques. Le **PRA/PCA** inclura des mécanismes de reprise rapide des services **EDR/XDR**, permettant de rétablir la surveillance après une attaque en moins de 30 minutes via des solutions redondantes dans le cloud.
- **SIEM** : La solution de sécurité devra inclure une plateforme **SIEM** (ex. **Splunk**, **IBM QRadar**) pour centraliser les logs, analyser les événements en temps réel, et corréler les données de sécurité afin de détecter les anomalies et menaces potentielles. Le **PRA/PCA** prévoira la redondance du **SIEM** avec une réplication des données dans des environnements distants, permettant une restauration complète et rapide des logs en cas d'incident majeur.

Administration des équipements des utilisateurs :

- **Clients légers pour les services administratifs** : Les services administratifs seront équipés de **clients légers** qui se connecteront à des serveurs centralisés via **Virtual Desktop Infrastructure (VDI)**. Les solutions comme **VMware Horizon** ou **Citrix** seront utilisées pour garantir une gestion flexible des bureaux virtuels, tout en réduisant la maintenance des postes clients. Le **PRA/PCA** inclura des solutions de réplication des sessions **VDI** pour assurer la continuité des services en cas de panne du serveur principal.
- **PC portables pour les responsables et commerciaux** : Les responsables et les commerciaux seront équipés de **PC portables** sécurisés avec des mécanismes d'authentification forte (**MFA**, **biométrie**). Ces appareils seront intégrés à la solution de **Mobile Device Management (MDM)** comme **Microsoft Intune** ou **Jamf**, permettant une gestion centralisée des terminaux, y compris pour la sécurité des données en cas de perte ou de vol. Le **PRA** inclura des sauvegardes automatisées et des restaurations rapides des configurations des appareils dans des environnements sécurisés.
- **Postes fixes pour les services opérationnels** : Les services opérationnels seront équipés de **PC fixes** performants avec des ressources suffisantes pour gérer les applications métier critiques. Ces postes devront être intégrés dans le système de gestion du parc (via **Ansible**, **PDQ Deploy**, ou **ServiceNow**) pour assurer un déploiement rapide des mises à jour et correctifs de

sécurité. Le **PRA/PCA** garantira la redondance des postes critiques avec la possibilité de répliquer les images des systèmes sur des machines de secours.

Infrastructure informatique :

- **Infrastructure Cloud Hybride** : La solution devra inclure un couplage avec une infrastructure de **cloud public ou privé** (ex. **AWS**, **Azure**, **Google Cloud**) pour permettre une scalabilité automatique en fonction des besoins saisonniers de l'entreprise. Le cloud devra être intégré avec les systèmes on-premises pour garantir une élasticité transparente et une continuité des services. Le **PRA/PCA** assurera la bascule automatique vers des infrastructures cloud en cas de panne locale, avec un plan de tests réguliers pour vérifier la continuité des services.
- **Virtualisation** : L'architecture IT reposera sur la virtualisation via des solutions comme **VMware vSphere** ou **Hyper-V** pour permettre une gestion optimisée des serveurs et un provisionnement dynamique des ressources. Cette architecture garantira la haute disponibilité, la résilience, et l'optimisation des coûts. Le **PRA/PCA** intégrera des solutions de bascule automatique des **VMs** sur des serveurs de secours, avec des sauvegardes régulières pour assurer la reprise des services sans perte de données.
- **Administration centralisée** : Tous les équipements (clients légers, PC, portables, serveurs, appareils réseau, **switches**, **routeurs**) devront être administrés de manière centralisée via des outils comme **SolarWinds**, **Cisco Meraki**, ou **Microsoft Endpoint Manager**, permettant la gestion des performances et l'automatisation des tâches de maintenance. La gestion des **switches** et **routeurs** inclura des fonctionnalités avancées d'optimisation de la bande passante, ainsi que la configuration automatisée des politiques de sécurité. Le **PRA/PCA** garantira la restauration rapide des consoles d'administration en cas de défaillance, avec une redondance assurée via des solutions cloud pour permettre une reprise immédiate des services critiques, y compris la gestion des infrastructures réseau.

Facilitation de l'exploitation (DEVOPS) :

- **Infrastructure as Code (IaC)** : L'automatisation du déploiement des infrastructures et des services sera primordiale. Des solutions comme **Terraform** et **Ansible** devront être proposées pour permettre un provisioning rapide et reproductible des environnements, assurant une gestion simplifiée et une réduction des erreurs humaines. Le **PRA/PCA** inclura des plans de restauration des configurations **IaC** en cas de défaillance des systèmes d'automatisation, garantissant la possibilité de reprovisionner les environnements rapidement.
- **Automatisation de la gestion des incidents** : Les solutions d'automatisation de la gestion des incidents (ex. **ServiceNow**, **Splunk Phantom**) devront être intégrées pour minimiser le temps de réponse en cas de défaillance ou de menace, permettant ainsi de résoudre rapidement les incidents sans intervention humaine directe. Le **PRA/PCA** inclura des plans de reprise des workflows automatisés avec une restauration rapide des processus critiques en cas d'incident.
- **Monitoring et alertes en temps réel** : Le monitoring proactif de l'ensemble des systèmes devra être assuré par des outils comme **Prometheus** ou **Grafana** pour garantir la surveillance des performances des serveurs, des applications et du réseau, avec des alertes automatiques en cas d'anomalies. Le **PRA/PCA** intégrera des mécanismes de reprise automatique des systèmes de surveillance et d'alerte en cas de défaillance, avec des redirections vers des serveurs de secours.

Plans de Reprise d'Activité (PRA) et de Continuité d'Activité (PCA) :

Chaque partie devra respecter le **Plans de Reprise d'Activité (PRA)** et le **Plan de Continuité d'Activité (PCA)** :

- La solution proposée devra inclure un **PRA/PCA** robuste pour garantir la continuité des services critiques en cas d'incident majeur. Des sauvegardes régulières et une réplication des données sur plusieurs sites seront intégrées pour assurer la résilience des systèmes et des données.
- **Veeam**, **Commvault**, ou **Bacula** seront utilisés pour gérer les sauvegardes automatiques et la restauration rapide des services en cas de sinistre. Des tests réguliers de restauration seront planifiés et exécutés pour s'assurer que les objectifs de temps de reprise (**RTO**) et de point de reprise (**RPO**) sont respectés.

Résumé des fonctionnalités principales :

1. Sécurité :
    - Zero Trust Architecture : Vérification continue des utilisateurs et appareils avec des solutions pour garantir la continuité après une attaque.
    - EDR/XDR et SIEM : Surveillance des et centralisation des. Réponse rapide aux incidents avec redondance pour la restauration.
2. Administration des équipements :
    - Clients légers (VDI) : Gestion centralisée des bureaux virtuels incluant un PRA pour la continuité.
    - PC portables et fixes : Sécurisés avec MFA et MDM, gestion des mises à jour avec Ansible, et PRA pour restauration rapide.
3. Infrastructure informatique :
    - Cloud hybride et virtualisation : Scalabilité avec bascule automatique en cas de panne.
    - Administration centralisée : Gestion des équipements avec redondance cloud pour reprise rapide.
4. DevOps et automatisation :
    - IaC : Automatisation du et restauration des configurations en cas d'incident.
    - Monitoring et alertes : Surveillance proactive avec mécanismes de reprise automatique.
5. PRA/PCA : Sauvegardes régulières et réplication pour assurer la continuité des services critiques en cas de sinistre.

VI. DESCRIPTION DES PRESTATIONS

L'entreprise retenue pour ce marché devra fournir les **études détaillées** suivantes, dans le cadre de la mise en place de l'infrastructure réseau et des services associés :

Étude détaillée complète du réseau et des services demandés :

L'étude devra inclure une analyse complète et approfondie de l'architecture réseau proposée, comprenant :

- La **topologie du réseau** (LAN, WAN, Wi-Fi), y compris les interconnexions entre les sites (Paris, Genève) ;
- Le schéma d'**adressage IP** (avec des propositions de segmentation des réseaux pour des raisons de sécurité et de gestion) ;
- Les solutions d'**optimisation du trafic** pour garantir des performances réseau optimales (QoS, gestion de la bande passante, latence, etc.) ;
- La sécurisation des services via des technologies **firewalls**, **IPS/IDS**, et **filtrage des flux** Est-Ouest et Nord-Sud ;
- L'intégration des services **Wi-Fi** avec plusieurs **SSID** et des règles spécifiques pour chaque segment de réseau (Wi-Fi Guest, Wi-Fi Corp, etc.).

Cette étude devra également inclure un plan de **sécurité réseau** avec des mécanismes de **chiffrement**, d'**authentification forte** et des dispositifs de **détection et réponse aux menaces** (EDR/XDR, SIEM), ainsi qu'une proposition de plan de **redondance réseau** pour garantir la continuité des services.

Définition des conditions d'exploitation du système informatique :

L'entreprise devra définir les conditions d'exploitation optimales du système informatique, en spécifiant :

- Les **normes et bonnes pratiques** à respecter pour garantir la stabilité et la sécurité du système ;
- Les procédures de **gestion des incidents**, incluant des indicateurs de performance (SLA) pour assurer un suivi efficace des pannes et des résolutions ;
- Les processus de **maintenance préventive et corrective** des infrastructures (équipements actifs, serveurs, points d'accès Wi-Fi, etc.), ainsi que les outils de **monitoring** proposés pour superviser l'ensemble des services en temps réel ;
- La gestion de la **sécurité des accès** utilisateurs (rôles et permissions) avec une **authentification centralisée** (via Active Directory ou autre solution) et des règles de **rotation des mots de passe**.

