<<Cisco Business Critical Services>>
Services opérationnels essentiels Cisco

Services pour l'ingénierie

Ce document contient la description détaillée des capacités et des livrables associés aux Services opéwrationnels essentiels Cisco pour l'ingénierie.

Remarque : Le présent document doit être lu conjointement avec les Conditions générales des Services opérationnels essentiels Cisco.

Liens de navigation :

Nom du document	Lien
Conditions générales des services opérationnels essentiels Cisco	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_General_Terms.pdf
Services opérationnels essentiels Cisco pour les opérations	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Operations.pdf
Services opérationnels essentiels Cisco pour l'ingénierie	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Engineering.pdf
Services opérationnels essentiels Cisco pour l'architecture	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Architecture.pdf

TABLE DES MATIÈRES

Aperçu des Services pour l'ingénierie

Les Services pour l'ingénierie englobent les capacités et les livrables à l'appui de la conception et de la validation, de la maîtrise des applications, de l'analyse des menaces, de l'automatisation, des programmes de sécurité et du renforcement de l'infrastructure et de l'environnement d'applications de Cisco. Les livrables décrits dans le volet Services pour l'ingénierie sont regroupés par capacités, puis par technologies, solutions et architectures prises en charge.

Capacités et livrables des Services pour l'ingénierie

Les capacités et les livrables du volet Services pour l'ingénierie aident les clients à évoluer et à s'adapter rapidement en fonction des exigences et des technologies en constante transformation et en vue de l'accélération du changement au sein de leur infrastructure et de leurs applications.

1. INGÉNIERIE DE LA CONCEPTION

L'ingénierie de la conception aide les clients à mettre en œuvre des pratiques exemplaires, des renseignements et des recommandations en matière de conception, de validation et d'ingénierie des fonctionnalités afin d'accélérer et de faire avancer leur conception de l'infrastructure et des applications.

Navigation par section

La **section Ingénierie de la conception** inclut les capacités et les livrables des services suivants, qui sont tous associés à un signet pour faciliter la navigation :

1.1. Conception et validation

Le service de conception et de validation est axé sur l'offre de recommandations et de soutien concernant le développement, l'amélioration, la validation et la prise en charge des applications et des conceptions de l'infrastructure pour atteindre les objectifs en matière d'activités auprès des clients et de conception de solution.

1.1.1. Étude de la conception

L'étude de la conception aide le client à vérifier que les conceptions intègrent les meilleures pratiques de Cisco afin de remplir les exigences commerciales et techniques actuelles et futures en matière de fonctionnalités, de résilience, d'efficacité et d'évolutivité.

L'étude se concentre sur l'évaluation de la solution du client et des exigences techniques de conception, l'évaluation de la capacité actuelle et de l'évaluation des risques et la formulation de recommandations de conception pour la réalisation des objectifs du client.

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Gestion et orchestration de réseau
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services
- Réseautique industrielle et collaboration

Solutions prises en charge

- Réseau étendu défini par logiciel
    - Routage et commutation
    - Gestion et orchestration de réseau
- Accès défini par logiciel
    - Routage et commutation
    - Réseau sans fil

- Virtual Packet Core
  - Réseau central de transmission par paquets
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
  - Gestion et orchestration de réseau
  - Politique de sécurité et accès
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage
- Réseau à optimisation autonome
  - Politique de mobilité et accès

Responsabilités de Cisco

- Analyser les répercussions et les risques des nouvelles exigences et des modifications (comme les configurations et les protocoles) associées à la conception existante.
- Élaborer une feuille de route des conceptions à venir optimisées pour la résilience, la disponibilité, la sécurité et l'évolutivité.
- Vérifier que les plateformes, les fonctions et les fonctionnalités recommandées respecteront les objectifs de conception communiqués par le client.
- Recommander et examiner les modifications apportées aux renseignements la conception, notamment :
  - Les modifications générales ou précises apportées à la conception.
  - Les principaux risques et les plans d'action recommandés par rapport aux modifications de la conception proposées.
  - La topologie et l'architecture logiques et physiques et, s'il y a lieu, le diagramme de topologie.
  - Les politiques de provisionnement.
  - Les modèles de configuration des appareils Cisco.
  - Les fonctions et fonctionnalités des logiciels Cisco.
  - La compatibilité de la plateforme matérielle.
  - La continuité des activités et du service, ainsi que la reprise après sinistre.
  - Les améliorations de l'efficacité opérationnelle à l'aide de nouvelles fonctionnalités, de mises à jour de la configuration et des améliorations des processus.

Remarque : Cisco n'est pas responsable de l'élaboration des documents de conception dans le cadre de ce livrable, mais il aidera à répondre aux questions de conception liées à la mise en œuvre de nouvelles fonctionnalités.

Livrable

- Rapport de l'étude de la conception

Responsabilités du client

- Élaborer le document de conception complet en vue du déploiement de toutes les nouvelles fonctionnalités ou de toute nouvelle application.
- Réviser et mettre à jour le protocole des tests d'acceptation et le plan d'assistance continue pour la conception détaillée, comme recommandé par Cisco.

Restriction

** Propre au réseau optique*

- Un (1) rapport sur l'étude de conception porte sur 20appareils au plus.

1.1.1a. Étude de la conception – Service à la clientèle

Les responsabilités suivantes en matière d'étude de la conception fondée sur la logique de routage des appels s'appliquent particulièrement au service à la clientèle dans les domaines décrits ci-dessous :

- Étude de la conception des scénarios
- Étude de la conception du routage de précision

Étude de la conception des scénarios

Technologies prises en charge

- Service à la clientèle

Responsabilités de Cisco

- Discuter avec le client des scénarios à examiner.
- Passer en revue les scénarios prédéterminés relevés par le client (jusqu'à 12 au total).
- Effectuer un examen des scénarios relevés par le client et fournir des recommandations.
- Relever les méthodologies qui entrent en conflit avec les meilleures pratiques et les recommandations.
- Relever les situations dans lesquelles les scénarios peuvent être modifiés pour améliorer l'efficacité de l'administration des scénarios.
- Examiner la cohérence et le respect des normes reproductibles des scénarios du client.
- Présenter des stratégies de conception de scénario normalisées dans l'ensemble des applications et de l'entreprise.
- Collaborer et planifier des stratégies de mise en œuvre pour apporter les modifications recommandées aux scénarios.

Livrable

- Rapport d'examen de la conception de scénarios

Responsabilités du client

- Fournir un accès à la bibliothèque de scénarios.
- Fournir un accès aux ressources du client ou du développeur pour examiner les composants de scénario personnalisés et provenant de tiers qui interagissent avec les scénarios standard.

Restrictions

** Propre au service à la clientèle*

Les éléments suivants ne sont pas fournis dans le cadre de l'examen de conception des scénarios pour le service à la clientèle :

- Examens et recommandations de scénarios dépassant la quantité convenue.
- Configuration des solutions Cisco Unified Communications Manager (CUCM).
- Multiplexage par division dans le temps (Time-Division Multiplexing ou TDM) automatisé de la configuration du système de distribution automatique des appels (Automated Call Distribution ou ACD).
- Applications tierces, intégrations et objets de scénario (par exemple, Java personnalisé).
- Reconnaissance de la voix et scénarios de synthèse texte-parole (à l'exception des solutions intégrées).
- Objets ou codes développés de façon personnalisée (par exemple, un code Java personnalisé dans le scénario Unified Customer Voice Portal Studio).
- Rapprochement des données de rapport.
- Dépannage et escalade au centre d'assistance technique (TAC) de Cisco des problèmes liés aux scénarios.