L'ensemble de ces conditions d'exploitation devra s'assurer de la **haute disponibilité** du système, tout en respectant les objectifs définis dans les **PRA/PCA**.

Estimation financière des fournitures et prestations :

Une **estimation détaillée** des coûts sera fournie, incluant :

- Le coût de tous les **équipements matériels** nécessaires (serveurs, switches, routeurs, points d'accès Wi-Fi, pare-feux, etc.) ;
- Les coûts des **logiciels** indispensables pour l'exploitation et la sécurité du réseau (licences, logiciels de monitoring, gestion des accès, sécurité, etc.) ;
- Les **prestations de service** associées, comme le déploiement, l'installation, la configuration, la mise en service des infrastructures, et l'assistance technique ;
- Une **analyse comparative** des coûts et bénéfices des différentes options technologiques proposées (solutions cloud, virtualisation, redondance des services).

L'estimation financière devra également inclure les **coûts récurrents** liés à la maintenance, aux abonnements, aux licences, et au support technique, ainsi que les investissements nécessaires pour l'évolution future des infrastructures (scalabilité).

Planning prévisionnel de la prestation :
Le **planning prévisionnel** devra détailler toutes les étapes clés du projet, incluant :

- Les **phases de conception** et de validation des études techniques ;
- Les **jalons de livraison** des équipements matériels et logiciels ;
- Le **déploiement des infrastructures** réseau et serveur (physiques et virtuels) ;
- La **création des nouvaux services** et des données, avec des périodes de tests et de validation ;
- Les tests de **PRA/PCA** et la validation des objectifs **RTO/RPO** ;
- La formation des équipes internes et le **suivi post-déploiement**.

Chaque phase devra être accompagnée d'un **diagramme de Gantt** pour visualiser les échéances, les interdépendances et les périodes de tests et de validation. Le planning tiendra compte des temps d'interruptions minimales de service, ainsi que des ressources humaines nécessaires à chaque étape du projet.

LA RECETTE

La procédure de **recette** effectuée par le fournisseur devra apporter la preuve que l'ensemble des systèmes installés respecte les critères suivants :

- **Opérabilité des systèmes** : Tous les systèmes déployés (serveurs, réseau, équipements utilisateurs) doivent être entièrement opérationnels et conformes aux spécifications techniques du cahier des charges. Chaque composant sera soumis à des **tests de performance** pour vérifier son bon fonctionnement dans les conditions réelles d'exploitation.
- **Ergonomie du système** : L'interface utilisateur, la configuration des postes, ainsi que l'organisation générale du réseau devront correspondre aux besoins exprimés par l'entreprise. L'objectif est de s'assurer que l'ergonomie des systèmes et des outils logiciels facilite l'usage par les équipes internes et soit adaptée à leur environnement de travail quotidien.
- **Conformité des performances** : Les performances (bande passante réseau, capacité de traitement des serveurs, temps de réponse des applications) devront être en accord avec les promesses faites par le fournisseur lors de l'appel d'offres. Des **tests de charge** et des simulations de pic d'utilisation seront réalisés pour vérifier la capacité du système à gérer des charges de travail élevées sans dégradation notable des performances.
- **Sécurité du système** : La sécurité des systèmes, en particulier contre les **intrusions** internes et externes, devra être rigoureusement vérifiée. Cela inclut la validation des **pare-feux**, des solutions de **chiffrement**, des contrôles d'accès, et des mécanismes de **détection des menaces** (EDR/XDR). Des tests d'intrusion simulés (**pentests**) devront être réalisés pour vérifier la robustesse de la protection contre les attaques.

Le fournisseur devra fournir un **bordereau récapitulatif des logiciels installés**, indiquant la version, la référence et l'emplacement de chaque logiciel. Ce bordereau sera validé par le **Maître d'Ouvrage** ou son représentant et servira de référence pour d'éventuels ajustements.
Un **procès-verbal de recette** détaillera les résultats des tests, les observations faites et les conclusions du fournisseur, avec un résumé des performances mesurées et des écarts constatés (le cas échéant) par rapport aux attentes initiales.

LE PARAMÉTRAGE ET LE DÉPLOIEMENT
Dans le cadre de l'installation, le fournisseur devra assurer les prestations suivantes :

- **Fourniture, pose et mise en œuvre des équipements réseau** : Cette prestation inclut l'installation physique des **switches**, **routeurs**, **points d'accès Wi-Fi**, et autres équipements réseau, ainsi que leur configuration pour s'intégrer dans l'architecture réseau existante.
- **Fourniture et paramétrage des logiciels de base** : L'entreprise fournira et mettra en œuvre tous les **systèmes d'exploitation** et les **logiciels réseau** nécessaires au bon fonctionnement des serveurs et des équipements connectés. Ces logiciels devront être configurés selon les bonnes pratiques de sécurité et d'optimisation des performances (telles que la gestion de la charge sur les serveurs, le partitionnement des ressources, etc.).
- **Mise en œuvre des cartes de communication** : Les **cartes réseau** pour les serveurs devront être installées et configurées pour assurer une communication optimale avec le réseau fédérateur (10 GbE). Cela inclut également la gestion des **SFP** et autres modules d'interconnexion pour la transmission de données par fibre optique.
- **Plan d'adressage du réseau** : Un **plan d'adressage IP** complet devra être fourni, incluant la segmentation des réseaux pour les différents services (réseau interne, Wi-Fi invité, réseau sécurisé, etc.), et des règles claires pour le routage et la gestion des flux.
- **Adressage des périphériques** : L'adressage IP et la configuration des **périphériques** (imprimantes, scanneurs, etc.) devront être effectués à partir des postes clients pour assurer une utilisation simple et sécurisée. Ces périphériques devront être accessibles en réseau et correctement intégrés au système de gestion documentaire de l'entreprise.

L'ASSISTANCE TECHNIQUE

L'assistance technique sera fournie tout au long des opérations d'installation, et de paramétrage des systèmes. Cela inclura :

- **Support proactif** : Le fournisseur devra garantir une présence continue d'ingénieurs ou de techniciens spécialisés pendant toute la durée des travaux pour répondre rapidement à toute question ou incident technique.
- **Assistance post-installation** : Après la mise en service de l'ensemble des équipements, une période de **support technique** sera fournie pour résoudre tout problème éventuel et ajuster les configurations si nécessaire. Le fournisseur devra assurer une disponibilité rapide en cas d'incident, notamment lors des premières semaines d'exploitation.

L'entreprise assurera les prestations suivantes dans le cadre du déploiement des solutions proposées :

- **Fourniture des équipements réseau** : L'ensemble des **switches**, **routeurs**, **firewalls**, points d'accès **Wi-Fi**, et autres équipements nécessaires à la mise en œuvre du réseau ;
- **Fourniture des équipements serveurs** : Les serveurs physiques et virtuels seront fournis, installés, et configurés pour assurer la haute disponibilité et l'évolutivité des services ;
- **Fourniture des logiciels** : Tous les logiciels requis pour l'infrastructure réseau et serveur (hors ceux déjà fournis par le client) seront inclus dans la proposition. Cela inclut les logiciels de sécurité, de gestion du réseau, ainsi que les outils de virtualisation ;
- **Déploiement et installation des équipements** : L'installation des équipements réseau, des serveurs, des postes de travail, et des imprimantes sera réalisée par des experts certifiés, garantissant le respect des meilleures pratiques d'installation et de configuration ;
- **Mise en service de l'ensemble** : La mise en service de l'infrastructure complète, incluant la validation du bon fonctionnement des systèmes, la connexion des utilisateurs, et la configuration des services cloud, si applicable ;
- **Assistance technique** : Un support technique sera fourni à l'équipe informatique du client pour assurer la bonne prise en main des systèmes. Un suivi post-installation sera mis en place pour répondre à tout problème technique éventuel
- **Formation des exploitants du réseau** : Une formation complète sera fournie aux administrateurs du réseau, couvrant l'utilisation des nouveaux équipements et logiciels, la gestion des incidents, et les bonnes pratiques de maintenance et de sécurité.

VII. ÉTUDES

L'entreprise retenue pour ce marché devra fournir les **études détaillées** suivantes, dans le cadre de la mise en place de l'infrastructure réseau et des services associés :

Étude détaillée complète du réseau et des services demandés :

L'étude devra inclure une analyse complète et approfondie de l'architecture réseau proposée, comprenant :

- La **topologie du réseau** (LAN, WAN, Wi-Fi), y compris les interconnexions entre les sites (Paris, Genève) ;
- Le schéma d'**adressage IP** (avec des propositions de segmentation des réseaux pour des raisons de sécurité et de gestion) ;
- Les solutions d'**optimisation du trafic** pour garantir des performances réseau optimales (QoS, gestion de la bande passante, latence, etc.) ;
- La sécurisation des services via des technologies **firewalls**, **IPS/IDS**, et **filtrage des flux** Est-Ouest et Nord-Sud ;
- L'intégration des services **Wi-Fi** avec plusieurs **SSID** et des règles spécifiques pour chaque segment de réseau (Wi-Fi Guest, Wi-Fi Corp, etc.).

Cette étude devra également inclure un plan de **sécurité réseau** avec des mécanismes de **chiffrement**, d'**authentification forte** et des dispositifs de **détection et réponse aux menaces** (EDR/XDR, SIEM), ainsi qu'une proposition de plan de **redondance réseau** pour garantir la continuité des services.