Étude de la conception du routage de précision

Technologies prises en charge

- Service à la clientèle

Renseignements supplémentaires à recueillir

- Modifications du processus opérationnel nécessaires pour mettre en œuvre le routage de précision.
- Règles commerciales actuelles et propositions d'acheminement des appels de routage postprécision.

Responsabilités de Cisco

- Déterminer ce qui suit :
    - Les secteurs d'activité qui englobent plusieurs sites et qui nécessitent des aptitudes avancées en configuration et en routage.
    - Les exigences de rapport et la façon dont les politiques de rapport actuelles devront changer en raison de la mise en œuvre du routage de précision.
    - Les règles commerciales actuelles et la façon dont elles changeront en raison du routage de précision proposé pour le routage des appels.
    - Les schémas de flux d'appels servant à évaluer l'applicabilité du routage de précision.

- La configuration des groupes de compétences afin d'identifier les personnes qui bénéficieront du routage de précision.
- Les documents supplémentaires approuvés lors de la réunion de lancement pour les détails des règles commerciales actuelles et les propositions d'acheminement des appels de routage post-précision.

- Présenter les stratégies de conception de routage de précision dans différents secteurs d'activité, dans de multiples sites et l'entreprise.
- Présenter comment la gestion de la file d'attente change d'un secteur d'activité à un autre.
- Collaborer avec le client pour planifier une stratégie de mise en œuvre.

Livrable

- Rapport de l'étude de la conception du routage de précision

Restrictions

** Propre à l'étude de la conception du routage de précision pour le système de service à la clientèle*

Les éléments suivants ne sont pas fournis dans le cadre de l'étude de la conception du routage de précision :

- Examens et recommandations de scénarios dépassant la quantité convenue.
- Configuration de CUCM.
- Configuration du MDT du système de DA.
- Applications tierces, intégrations et objets de scénario (par exemple, Java personnalisé).
- Reconnaissance de la voix et scénarios de synthèse texte-parole (à l'exception des solutions intégrées).
- Objets ou codes développés de façon personnalisée (par exemple, un code Java personnalisé dans le scénario Unified Customer Voice Portal Studio).
- Rapprochement des données de rapport.
- Le dépannage et le signalement au TAC de Cisco des problèmes liés aux scénarios.

1.1.1b. Étude de la conception – Orchestration et automatisation du centre de données

L'étude de la conception aide le client en fournissant des conseils et des recommandations concernant l'infrastructure actuelle de l'automatisation de la gestion du client, comme l'orchestration, les outils de provisionnement et le portail de gestion, qui sont nécessaires pour prendre en charge une infrastructure infonuagique capable d'offrir une infrastructure-service (IaaS) en nuage ou un service d'infrastructure de nuage hybride.

Technologies prises en charge

- Orchestration et automatisation de centre

Responsabilités de Cisco

- Analyser l'incidence des exigences d'intégration nouvelles ou supplémentaires et optimiser le déploiement actuel.
- Offrir une assistance en matière de conception en alignant l'évolution de l'architecture d'automatisation, d'intégration et de gestion sur le développement du modèle de service.
- Examiner les interfaces utilisateurs pour adapter la solution aux besoins du client.

Livrable

- Rapport d'évaluation de la conception de l'automatisation, de l'intégration et de la gestion

1.1.1c. Étude de la conception – Orchestration du service réseautique

Cette étude de conception aide les clients à concevoir et à mettre en œuvre efficacement les capacités d'orchestration des services au sein de leur infrastructure Cisco.

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau

Responsabilités de Cisco

- Analyser l'incidence des nouvelles exigences sur l'orchestration de services actuelle.
- Offrir une assistance en matière de conception en alignant la conception de l'orchestration des services sur l'évolution de l'architecture de déploiement et le développement du modèle de service.