Définition des conditions d'exploitation du système informatique :

L'entreprise devra définir les conditions d'exploitation optimales du système informatique, en spécifiant :

- Les **normes et bonnes pratiques** à respecter pour garantir la stabilité et la sécurité du système ;
- Les procédures de **gestion des incidents**, incluant des indicateurs de performance (SLA) pour assurer un suivi efficace des pannes et des résolutions ;
- Les processus de **maintenance préventive et corrective** des infrastructures (équipements actifs, serveurs, points d'accès Wi-Fi, etc.), ainsi que les outils de **monitoring** proposés pour superviser l'ensemble des services en temps réel ;
- La gestion de la **sécurité des accès** utilisateurs (rôles et permissions) avec une **authentification centralisée** (via Active Directory ou autre solution) et des règles de **rotation des mots de passe**.

L'ensemble de ces conditions d'exploitation devra s'assurer de la **haute disponibilité** du système, tout en respectant les objectifs définis dans les **PRA/PCA**.

Estimation financière des fournitures et prestations :

Une **estimation détaillée** des coûts sera fournie, incluant :

- Le coût de tous les **équipements matériels** nécessaires (serveurs, switches, routeurs, points d'accès Wi-Fi, pare-feux, etc.) ;
- Les coûts des **logiciels** indispensables pour l'exploitation et la sécurité du réseau (licences, logiciels de monitoring, gestion des accès, sécurité, etc.) ;
- Les **prestations de service** associées, comme le déploiement, l'installation, la configuration, la mise en service des infrastructures, et l'assistance technique ;

- Une **analyse comparative** des coûts et bénéfices des différentes options technologiques proposées (solutions cloud, virtualisation, redondance des services).

L'estimation financière devra également inclure les **coûts récurrents** liés à la maintenance, aux abonnements, aux licences, et au support technique, ainsi que les investissements nécessaires pour l'évolution future des infrastructures (scalabilité).

Planning prévisionnel de la prestation :

Le **planning prévisionnel** devra détailler toutes les étapes clés du projet, incluant :

- Les **phases de conception** et de validation des études techniques ;
- Les **jalons de livraison** des équipements matériels et logiciels ;
- Le **déploiement des infrastructures** réseau et serveur (physiques et virtuels) ;
- La **création des nouvaux services** et des données, avec des périodes de tests et de validation ;
- Les tests de **PRA/PCA** et la validation des objectifs **RTO/RPO** ;
- La formation des équipes internes et le **suivi post-déploiement**.

Chaque phase devra être accompagnée d'un **diagramme de Gantt** pour visualiser les échéances, les interdépendances et les périodes de tests et de validation. Le planning tiendra compte des temps d'interruptions minimales de service, ainsi que des ressources humaines nécessaires à chaque étape du projet.

LA RECETTE

La procédure de **recette** effectuée par le fournisseur devra apporter la preuve que l'ensemble des systèmes installés respecte les critères suivants :

- **Opérabilité des systèmes** : Tous les systèmes déployés (serveurs, réseau, équipements utilisateurs) doivent être entièrement opérationnels et conformes aux spécifications techniques du cahier des charges. Chaque composant sera soumis à des **tests de performance** pour vérifier son bon fonctionnement dans les conditions réelles d'exploitation.
- **Ergonomie du système** : L'interface utilisateur, la configuration des postes, ainsi que l'organisation générale du réseau devront correspondre aux besoins exprimés par l'entreprise. L'objectif est de s'assurer que l'ergonomie des systèmes et des outils logiciels facilite l'usage par les équipes internes et soit adaptée à leur environnement de travail quotidien.
- **Conformité des performances** : Les performances (bande passante réseau, capacité de traitement des serveurs, temps de réponse des applications) devront être en accord avec les promesses faites par le fournisseur lors de l'appel d'offres. Des **tests de charge** et des simulations de pic d'utilisation seront réalisés pour vérifier la capacité du système à gérer des charges de travail élevées sans dégradation notable des performances.
- **Sécurité du système** : La sécurité des systèmes, en particulier contre les **intrusions** internes et externes, devra être rigoureusement vérifiée. Cela inclut la validation des **pare-feux**, des solutions de **chiffrement**, des contrôles d'accès, et des mécanismes de **détection des menaces** (EDR/XDR). Des tests d'intrusion simulés (**pentests**) devront être réalisés pour vérifier la robustesse de la protection contre les attaques.

Le fournisseur devra fournir un **bordereau récapitulatif des logiciels installés**, indiquant la version, la référence et l'emplacement de chaque logiciel. Ce bordereau sera validé par le **Maître d'Ouvrage** ou son représentant et servira de référence pour d'éventuels ajustements.

Un **procès-verbal de recette** détaillera les résultats des tests, les observations faites et les conclusions du fournisseur, avec un résumé des performances mesurées et des écarts constatés (le cas échéant) par rapport aux attentes initiales.

LE PARAMÉTRAGE ET LE DÉPLOIEMENT

Dans le cadre de l'installation, le fournisseur devra assurer les prestations suivantes :

- **Fourniture, pose et mise en œuvre des équipements réseau** : Cette prestation inclut l'installation physique des **switches**, **routeurs**, **points d'accès Wi-Fi**, et autres équipements réseau, ainsi que leur configuration pour s'intégrer dans l'architecture réseau existante.
- **Fourniture et paramétrage des logiciels de base** : L'entreprise fournira et mettra en œuvre tous les **systèmes d'exploitation** et les **logiciels réseau** nécessaires au bon fonctionnement des serveurs et des équipements connectés. Ces logiciels devront être configurés selon les bonnes pratiques de sécurité et d'optimisation des performances (telles que la gestion de la charge sur les serveurs, le partitionnement des ressources, etc.).
- **Mise en œuvre des cartes de communication** : Les **cartes réseau** pour les serveurs devront être installées et configurées pour assurer une communication optimale avec le réseau fédérateur (10 GbE). Cela inclut également la gestion des **SFP** et autres modules d'interconnexion pour la transmission de données par fibre optique.
- **Plan d'adressage du réseau** : Un **plan d'adressage IP** complet devra être fourni, incluant la segmentation des réseaux pour les différents services (réseau interne, Wi-Fi invité, réseau sécurisé, etc.), et des règles claires pour le routage et la gestion des flux.
- **Adressage des périphériques** : L'adressage IP et la configuration des **périphériques** (imprimantes, scanneurs, etc.) devront être effectués à partir des postes clients pour assurer une utilisation simple et sécurisée. Ces périphériques devront être accessibles en réseau et correctement intégrés au système de gestion documentaire de l'entreprise.

L'ASSISTANCE TECHNIQUE

L'assistance technique sera fournie tout au long des opérations d'installation, et de paramétrage des systèmes. Cela inclura :

- **Support proactif** : Le fournisseur devra garantir une présence continue d'ingénieurs ou de techniciens spécialisés pendant toute la durée des travaux pour répondre rapidement à toute question ou incident technique.
- **Assistance post-installation** : Après la mise en service de l'ensemble des équipements, une période de **support technique** sera fournie pour résoudre tout problème éventuel et ajuster les configurations si nécessaire. Le fournisseur devra assurer une disponibilité rapide en cas d'incident, notamment lors des premières semaines d'exploitation.

Résumé des fonctionnalités principales :

- Étude du réseau : Analyse de l'architecture réseau (LAN/WAN/Wi-Fi), optimisation des performances, sécurisation (firewalls, IPS/IDS).
- Conditions d'exploitation : Normes de sécurité, gestion des incidents, maintenance, et accès centralisé avec authentification.
- Estimation financière : Coût des équipements, logiciels, services, et analyse des options technologiques.
- Planning : Conception, livraison, déploiement, tests PRA/PCA, et validation des performances avec suivi via un diagramme de Gantt.
- Recette : Vérification de l'opérabilité, sécurité, et performances réseau par des tests d'intrusion.
- Paramétrage : Installation et configuration des équipements et logiciels réseau.
- Assistance technique : Support proactif et post-installation pour résoudre les incidents techniques.

VIII. REPARTITION DES TACHES MINIMUN PAR ETUDIANT

La liste d'activités présentée pour chaque groupe est une recommandation visant à vous guider dans vos travaux. Elle vous oriente sur les aspects essentiels à traiter pour développer une solution complète et alignée avec les attentes du client. Toutefois, il est important de noter que ce travail nécessite un approfondissement supplémentaire de votre part, ainsi que des recherches individuelles pour assurer une implémentation correcte et détaillée. Suivre ces recommandations ne garantit pas automatiquement une note maximale. L'évaluation prendra en compte la qualité de l'analyse, l'originalité des solutions proposées, la rigueur dans la mise en œuvre technique, ainsi que la capacité à aller au-delà des exigences de base pour fournir une réponse approfondie et bien documentée.

Groupe	**Activités recommandés à réaliser**	**Détails**
Sécurité : Etudiant 1	Zero Trust Architecture	Implémenter les principes de Zero Trust, assurer une gestion granulaire des accès via Zscaler ou Palo Alto Prisma Access, prévoir le PRA/PCA avec redirections automatiques.
	EDR/XDR	Intégrer des solutions EDR/XDR (CrowdStrike Falcon, SentinelOne, Palo Alto Cortex XDR) pour surveillance des menaces et réponse automatisée, assurer un PRA/PCA pour reprise rapide des services EDR/XDR.
	SIEM	Mettre en place une plateforme SIEM (Splunk, IBM QRadar) pour centralisation des logs et corrélation des événements, garantir la redondance du SIEM via PRA/PCA.
Administration des équipements utilisateurs : Étudiant 2 **(facultatif à repartir)**	Clients légers	Déployer des clients légers pour les services administratifs avec VMware Horizon ou Citrix VDI, assurer la continuité des services via PRA/PCA.
	PC portables	Sécuriser les PC portables avec MFA et intégration MDM (Microsoft Intune, Jamf), implémenter un PRA pour sauvegarde et restauration rapide en cas de perte ou vol.
	Postes fixes	Assurer la gestion des postes fixes pour les services opérationnels, utiliser des outils comme Ansible ou PDQ Deploy pour les mises à jour, intégrer un PRA pour la redondance des postes critiques.
Infrastructure informatique : Étudiant 3	Infrastructure Cloud Hybride	Intégrer une infrastructure hybride avec AWS, Azure ou Google Cloud, assurer la bascule automatique vers le cloud en cas de panne via PRA/PCA.

	Virtualisation	Mettre en œuvre la virtualisation via VMware vSphere ou Hyper-V pour gestion des serveurs, inclure un PRA pour bascule automatique et sauvegarde des VMs.
	Administration centralisée	Administrer les équipements via SolarWinds, Cisco Meraki, ou Microsoft Endpoint Manager, optimiser les performances réseau et configurer les politiques de sécurité, prévoir un PRA pour la restauration des consoles.
DEVOPS: Étudiant 4	Infrastructure as Code (IaC)	Automatiser le déploiement des infrastructures avec Terraform et Ansible, intégrer un PRA pour restauration rapide des configurations IaC en cas de défaillance.
	Automatisation des incidents	Mettre en place des solutions d'automatisation des incidents (ServiceNow, Splunk Phantom), intégrer des workflows automatisés dans le PRA pour gestion rapide des incidents.
	Monitoring et alertes	Implémenter des solutions de monitoring en temps réel avec Prometheus ou Grafana, prévoir un PRA pour reprise automatique des systèmes de surveillance en cas de défaillance.

IX. GLOSSAIRE DES TECHNOLOGIES

Partie	Technologies Recommandées	Détails Supplémentaires
Messagerie Collaborative	Microsoft 365, Google Workspace, Zimbra, Zoho Mail, Proofpoint, Barracuda Email Security Gateway, Cisco Email Security, Mimecast, Virtru, ProtonMail, Hushmail, Open-Xchange	Messagerie chiffrée, collaboration sécurisée, solutions d'anti-phishing, gestion d'emails basée sur le cloud avec protection avancée contre les menaces
Internet (Intranet/Extranet/Web)	NGINX, HAProxy, SharePoint, Confluence, VPN, Let's Encrypt, DigiCert, Apache HTTP Server, IIS, Citrix ADC, Fortinet Secure Web Gateway, Cloudflare, Squid Proxy, Fastly, Varnish, F5 Networks, Kemp LoadMaster	Sécurité et accélération des flux web, gestion d'intranet et extranet sécurisés, reverse proxy pour équilibrage de charge, CDN pour performance améliorée
Administration du Réseau et Gestion du Parc	Cisco Meraki, Palo Alto Panorama, SolarWinds NPM, Jamf, Microsoft Intune, PDQ Deploy, PDQ Inventory, Ansible Tower, ServiceNow, Ivanti Endpoint Manager, ManageEngine OpManager, Nagios, Spiceworks, PRTG Network Monitor, Zenoss, Zabbix	Surveillance du réseau, gestion centralisée des appareils, automatisation des déploiements et des correctifs, monitoring avancé pour les infrastructures réseau et IT
Gestion des Accès Distants	Zscaler, Okta, OpenVPN, Palo Alto GlobalProtect, Fortinet, Duo Security, Yubico, Pulse Secure, Citrix Gateway, Cisco AnyConnect, RSA SecurID, NetMotion, Perimeter 81, Cloudflare Zero Trust, SecureLink, Ivanti Secure Access	Accès distant sécurisé avec MFA et Zero Trust, VPN pour une gestion sécurisée des connexions à distance, contrôle des identités pour des accès à distance
Télécommunications	Microsoft Teams, Zoom, Cisco Webex, RingCentral, 8x8, Avaya Cloud Office, Mitel MiCloud Connect, BlueJeans, Polycom RealPresence, Vonage Business Communications, Slack, Workplace by Facebook, Dialpad, Jitsi, FreePBX	Solutions UCaaS, communication VoIP et collaboration, outils de visioconférence et de messagerie instantanée pour équipes distribuées, intégration transparente avec d'autres outils de gestion et collaboration
Virtualisation	VMware vSphere, Microsoft Hyper-V, KVM, Citrix XenServer, VMware Horizon, Red Hat Virtualization, Oracle	Virtualisation de serveurs et de postes de travail, gestion de machines virtuelles avec

Partie	Technologies Recommandées	Détails Supplémentaires
	VM VirtualBox, Nutanix AHV, Proxmox VE, QEMU, OpenStack, Xen Project, Virtuozzo, Parallels RAS, Nutanix Prism	orchestration avancée, hyperviseurs pour environnements on-premises et cloud
Analyse des Données	Microsoft Power BI, Tableau, QlikView, Apache Hadoop, Apache Spark, Azure ML, Google Cloud AI, Amazon QuickSight, SAS Visual Analytics, Looker, Domo, Cloudera, Databricks, Snowflake, BigQuery, Splunk, Microsoft SQL Server Analysis Services (SSAS)	Plateformes de Big Data, outils de Business Intelligence, traitement et analyse des données volumineuses avec machine learning et IA intégrée
Sécurité des Données et des Applications	CrowdStrike Falcon, SentinelOne, Palo Alto Cortex XDR, Splunk, IBM QRadar, McAfee Endpoint Security, Symantec Endpoint Protection, Bitdefender GravityZone, Fortinet FortiEDR, Sophos Intercept X, Trend Micro Apex One, Kaspersky Security, ESET Endpoint Security, F-Secure Protection Service for Business, Cisco AMP, Deep Instinct	Protection complète des endpoints, analyse et détection des menaces, chiffrement avancé pour les données en transit et au repos
Serveurs Web (Site SaaS)	Linux VM, **OpenShift**, Kubernetes, Prometheus, Apache Tomcat, NGINX, HAProxy, Varnish, Docker, Rancher, Istio, Elastic Load Balancer (AWS), Jetty, WebSphere Application Server, JBoss EAP, Litespeed, Traefik	Orchestration des conteneurs, outils de monitoring et équilibrage de charge pour haute disponibilité et performance des applications web, OpenShift pour gestion de clusters Kubernetes à l'échelle entreprise
Serveurs SOC (Security Operations Center)	Splunk, IBM QRadar, ArcSight, LogRhythm, SolarWinds Security Event Manager, AlienVault OSSIM, RSA NetWitness, SIEMonster, Exabeam, Devo, Securonix, AT&T Cybersecurity	Solutions de corrélation des événements, détection des menaces, génération d'alertes en temps réel, SIEM pour surveillance centralisée
Serveurs EDR/XDR	CrowdStrike Falcon, SentinelOne, Palo Alto Cortex XDR, Microsoft Defender for Endpoint, Sophos XDR, Fortinet FortiXDR, Kaspersky EDR, BlackBerry CylancePROTECT, Cisco Secure Endpoint, Trend Micro Vision One, FireEye Endpoint Security	EDR et XDR pour détection et réponse automatisée aux menaces, solutions pour endpoints et infrastructures IT critiques

Partie	Technologies Recommandées	Détails Supplémentaires
Gestion des Logs	Splunk, Elastic Stack (ELK), Graylog, Loggly, Papertrail, Fluentd, Datadog, Sumo Logic, SolarWinds Log Analyzer, LogRhythm, XpoLog, ManageEngine EventLog Analyzer, InsightOps (Rapid7), Humio	Collecte centralisée des logs, gestion des événements de sécurité, analyse en temps réel et génération d'alertes sur incidents
Virtualisation et Plan de Reprise d'Activité (PRA)	VMware vSphere, Microsoft Hyper-V, Proxmox, Veeam, Bacula, Commvault, Acronis Backup, Zerto, Rubrik, Nutanix Xi Leap, Arcserve, Carbonite, IBM Spectrum Protect	Solutions de sauvegarde et restauration, virtualisation pour PRA, reprise rapide après incident majeur
Hybridation, Élasticité et Automatisation	**OpenShift**, VMware Cloud on AWS, Microsoft Azure Arc, Terraform, Ansible, AWS Auto Scaling, Google Cloud Compute Engine, HashiCorp Vault, Puppet, Chef, SaltStack, Red Hat OpenShift, OpenNebula, Scalr	Automatisation du provisioning d'infrastructures, gestion hybride cloud/on-premises, OpenShift pour orchestration multi-cloud et gestion des conteneurs à grande échelle
Active Directory	Microsoft Active Directory, OpenLDAP, FreeIPA, Active Directory Certificate Services (AD CS), Centrify, Okta, Ping Identity, OneLogin, AWS Directory Service, JumpCloud	Gestion centralisée des identités, authentification unique (SSO), gestion des certificats pour accès sécurisé aux ressources
Service de Fichiers	NetApp, Dell EMC Isilon, ZFS, Microsoft Storage Spaces Direct, Synology NAS, QNAP NAS, TrueNAS, OpenZFS, Veeam, Commvault, IBM Cloud Object Storage, AWS S3, Wasabi, Panzura	Stockage distribué, gestion des fichiers avec réplication et redondance, solutions de sauvegarde cloud pour continuité des opérations
Gestion des accès Wi-Fi	Cisco Meraki, Aruba ClearPass, Ruckus Wireless, Ubiquiti UniFi, Extreme Networks, Fortinet FortiAP, Mist Systems, Cambium Networks, Aerohive, Mojo Networks, Netgear Insight, Juniper Networks	Solutions Wi-Fi d'entreprise avec gestion centralisée, sécurité renforcée, gestion des accès par SSID avec segmentation réseau pour isolation des flux
Sécurité Réseau et Firewall	Palo Alto Next-Gen Firewall, Fortinet FortiGate, Check Point Firewall, Cisco ASA, Juniper SRX, WatchGuard Firebox, Barracuda CloudGen Firewall, SonicWall TZ, Sophos XG Firewall, pfSense, Untangle, Forcepoint NGFW, Stormshield	Pare-feux nouvelle génération, prévention et détection d'intrusions, segmentation réseau pour protection renforcée des flux