Livrable

- Rapport sur la conception de l'orchestration des services

1.1.2. Assistance permanente à la conception

L'assistance permanente à la conception aide le client en offrant des conseils et des recommandations sur l'ajout de modifications aux conceptions du client. L'examen vise à évaluer les exigences de modification du client, en effectuant une analyse des écarts sur l'état actuel de la conception et en offrant des recommandations sur la mise en œuvre ou la modification de ces conceptions selon les pratiques exemplaires publiées et les normes de l'industrie.

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Gestion et orchestration de réseau
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Infrastructure centrée sur les applications
- Orchestration et automatisation de centre de données
- Communications unifiées
- Service à la clientèle
- Collaboration vidéo
- Réunions et messagerie infonuagiques
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services
- Réseautique industrielle et collaboration

Solutions prises en charge

- Réseau étendu défini par logiciel
  - Routage et commutation
  - Gestion et orchestration de réseau
- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Gestion et orchestration de réseau
  - Politique de sécurité et accès

- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données
  - Réseau central de transmission par paquets
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Responsabilités de Cisco

- Formuler des recommandations pour mettre en œuvre les modifications à la conception du client, notamment :
  - Risques connus et possibles en cause.
  - Répercussions sur l'environnement actuel du client.
- Fournir des conseils continuels au sujet des exigences susmentionnées qui peuvent avoir une incidence sur les conceptions actuelles du client.

Remarque : Cisco n'est pas responsable de l'élaboration des documents de conception dans le cadre de ce service, mais aidera à répondre aux questions de conception liées à la mise en œuvre de nouvelles fonctionnalités.

Autres responsabilités

** Propre aux communications unifiées, au service à la clientèle, à la collaboration vidéo et aux réunions et à la messagerie infonuagiques*

- Effectuer un examen pour chaque modèle de site dans les déploiements multisites.
- Discuter du matériel et des logiciels nécessaires pour répondre aux exigences de capacité et de croissance, y compris les problèmes liés aux composants de fin de vente ou de fin de durée de vie.
- Examiner le plan détaillé du client pour évaluer la croissance indiquée en offrant des recommandations afin d'atténuer tout problème possible.

** Propre à l'infrastructure centrée sur les applications*

- Offrir une assistance en vue des modifications et des améliorations apportées à la trame de l'infrastructure axée sur les applications (Application Centric Infrastructure ou ACI™) afin de respecter les nouvelles exigences liées à l'évolutivité et les autres exigences d'intégration et d'optimiser l'architecture actuelle.
- Formuler des recommandations, notamment sur les modifications précises apportées à la trame d'ACI de couche 2 ou 3 afin de répondre aux nouvelles exigences.

- Fournir un résumé de tous les aspects de la conception, y compris le routage, la sécurité, la haute disponibilité, l'intégration des services des couches 4 à 7 (L4 à L7) pour les trousses d'appareils standard, publiées et prises en charge. Remarque : Les configurations matérielles ou logicielles et le soutien des appareils de service des couches L4 à L7 fournis par des tiers ne sont pas inclus dans ce service.

Livrable

- Rapport d'assistance à la conception

Restrictions

** Propre à l'orchestration et à l'automatisation de centre de données*

- Pour Cisco CloudCenter™ (CCC), ce livrable ne couvre que la conception des éléments suivants :
    - Composants de CCC
    - Applications et services créés à l'aide de la plateforme Cisco CloudCenter.

** Propre au réseau optique*

    - Un (1) rapport d'assistance à la conception porte sur un maximum de 20 appareils.

1.1.3. Développement de la conception

La mise au point de la conception permet d'offrir des conseils et une assistance dans l'élaboration ou l'amélioration des conceptions de l'infrastructure de Cisco (générale ou précise).