Partie	Technologies Recommandées	Détails Supplémentaires
Plan de Reprise d'Activité (PRA) et Continuité d'Activité (PCA)	Veeam, Commvault, Bacula, Zerto, Datto, Arcserve, Acronis Cyber Backup, Carbonite, IBM Spectrum Protect, Asigra, Infrascale, Druva, Rubrik Polaris	Solutions robustes pour PRA/PCA avec automatisation de la reprise, sauvegardes redondantes et tests de restauration réguliers pour garantir la continuité des services
Infrastructure Cloud Hybride	AWS, Microsoft Azure, Google Cloud, VMware Cloud on AWS, Microsoft Azure Arc, IBM Cloud, Oracle Cloud Infrastructure, Alibaba Cloud, Rackspace, Linode, DigitalOcean, Nutanix Xi, OpenStack, **OpenShift**	Plateformes de cloud hybride pour scalabilité automatique, OpenShift pour gestion d'environnements multi-cloud et orchestration de conteneurs, bascule fluide entre infrastructures cloud et on-premises

Livrables - GIT, Documentation Technique, Architecture Système et Scripting :

Objectif : Modernisation des infrastructures informatiques de l'entreprise dans le cadre du projet de déménagement vers Genève, mise en place d'une architecture cloud hybride et automatisation de la gestion des infrastructures via des scripts et outils d'Infrastructure as Code (IaC).

1. Repository GIT pour la gestion des configurations et des scripts d'automatisation :

- Mise en place d'un repository GIT pour centraliser les fichiers de configuration réseau (switches, routeurs, pare-feux) ainsi que tous les scripts d'automatisation (Terraform, Ansible, etc.).
- Chaque script devra suivre un processus de versioning afin de permettre une traçabilité complète des modifications et des déploiements automatisés.
- Les scripts devront inclure des commentaires explicatifs et respecter les standards de l'entreprise en termes de nommage des variables et des fonctions.

2. Infrastructure as Code (IaC) - Automatisation des infrastructures :

- **Scripts Terraform :**
    - Création d'un ensemble de scripts Terraform pour automatiser le provisionnement des environnements cloud (Azure, AWS) ainsi que la configuration réseau (VPC, subnets, security groups).
    - Les scripts doivent être paramétrables pour permettre la réutilisation des configurations sur plusieurs environnements (test, préproduction, production).
    - Chaque script doit inclure des mécanismes de rollback en cas d'erreur de déploiement et générer des logs détaillés.
- **Automatisation avec Ansible :**
    - Fournir des **playbooks Ansible** pour automatiser la configuration des serveurs (VMs), des services réseau (DNS, DHCP), et des équipements réseau (pare-feux, switches).
    - Les playbooks doivent être modulaires et permettre une configuration déclarative pour chaque type d'équipement ou de service.
    - Inclure des tests de validation automatisés pour vérifier la bonne application des configurations.
- **Déploiement des conteneurs avec Docker/Kubernetes :**
    - Fournir des scripts pour le déploiement automatisé des conteneurs Docker sur un cluster Kubernetes.
    - Les scripts doivent gérer le scaling automatique des conteneurs en fonction de la charge (autoscaling).
    - Utilisation de Helm charts pour gérer les configurations des applications déployées sur Kubernetes.

- Inclure un script de monitoring via **Prometheus** et **Grafana** pour surveiller les performances des services conteneurisés.

3. Livrables - Architecture Cloud Hybride et Sécurité :

- **Diagrammes d'architecture technique :**
  - Un diagramme détaillé montrant l'intégration de l'infrastructure cloud avec les composants on-premises, illustrant comment les services (VMs, conteneurs, bases de données) sont déployés via Terraform.
  - Diagramme de flux montrant les pipelines CI/CD pour automatiser le déploiement continu et les tests via des outils comme Jenkins ou GitLab CI.
- **Automatisation des règles de sécurité avec Ansible :**
  - Mise en place de scripts Ansible pour automatiser la configuration des firewalls (pare-feux nouvelle génération) et des règles de sécurité dans les environnements cloud.
  - Les scripts doivent être capables d'appliquer des politiques de sécurité Zero Trust et de les mettre à jour dynamiquement selon les besoins du réseau.
- **Plan de continuité d'activité (PCA) et de reprise après sinistre (PRA) - Automatisation des sauvegardes :**
- Utiliser des scripts pour automatiser les sauvegardes des configurations réseau et des systèmes critiques (VMs, bases de données) via des outils comme **Veeam** ou **Commvault**.
- Des playbooks Ansible ou des scripts Terraform doivent être fournis pour automatiser la restauration des services critiques en cas de sinistre, garantissant une reprise d'activité rapide et conforme aux objectifs RTO/RPO.

5. Documentation technique complète et guide d'utilisation des scripts :

- **Guide d'utilisation des scripts Terraform et Ansible :**
  - Explication détaillée de chaque fichier et script présent dans le repository GIT, incluant les prérequis et les dépendances.
  - Instructions sur la manière de déployer des environnements cloud ou de configurer des équipements réseau à l'aide de scripts.
- **Documentation des API et des services automatisés :**
  - Documenter les API utilisées pour automatiser la création et la gestion des ressources cloud (AWS Lambda, Azure Functions).
  - Détails sur l'intégration des services de monitoring automatisé avec Prometheus, Grafana, et les alertes configurées via des outils comme **PagerDuty** ou **OpsGenie**.
- **Tests d'intégration continue (CI) :**
  - Les scripts doivent être testés automatiquement dans un pipeline CI (via Jenkins, GitLab CI, etc.). Fournir un **guide pour configurer le pipeline CI**, incluant les tests d'intégration et les tests unitaires pour les scripts Terraform/Ansible.

6. Suivi de l'évolution des livrables et rapport de progression avec automatisation :

- Chaque phase de déploiement doit être suivie via des outils de gestion de projet (JIRA, Confluence) et automatisée via des scripts pour générer des rapports de progression.
- Les commits GIT doivent inclure des informations sur les modifications apportées aux scripts d'automatisation et les configurations réseau.

7. Date limite de livraison :

- La livraison finale de l'infrastructure réseau et cloud automatisée est fixée à **8 mois après le début du projet**. Cela inclut :
    - La mise en place de l'architecture cloud hybride et la configuration automatisée des infrastructures.
    - Les scripts Terraform, Ansible, et Kubernetes complets.
    - La documentation technique, les tests CI, et les procédures de reprise après sinistre.

PROJET FIL ROUGE : PROJET D'ETUDE B3

COORDINATEUR DE PROJETS INFORMATIQUES (INFRASTRUCTURES CLOUD, APPLICATIVES OU DATA)

A destination des candidats

SOMMAIRE

I. PRINCIPAUX ELEMENTS DU PROJET

I.1 - OBJECTIFS

Le projet fil rouge se déroule tout au long de la formation.

Le but du projet est d'acquérir et de développer les compétences des 3 premiers blocs du titre CPI ainsi que de valider l'acquisition de ces compétences.

BLOC DE COMPETENCES		OBJECTIF GENERAL	ACTIVITES
BLOCS COMMUNS	BC1 - Piloter un projet informatique	Acquérir les compétences nécessaires pour gérer un projet informatique de l'analyse du besoin jusqu'à la livraison finale en intégrant une méthodologie adaptée et responsable	- Conception du cadrage technique et méthodologique du projet informatique responsable - Structuration de la veille technologique, concurrentielle et règlementaire - Planification des différentes étapes du projet - Prévention des risques informatiques
	BC2 - Coordonner une équipe projet	Apprendre à coordonner une équipe projet en assurant une communication fluide, la mobilisation des ressources et la présentation des résultats de manière claire et convaincante	- Transmission d'informations autour des étapes du projet - Entretien de la relation client - Conduite des échanges avec l'ensemble des parties prenantes - Mobilisation d'une équipe projet et conduite du changement
	BC3 - Superviser la mise en œuvre d'un projet informatique	Assurer la supervision de la mise en œuvre du projet, y compris le déploiement de l'infrastructure, la documentation technique et la gestion de la sécurité	- Mise en place de l'installation et de la configuration - Gouvernance des systèmes d'information - Gestion de la sécurité de l'information - Organisation des phases de tests et de validation - Elaboration de la documentation technique

Bloc 1 Piloter un projet pédagogique :

• Recueillir, analyser et comprendre les besoins du client pour proposer des solutions adaptées.
• Rédiger des spécifications fonctionnelles et techniques pour garantir la faisabilité du projet.
• Mettre en place un plan de gestion de projet (Agile, Waterfall) ainsi qu'un planning.

Bloc 2 Coordonner une équipe projet :

• Coordonner les tâches entre les membres de l'équipe et gérer les flux d'information pour assurer la réussite du projet.
• Conduire les réunions de suivi, présenter le projet aux parties prenantes.
• Présenter les résultats du projet de manière claire et professionnelle lors d'une soutenance orale.

Bloc 3 Superviser la mise en œuvre d'un projet informatique :

• Déployer une infrastructure technique tout en assurant sa sécurité et sa maintenance.
• Documenter toutes les étapes techniques du projet.
• Identifier et proposer des solutions pour anticiper les risques techniques et les incidents éventuels.

Mais aussi des compétences transverses :

- Travailler en équipe : Capacité à collaborer avec des équipes pluridisciplinaires, à utiliser des outils de gestion de projets (Jira, Trello) et à communiquer efficacement.
- Développer sa communication : savoir échanger avec des clients maîtrisant les aspects techniques et non techniques, développer sa capaciter à présenter de solutions logicielles.
- Pour les étudiants en développement : capacité à diagnostiquer des erreurs dans le code, à résoudre les bogues, et à optimiser le développement des applications tout en respectant les délais.
- Pour les étudiants en Systèmes, Réseaux et Cloud : capacité à diagnostiquer et résoudre les erreurs de configuration, pannes réseau et dysfonctionnements des infrastructures. Optimisation des performances et gestion rapide des incidents pour assurer la continuité des services.

I.2 - ORGANISATION

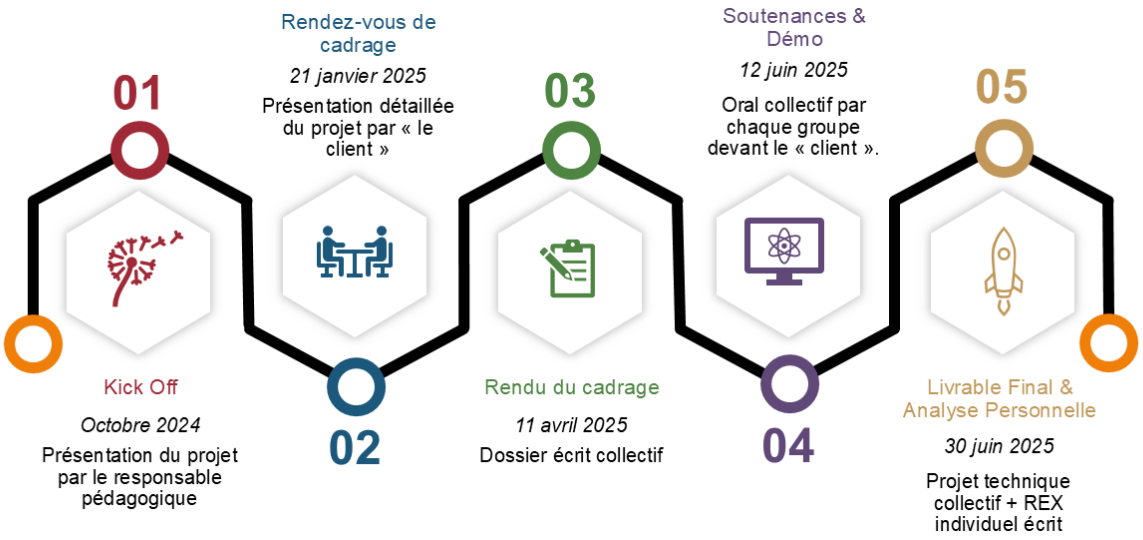
Le projet est décomposé en 5 étapes dont 3 étapes débouchent sur des rendus.

Les 5 étapes :

	Evaluation certifiante adossée à l'étape
1. **Le Kick off :** présentation du projet aux étudiants par l'animateur.	
2. **Le Rendez-vous de cadrage :** présentation détaillée du projet par « le client » - étape qui permet aux étudiants de recueillir le besoin et de comprendre les enjeux du projet	oui
3. **Livraison du cadrage technique :** Les premières pierres du projet sont présentées par les étudiants via un document écrit	Oui (rendu)
4. **Soutenance & démo du projet :** par chaque groupe de projet étudiant devant le « client ». L'idée est de convaincre le client final via la démonstration ainsi que de revenir sur le déroulement projet en faisant une rétrospective.	Oui (rendu)
5. **Livrable final & livraison analyse personnelle :** C'est la dernière étape du projet, les étudiants rendent le projet technique et chacun	Oui (rendu)

d'entre eux livre un rapport personnel qui lui permet de livrer son analyse personnelle du déroulement du projet et de la dynamique collaborative.	

Voici une roadmap du projet d'étude :



Composition des équipes :

L'équipe projet est composée de 3 ou 4 personnes. Les groupes sont composés par le responsable pédagogique.

I.3 - EVALUATION CERTIFIANTE DU PROJET D'ETUDE / FIL ROUGE

L'évaluation du projet d'étude est découpée en plusieurs épreuves certifiantes correspondant aux blocs de compétences.

Chaque épreuve, écrite ou orale, collective ou individuelle, est évaluée via une grille spécifique reprenant les compétences correspondant à chacun des blocs.

BC1 - Piloter un projet informatique	1.1 - Document de cadrage – écrit collectif	80 % de l'évaluation du bloc
	1.2 - Evaluation du rendez-vous de cadrage – évaluation collective avec pondération individuelle –	20 % de l'évaluation du bloc
BC2 - Coordonner une équipe projet	2.1 - Soutenance de présentation de la solution – oral collectif devant jury	80 % de l'évaluation du bloc
	2.2 - Analyse de la dynamique du projet - écrit individuel	20 % de l'évaluation du bloc
BC3 - Superviser la mise en œuvre d'un projet informatique	Livrable technique final – écrit collectif –	100 % de l'évaluation du bloc

LES ETAPES CHRONOLOGIQUES DU PROJET

II.1 – KICK-OFF

Calendrier : Octobre

Objectif : Présentation de l'objectif du projet et du sujet

Organisation

- Première ½ J :
  - Introduction : présentation de l'ensemble des éléments structurants du projet (objectifs, calendrier, modalités d'évaluation, …) afin de bien préciser les attendus, expliquer les temps forts et fournir des conseils
  - Présentation du sujet / temps de réponse aux questions
- Le reste de la demi-journée vous permettra de commencer à réfléchir au projet.

II.2 - RENDEZ-VOUS DE CADRAGE

Calendrier : 21 janvier

Modalités :

- Chaque groupe pourra poser des questions d'éclaircissement au client et valider sa compréhension du sujet.
- Vous disposez de 15 min pour interroger le client.
- Le groupe doit mener l'échange en mode workshop.

Préparation :
Chaque groupe transmet la liste des questions à l'animateur pédagogique avant le rendez-vous client à minima deux semaines avant. L'animateur pédagogique transmet les questions au client qui peut ainsi s'y préparer en collaboration avec l'animateur pédagogique.

Evaluation :
Epreuve notée comptant pour 20 % de la note d'oral du bloc 2 « Coordonner une équipe projet ».
La qualité de l'échange est évaluée immédiatement à l'issue du rendez-vous de cadrage par l'animateur pédagogique en évaluant la logique et la qualité des questions ainsi que la qualité de l'oral.

II.3 - PREMIER RENDU : DOCUMENT DE CADRAGE

Calendrier : 11 avril

Modalités : Compte pour 80 % de la note du bloc 1 « Piloter un projet Informatique ».

Livrables attendus :

1) SPECIFICATIONS FONCTIONNELLES :

Option dev

2) MODELE D'ARCHITECTURE CIBLE :

Le modèle d'architecture cible décrit la structure technique du système, les composants principaux, et leur interaction. Il s'agit de l'architecture qui sera mise en œuvre pour répondre aux besoins techniques et fonctionnels du projet.

Contenu attendu :

- **Diagramme d'architecture :** Schéma décrivant l'architecture du système, incluant : Les composants logiciels : Modules principaux, microservices, bases de données.
- **Les interfaces :** Comment les différents composants interagissent entre eux (API, services REST, etc.).
- **Infrastructure matérielle :** Serveurs, cloud, bases de données, systèmes de stockage, réseaux.
  Niveaux d'abstraction : Détailler les différents niveaux de l'architecture (front-end, back-end, base de données, intégrations).
- **Flux de données :** Représentation des flux de données et des processus entre les composants (inclure des schémas UML, diagrammes de séquence).
- **Scalabilité et haute disponibilité :** Explication de comment le modèle peut évoluer et supporter une montée en charge.

Outils technologiques pour Systèmes, Réseaux, Cloud :

- **Infrastructure as Code (IaC)** : Utilisez Terraform, AWS CloudFormation, ou VMware vSphere pour modéliser et déployer votre architecture cloud et virtualisée.
- **Virtualisation des serveurs :** Utilisez VMware ESXi pour la gestion et la virtualisation des serveurs physiques, permettant de créer plusieurs machines virtuelles sur un même hôte physique.
- **Surveillance des infrastructures :** Outils comme Zabbix, Nagios, ou vRealize Operations pour surveiller les performances des infrastructures virtuelles et physiques.
- **Conteneurisation :** Pour des architectures basées sur des microservices, utilisez Docker pour créer et déployer des conteneurs, et Kubernetes pour orchestrer ces conteneurs dans un environnement cloud ou sur des serveurs virtualisés avec VMware Tanzu.
- **Virtualisation réseau :** Utilisez VMware ESXI pour virtualiser et automatiser le réseau à l'échelle du data center ou du cloud.
- **Outils de gestion des environnements virtualisés :** VMware vCenter pour gérer l'infrastructure virtuelle, surveiller les machines virtuelles (VMs), et organiser les tâches quotidiennes de gestion des systèmes.
- **Automatisation des tâches d'infrastructure :** outils comme Ansible, Puppet ou VMware PowerCLI pour automatiser la gestion des infrastructures et des réseaux virtualisés.
- **Gestion des configurations** : Puppet ou Chef pour gérer la configuration des infrastructures réseau et cloud.

Outils technologiques pour Développement Full Stack :

- **Modélisation des architectures applicatives :** Utilisez C4 Model pour modéliser les niveaux d'architecture des applications.
- **Outillage DevOps :** Utilisez Jenkins, GitLab CI ou CircleCI pour automatiser les déploiements sur une architecture cible.
- **Diagrammes UML et de flux :** Outils comme Lucidchart ou Enterprise Architect pour modéliser les composants de votre application (front-end, back-end, bases de données).