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Sécurité de réseau
- Orchestration et automatisation de centre de données
- Sécurité du nuage
- Menace avancée
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Politique de sécurité et accès

Solutions prises en charge

- Accès défini par logiciel
    - Routage et commutation
    - Réseau sans fil
    - Gestion et orchestration de réseau
    - Politique de sécurité et accès
- Réseau étendu défini par logiciel
    - Routage et commutation
    - Gestion et orchestration de réseau
- Virtual Packet Core
    - Réseau central de transmission par paquets

Responsabilités de Cisco

- Aider le client à vérifier que les plateformes, les fonctions et les fonctionnalités choisies respecteront les objectifs de conception communiqués par le client.
- Aider le client à créer le document de conception, qui peut comprendre les éléments suivants :
    - Objectifs et priorités associés aux activités, aux applications et aux éléments techniques.
    - Exigences de conception générales ou précises.

- Recommandations de conception.
- Principaux risques associés à la conception proposée.
- Topologie et architecture logiques et physiques.
- Modèles de configuration des appareils d'infrastructure Cisco.
- Recommandations pour les nouvelles versions logicielles selon les caractéristiques et les fonctionnalités de la conception.
- Considérations relatives à la plateforme matérielle et logicielle.

Livrable

- Document de conception

Restrictions

** Propre à la sécurité du réseau, à la sécurité du nuage, à la politique de sécurité et d'accès et à la protection avancée contre les menaces*

- Les responsabilités de Cisco sont limitées à un (1) ensemble de solutions complexes (par exemple, les déploiements Cisco ISE, Cisco Secure ACS et 802.1x), ou à une (1) solution non complexe configurée pour un maximum de quarante (40) appareils.

** Propre au réseau optique*

- Prise en charge des documents de conception d'un maximum de vingt (20) appareils.

1.1.4. Prise en charge des modifications de conception

Le soutien pour les modifications de conception consiste en une aide pour évaluer la faisabilité et les répercussions possibles des modifications proposées aux conceptions des clients.

Le soutien est axé sur l'évaluation des exigences et des risques de modification de la conception du client, la vérification de la planification du changement du client, la mise en œuvre, les procédures de soutien et l'assistance à distance au personnel du client pendant les fenêtres de changement prévues.

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Infrastructure centrée sur les applications
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services
- Réseautique industrielle et collaboration

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Réseau central de transmission par paquets
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau

Responsabilités de Cisco

- Examiner les processus de planification, de mise en œuvre et de soutien de la clientèle liés aux modifications de conception proposées qui peuvent comprendre un ou plusieurs des domaines suivants :
    - Évaluation et les priorités de planification des modifications.
    - Analyse des répercussions des modifications sur l'architecture, les conceptions ou les configurations déployées, ainsi que sur les politiques et les fonctions des applications.
    - Méthodes de procédures (MOP) de mise en œuvre des modifications fondées sur les meilleures pratiques de Cisco.
    - Priorités potentielles de réduction des risques et mesures requises.
    - Plan de soutien, ressources et rôles liés à la mise en œuvre des modifications.
    - Processus de vérification de l'atteinte des objectifs de modifications.
    - Stratégie de sauvegarde associée aux modifications de conception planifiées.
- Fournir un document de recommandations de prise en charge des modifications de conception qui résume l'information recueillie, l'analyse des résultats et les recommandations (si Cisco le juge nécessaire).
- Fournir une personne-ressource de soutien à distance Cisco désignée pour offrir des conseils et répondre aux demandes des clients pendant les périodes de modifications de conception prévues.
- Collaborer avec le client pour vérifier l'état de préparation des systèmes pendant les fenêtres de changement de conception à la demande du client.
- Travailler avec le client pour rendre accessible, à la réception au moins vingt et un (21) jours avant la demande écrite du client à Cisco, une personne-ressource de soutien désignée qui peut accepter les appels pendant les heures d'ouverture standard, et offrir une disponibilité 24 heures sur 24, 7 jours sur 7.

Responsabilités exclues

** Propre à l'infrastructure centrée sur l'application (ACI)*

- Pour l'infrastructure ACI, Cisco ne fournira pas de rapport sur les recommandations de prise en charge des modifications de conception.