3) JUSTIFICATION DES CHOIX TECHNOLOGIQUES :

Les étudiants expliquent leurs choix en matière de technologies pour le développement, en fonction des besoins spécifiques du projet et des avantages et inconvénients de chaque technologie.

Contenu attendu pour Développement Full stack :

- **Liste des technologies** : Présentation des frameworks, langages, outils utilisés (ex : Java, React, Spring Boot, MongoDB, Docker, etc.).
- **Comparaison des technologies :** Comparaison avec d'autres technologies possibles, avec une explication des avantages et inconvénients.
- **Critères de comparaison :** Performance, facilité de développement, maintenabilité, coût, compatibilité avec les autres composants.
- **Pertinence par rapport aux spécifications fonctionnelles :** Justifier en quoi chaque choix technologique est pertinent vis-à-vis des fonctionnalités et de l'architecture. Retour d'expérience ou veille technologique : Si possible, inclure un retour d'expérience ou une veille technologique sur les technologies choisies.

Contenu attendu pour Systèmes, Réseaux, Cloud :

- **Liste des technologies** : Les technologies utilisées incluent la conteneurisation et la gestion des environnements isolés (**Docker**), l'orchestration des conteneurs dans un environnement cloud (**Kubernetes**), l'automatisation de l'infrastructure en tant que code (IaC) (**Terraform**), l'hébergement cloud avec (**AWS**), notamment **EC2**, **S3**, et **RDS**, l'automatisation de la configuration des systèmes et réseaux (**Ansible**), la gestion des clouds privés (**OpenStack**, **OpenShift**, **VMware ESXI**), ainsi que la surveillance des infrastructures et la gestion des logs (**Prometheus**, **Grafana**, **Nagios**, **Centreon**, **Zabbix**, et **Elastic)**. La liste des technologies est exhaustive et peut être adaptée en fonction des choix des étudiants.
- **Comparaison des technologies** : Différentes solutions peuvent être envisagées pour chaque domaine technologique. Une comparaison approfondie entre les solutions utilisées et d'autres alternatives permet d'évaluer leurs avantages et inconvénients respectifs. Cette analyse prend en compte des facteurs tels que la flexibilité, la scalabilité et la capacité à s'intégrer dans un environnement cloud hybride ou multi-cloud.
- **Critères de comparaison** : Les critères retenus pour la comparaison incluent la **performance** des technologies en termes de capacité à gérer des environnements complexes, la **facilité de développement** et de gestion au quotidien, la **maintenabilité** des solutions choisies, le **coût** d'exploitation et d'acquisition, ainsi que la **compatibilité** avec les autres composants du système d'information.
- **Pertinence par rapport aux spécifications fonctionnelles** : Chaque choix technologique doit être justifié par son adéquation avec les spécifications fonctionnelles et les besoins du système. Il est essentiel de s'assurer que les technologies choisies répondent aux exigences de l'architecture globale, en garantissant une infrastructure évolutive, sécurisée et performante.

- **Retour d'expérience ou veille technologique** : Un retour d'expérience sur l'utilisation des technologies choisies ou une veille technologique sur les dernières évolutions dans le domaine du cloud et des réseaux peut être inclus. Cela permet d'évaluer l'adoption de nouvelles technologies ou de valider la pertinence des solutions actuelles en fonction des tendances du marché.

Outils technologiques pour Développement Full Stack :

- **Comparateur de frameworks :** Utilisez des outils comme StackShare pour comparer les frameworks back-end (Django, Flask, Express.js, etc.) et front-end (React, Angular, Vue.js).
- **Technologies de base de données :** Justifiez le choix de la base de données relationnelle ou non relationnelle (PostgreSQL vs MongoDB) à l'aide d'outils comme DB-Engines pour comparer leur performance, évolutivité et intégration.
- **Gestion des versions** : Justifier l'utilisation de Git avec des services comme GitHub ou GitLab pour la gestion des versions et le contrôle des changements

4) METHODOLOGIE, OUTILS DE GESTION DE PROJET, ORGANISATION :

La méthodologie choisie et les outils de gestion de projet utilisés doivent permettre une gestion efficace du développement, de la collaboration et du suivi du projet.

Contenu attendu :

- **Méthodologie de gestion de projet :** Présentation de la méthodologie choisie (Scrum, Kanban, cycle en V, etc.) et des raisons de ce choix. Décrire les étapes du cycle de vie du projet (sprints, itérations, etc.).
- **Organisation de l'équipe :** Rôles et responsabilités au sein de l'équipe projet (Product Owner, Scrum Master, développeurs, etc.).
- **Outils de gestion de projet :** Outils utilisés pour le suivi des tâches, la gestion des sprints, les échanges (Trello, Jira, Confluence, Slack, etc.).
- **Processus de collaboration :** Description des réunions (stand-ups, rétrospectives, démos, etc.) et des livrables attendus à chaque étape du projet.
  Suivi qualité : Outils et processus mis en place pour suivre la qualité du code, les tests unitaires et les revues de code.

Outils technologiques pour Systèmes, Réseaux, Cloud :

- **Planification cloud et virtualisation :** Utilisez Microsoft Project ou Wrike pour créer des diagrammes de Gantt spécifiques aux tâches de configuration réseau, systéme, et déploiements cloud.
- **Gestion des tâches réseau et virtualisation :** Utilisez Smartsheet ou TeamGantt pour planifier la configuration des serveurs, le déploiement des machines virtuelles, conteneurs ou machines et la gestion des sauvegardes.
- **Outils d'automatisation :** Utilisez des outils comme Ansible pour gérer la configuration des systèmes et automatiser les processus de déploiement.
- **Gestion des configurations :** Utilisez Gitlab ci, Puppet ou Chef pour gérer la configuration des infrastructures.
- **Outils de gestion de projet :** Utilisez des outils comme Jira ou Trello pour suivre les tâches, les deadlines et la progression du projet.

Outils technologiques pour Développement Full Stack :

- **Gestion des sprints :** Utilisez Jira ou Trello pour organiser les sprints, suivre les user stories et les tâches techniques du projet.

- **Outils de collaboration :** Utilisez Slack ou Microsoft Teams pour améliorer la communication entre les développeurs.
- **Revues de code :** Utilisez des outils comme Gitlab pour mettre en place des revues de code automatisées (code reviews).

5) PLANNING GANTT :

Le diagramme de Gantt permet de visualiser le planning global du projet, les tâches à accomplir et les dates de début et de fin prévues pour chaque tâche.

Contenu attendu :

- Décomposition des tâches : Toutes les étapes du projet doivent être décomposées en tâches détaillées (conception, développement, tests, déploiement, etc.).
- Durée et dates de début et fin : Chaque tâche doit avoir une durée définie, avec des dates précises de début et de fin.
- Dépendances : Les relations entre les tâches (quelles tâches doivent être réalisées avant d'autres).
- Milestones : Inclusion de jalons (milestones) pour valider les étapes clés du projet.
  Ressources : Association des membres de l'équipe projet aux différentes tâches.

Outils pour créer un diagramme de Gantt

Chaque groupe est libre du choix de la solution utilisée pour créer et à gérer le diagramme de Gantt.

- **Logiciels dédiés à la gestion de projet :**
  - **Microsoft Project :** Un des outils les plus connus, offrant de nombreuses fonctionnalités avancées.
  - **Asana :** Une solution collaborative en ligne, idéale pour les petites et moyennes équipes.
  - **Trello :** Un outil visuel et flexible, parfait pour les projets agiles.
  - **Monday.com :** Une plateforme personnalisable qui s'adapte à différents types de projets.
  - **Logiciels bureautiques :**
    - **Excel :** Vous pouvez créer un diagramme de Gantt simple avec Excel, bien qu'il soit moins adapté pour les projets complexes.
- **Outils en ligne gratuits :**
  - **Lucidchart :** Un outil de création de diagrammes en ligne très complet.
  - **GanttPRO :** Spécialisé dans les diagrammes de Gantt, il offre une interface intuitive.
  - **Creately :** Un autre outil en ligne polyvalent pour créer différents types de diagrammes.

II.4 - SOUTENANCE ET DEMO DU PROJET

Calendrier : 12 juin

Modalités : Epreuve de jury comptant pour 80 % de la note d'oral du bloc 2 « Coordonner une équipe projet »

Objectifs :

En s'appuyant sur la présentation de la solution technique mise en œuvre et la méthodologie pour y parvenir, la soutenance a pour but de valider le bloc de compétences « **Coordonner une équipe projet »**

- Transmission d'informations autour des étapes du projet
- Entretien de la relation client
- Supervision des collaborations avec les parties prenantes
- Conduite des échanges avec l'ensemble des parties prenantes

Composition du Jury

- A minima 2 personnes dont un professionnel.
- Peut-être hybride entre distanciel et présentiel

Durée :

1h par groupe (40' de présentation en groupe + 20' de questions-réponses)

Déroulé :

Le groupe présente le projet via un PPT ainsi qu'une démonstration de l'application.
Dans la présentation, les thèmes suivants doivent absolument être abordés et sont évalués :

<u>Entretien de la relation client</u>

- Comment avez-vous mené les interactions avec le client ;
- Comment vous êtes-vous assurés de répondre au besoin client ;
- Adaptation et réaction vis-à-vis des attentes du client

<u>Supervision des collaborations avec les parties prenantes</u>
La collaboration dans le groupe :

- Répartition des tâches – comment en avez-vous réalisé l'attribution
- Comment avez-vous obtenu une coordination efficace (moyen de communication, outils (Trello, Jira… & méthodes (Kanban, Scrum …)
- Comment avez-vous traité les points de désaccord et avez-vous tranché

<u>Conduite du changement et fédération d'une équipe projet</u>

- Quelles ont été les problématiques rencontrées par le groupe et comment ont-elles été solutionnées ou contournées
- Capacité à convaincre l'utilisateur final via la démo :
    - Maquettes / Captures d'écran compréhensible
    - Format adapté
    - Qualité de la démo (compréhensible, clair, organisée, argumentation des points forts de l'application)
    - Qualité de la présentation du groupe, crédibilité vis-à-vis du client via les supports et la qualité des prises de paroles et la pertinence des propos

- Capacité de l'équipe à répondre aux questions du Client / Jury

Evaluation :

Le jury attribuera une note commune au groupe.

Il pourra évaluer l'engagement de chaque membre si nécessaire en abaissant ou relevant l'évaluation collective de 2 points maximum pour chacun des membres si des différences notables (qualité et professionnalisme des réponses / implication / pédagogie) …) sont constatées.

II.5 - RENDU FINAL

Calendrier : 30 juin

Modalités : Compte pour 100 % de la note du bloc 3 « Superviser un projet informatique »

Rendu attendu : Il s'agit de l'ultime rendu du projet contenant :

- Le DAT ;
- L'ensemble de la documentation du projet ;
- Le code du projet ;
- L'ensemble des éléments techniques outils, etc

DAT

La stratégie du DAT/DCT cible doit répondre à plusieurs objectifs clés : aligner les exigences techniques et fonctionnelles, garantir la scalabilité et la performance, et s'assurer que l'architecture est évolutive et maintenable à long terme.

Voici un cadre de modèle stratégique pour l'architecture cible :

1. Vision et Objectifs de l'Architecture

Objectif principal : Créer une architecture qui supporte les objectifs techniques et fonctionnels du projet, tout en assurant une performance optimale, une sécurité renforcée et une évolutivité à long terme.

Vision : Bâtir une architecture modulaire, évolutive et résiliente qui permet une intégration facile avec d'autres systèmes, tout en assurant une haute disponibilité, une récupération rapide en cas de panne, et une facilité de maintenance.

2. Approche Modulaire et Evolutive

Architecture microservices : Séparer les fonctionnalités en modules ou services indépendants, chacun géré et déployé de manière autonome. Cela favorise la flexibilité, les mises à jour incrémentales et la réutilisation de services. Par exemple, chaque microservice gère une fonctionnalité distincte comme l'authentification, les paiements, etc.

API-first : Toutes les interfaces de communication entre les systèmes internes et externes passent par des API, assurant ainsi une standardisation et facilitant l'intégration avec des services externes.

3. Adoption d'une stratégie Cloud-First

Cloud hybride ou multi-cloud : Tirer parti des solutions cloud pour la flexibilité, tout en maintenant certaines infrastructures critiques sur site si nécessaire (par exemple, pour des raisons de conformité ou de sécurité).

Conteneurisation et Orchestration : Utilisation les micro-services pour encapsuler les services, et d’une solution technique pour orchestrer les déploiements en assurant l'évolutivité et la haute disponibilité.

Infrastructure as Code (IaC) : Automatisation des déploiements et de la gestion de l'infrastructure via des solutions pour garantir la cohérence et la rapidité des déploiements.

4. Sécurité et résilience intégrées

Sécurité by Design : Intégrer la sécurité dès la conception avec des contrôles stricts d'accès, la gestion des identités, et la protection des données (chiffrement, audits de sécurité réguliers).

Redondance et tolérance aux pannes : Mettre en place des mécanismes de redondance (clustering des bases de données, backups fréquents, réplicas de serveurs) pour garantir la continuité de service en cas de panne.

Gestion des risques : Identification et gestion proactive des risques liés à la cybersécurité, aux défaillances matérielles, ou à la surcharge du système.

5. Stratégie d’optimisation des performances

Scalabilité horizontale et verticale : Permettre à l'architecture de grandir avec le projet en ajoutant des ressources (scalabilité horizontale) ou en augmentant les capacités des ressources existantes (scalabilité verticale).

Caching et CDN (Content Delivery Network) : Utiliser des mécanismes de cache pour réduire la latence des services et des CDN pour distribuer le contenu mondialement avec un temps de réponse optimal.

Surveillance et maintenance proactive : Intégrer des outils de monitoring en temps réel pour surveiller les performances et réagir rapidement à tout problème détecté.

6. Automatisation et DevOps

Pipelines CI/CD : Mettre en place des pipelines d'intégration et de déploiement continus pour automatiser les tests, la revue de code et les déploiements en production.

Tests automatisés : Automatisation des tests unitaires, d'intégration et de performance pour garantir que chaque mise à jour n'introduit pas de régression.

Infrastructure automatique : Utiliser des outils pour automatiser la configuration des serveurs et la gestion des environnements, minimisant ainsi les erreurs humaines.

7. Stratégie de Gouvernance et de Conformité

Gouvernance des données : Assurer la conformité aux réglementations locales et internationales (GDPR, HIPAA, etc.) via une gestion stricte des données, leur chiffrement et des audits réguliers.

Politiques de gestion des accès : Mettre en place des politiques strictes pour limiter l'accès aux ressources sensibles et garantir que seuls les utilisateurs autorisés peuvent accéder aux informations critiques.

Gestion des audits et des journaux : S’assurer que l'architecture permet une traçabilité complète, avec des journaux d’accès et d'événements pour toutes les interactions importantes.

8. Innovation et Agilité

Adaptabilité technologique : Se maintenir à jour avec les nouvelles technologies et les tendances, et intégrer rapidement de nouveaux outils ou si cela devient nécessaire pour répondre aux besoins du projet.

Prototypage rapide : Utiliser des environnements de développement rapides pour tester de nouvelles idées ou composants sans impacter la production.

II.5-BIS - ANALYSE PERSONNELLE DE LA DYNAMIQUE DU PROJET

Calendrier : 30 juin

Modalités : Travail individuel à rendre à l'issue du projet. Compte pour 20 % de la note du bloc 2 « Piloter un projet Informatique ».

Compétence évaluée : Mobilisation d'une équipe projet et conduite du changement

Rendu attendu :

A partir de votre analyse du travail collectif réalisé tout au long du projet d'étude, vous **présenterez individuellement une analyse de la dynamique du groupe projet ainsi qu'un bilan de votre communication / participation au sein de ce dernier**, en répondant par exemple aux questions :

- Quel a été votre apport technique au cours du projet ? Qu'avez-vous amené, qu'avez-vous à l'inverse appris des autres membres ?
- A votre avis, comment les spécificités des membres du groupe ont-elles été prise en compte ? En particulier, quelles démarches collaboratives et inclusives ont-elles déployées ?
- Comment a fonctionné le groupe, qu'est-ce que vous avez amené / proposé pour la dynamique et la coordination du projet ?
- Comment le groupe a-t-il traité les points de désaccord et a tranché ? Votre analyse.
- Quelles difficultés avez-vous rencontrées lors du projet, comment les avez-vous surmontées ?
- Quelle est votre vision du projet abouti, les points positifs et les points d'amélioration si c'était à refaire ?
- Pour vous que ressort-il de ce projet et de cette expérience, qu'avez-vous appris pour l'avenir ?

Livrable à fournir :

- Dossier rédigé de 10 pages de texte.

X. Résumé & timeline de rendu :

Rendu	Contenu (non exhaustif, cf XIX)	Date de rendu	Type de rendu	Forme de rendu
Rendu 1 : Proposition d'architecture et plan détaillé	- **Architecture réseau** : Schéma des interactions entre les différents services (SOC, EDR/XDR, VPN, etc.). - **Diagrammes techniques** : Diagramme des flux de données, topologie du réseau (LAN/WAN/Cloud). - **Choix technologiques** : Justification des choix (cloud hybride, SD-WAN, firewalls, etc.).	28/03	Travail de groupe	Présentation (PPTX), Schémas (PDF)
Rendu 2 : REX / analyse personnelle	- **Rôles et responsabilités** : Contributions individuelles dans le projet d'architecture. - **Défis rencontrés** : Problèmes techniques, organisationnels ou méthodologiques. - **Solutions apportées** : Comment les problèmes ont été résolus. - **Analyse critique** : Réflexion sur les choix technologiques et les méthodologies utilisées. - **Améliorations possibles** : Suggestions pour les futures itérations du projet.	02/07	Travail individuel	Rapport écrit (PDF, minimum 10 pages)
Rendu 3 : Document de conception technique complet (groupe)	- **Repository GIT pour scripts d'automatisation** : Scripts Terraform, Ansible, etc., pour l'infrastructure. - **Configuration réseau** : Paramétrages des équipements réseau via IaC (Infrastructure as Code). - **Automatisation des services cloud** : Déploiement cloud hybride et configuration automatisée. - **Documentation technique** : Guide de déploiement, structure du code, documentation des API. - **Suivi des livrables** :	02/07	Travail de groupe	Code (GIT), Document technique (PDF)

Rendu	Contenu (non exhaustif, cf XIX)	Date de rendu	Type de rendu	Forme de rendu
	Documentation des sprints et avancement via GIT.			

- **Légende des colonnes :**
- **Contenu** : Détails sur ce qui doit être inclus dans chaque rendu.
- **Date de rendu** : Date à laquelle chaque rendu est attendu.
- **Type de rendu** : Précise si le rendu est un travail de groupe ou individuel.
- **Forme de rendu** : Format dans lequel le travail doit être rendu (PPTX, PDF, code sur GIT, etc.).