Autres responsabilités

** Propre à la sécurité de réseau, à la politique de sécurité et d'accès, à la sécurité du nuage et à la protection avancée contre les menaces*

- Fournir un soutien pour les modifications de conception des plans du client (p. ex., illustrations du réseau, plan de mise en œuvre, plan de test et plan de restauration) et les modifications de configuration (p. ex., configuration des appareils et modifications du câblage).

** Propre au document de MOP pour le routage et la commutation, au réseau optique, au réseau sans fil, aux systèmes informatiques, au réseau de stockage, à la commutation de centre de données et au réseau central de transmission de paquets*

- Formuler des recommandations de modifications au plan de mise en œuvre, à la méthode de procédure et au plan de test du Client en fonction des données recueillies auprès du Client, de l'analyse des modifications proposées et des meilleures pratiques de Cisco.

- Fournir un document de MOP pour la plateforme Cisco au client qui peut comprendre les éléments suivants dans le soutien d'un changement de conception :
    - Procédures à suivre avant et après la mise en œuvre de modifications à la configuration ou au logiciel.
    - Procédures de restauration de la configuration planifiée ou des modifications logicielles.

Livrables

- Rapport sur les recommandations de prise en charge des modifications de conception
- Document de MOP (spécifique aux technologies prises en charge)

Remarque : Un document de MOP prend en charge un changement de conception, de configuration ou de mise à jour logicielle proposé ou prévu pour une technologie et une plateforme prises en charge par Cisco.

Restrictions

- Cisco n'est pas responsable de l'élaboration ou de la mise à l'essai de toute méthode de procédure liée aux modifications de conception planifiées ou proposées du client.
- Cisco n'est pas responsable de l'élaboration de méthodes de procédures (MOP) pour les plateformes non-Cisco et les technologies non mentionnées spécifiquement dans les responsabilités supplémentaires de Cisco spécifiques au document MOP.

** Propre à la sécurité de réseau, à la politique de sécurité et d'accès, à la sécurité du nuage et à la protection avancée contre les menaces*

- Les modifications ne peuvent pas englober plus de deux (2) dispositifs de sécurité ou deux (2) paires de dispositifs de sécurité (p. ex., des paires de pare-feu, un actif et un de secours).
- Les modifications ne peuvent pas couvrir plus de dix (10) périphériques réseau.
- La période d'assistance dans le cadre des modifications ne peut pas excéder huit (8) heures. Il ne peut pas y avoir plus de deux (2) périodes d'assistance pour les modifications. Le soutien aux modifications peut avoir lieu après les heures d'ouverture standard.
- Modifications d'urgence : la capacité de Cisco à soutenir une modification d'urgence dépend de la disponibilité des ressources. Cisco n'a aucunement l'obligation de fournir son assistance dans le cadre d'une modification urgente si elle est dans l'impossibilité d'affecter un expert-conseil spécialiste en sécurité Cisco pour la tâche.
- Modifications prévues : Pour les modifications planifiées (prévus vingt et un (21) jours civils à l'avance), Cisco affectera un ingénieur-conseil en sécurité Cisco.

* Propre au réseau optique

- Un (1) soutien aux modifications de conception couvre jusqu'à vingt (20) appareils.
- Un (1) soutien aux modifications de conception couvre jusqu'à deux (2) périodes de prise en charge des modifications.

** Propre au document de MOP pour les technologies suivantes : routage et commutation, réseau optique, réseau sans fil, systèmes informatiques, réseau de stockage, commutation de centre de données et réseau central de transmission de paquets.*

- La modification de l'analyse d'impact n'est pas effectuée à l'aide d'outils de simulation.
- La vérification des recommandations de Cisco contenues dans le document de MOP est limitée à la vérification des modifications de configuration, des procédures de mise à jour logicielle et de restauration pour un système d'exploitation et une plateforme Cisco similaires dans le cadre des travaux pratiques de Cisco, si Cisco le juge opportun.
- Cisco n'est pas responsable du développement d'une MOP pour aucune technologie qui n'est pas spécifiquement indiquée dans les responsabilités supplémentaires de Cisco spécifiques au document de MOP.
- Le document de MOP n'est pas prévu pour la migration d'une plateforme Cisco vers une autre plateforme Cisco.

1.1.5. tratégie de test et examen du plan

Le service de stratégie de test et d'examen du plan aide le client en lui fournissant une assistance dans l'évaluation des activités du client et des exigences et de contraintes d'essais opérationnels, en analysant les domaines de priorité aux fins d'examen ou d'amélioration, en fournissant un rapport qui indique la stratégie d'essai et de laboratoire de Cisco et en aidant les clients en matière de plan d'essai et d'analyse de résultats.

Technologies prises en charge

- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage

Exclusion

** Propre à l'orchestration et à l'automatisation de centre de données*

- Cisco CloudCenter (CCC) n'est pas pris en charge.

Responsabilités de Cisco

- Aider le client à élaborer le plan de test ou à examiner et à perfectionner le plan de test actuel, qui définit la portée suivante :
    - Objectif spécifique pour l'ensemble du plan de test et pour chaque test faisant partie du plan.
    - Processus ou étapes nécessaires, dépendances, calendrier et séquence de chaque test.
    - Périphériques matériels et versions logicielles de test nécessaires de Cisco et de tierces parties, y compris les configurations et les paramètres.
    - Résultats mesurables de test afin que l'on puisse déterminer un résultat positif ou négatif.
    - Concevoir un tableau des responsabilités de Cisco et du client concernant l'exécution du plan de test.
- Aider le client à exécuter le plan de test et documenter les résultats.
- Analyser les résultats de test et documenter l'analyse des résultats et des recommandations de Cisco dans un rapport de résultats de test.

Livrables

- Rapport d'examen de la stratégie de test et de laboratoire
- Rapport sur les résultats de test

Responsabilités du client

- Fournir l'installation et la configuration physiques du laboratoire de test et de l'équipement.
- Documenter et exécuter le plan de test avec l'aide de Cisco.
- Fournir des ressources techniques au client pour exécuter les cas de test particuliers (scénarios et charges de travail) dans des domaines du système relevés au préalable, comme l'indique le plan de test.
- Examiner et approuver le rapport des résultats de test.
- Offrir une assistance à la clientèle à distance selon les besoins pour les produits tiers ou concurrents de Cisco approuvés au préalable.
- Fournir l'équipement de tiers requis ou concurrent de Cisco nécessaire de Cisco (y compris l'expédition en direction et en provenance des installations de laboratoire de Cisco).

1.1.6. Évaluation de la stratégie de validation des tests et des laboratoires

L'évaluation de la stratégie de validation des tests et des laboratoires examine les pratiques et les principes de validation des tests actuels du client en matière de cohérence et d'automatisation de la conception, du développement et du déploiement des plans de test.

Architectures prises en charge

- Réseau de base
- Centre de données et nuage
- Collaboration
- Sécurité
- Services de mobilité des

Renseignements supplémentaires à recueillir

- Documents de l'environnement de test et objectifs des tests.

Responsabilités de Cisco

- Examiner l'environnement automatisé de validation du client, de même que les ressources, processus, outils, préoccupations et défis en la matière.
- Effectuer une analyse de l'environnement actuel de test et de validation du client pour l'un (1) des domaines suivants, comme indiqué dans le devis :
    - Évaluation générale de la stratégie de validation des laboratoires et des tests : examen de l'environnement, de la méthodologie, des outils, du plan de test et des résultats des tests du client. Identifier les opportunités d'amélioration des directives de planification des tests, des meilleures pratiques et des recommandations pour l'évaluation des résultats du rapport de test.
    - Évaluation de la stratégie de validation des laboratoires et des tests technologiques et des tests de migration de produit : comprend un (1) plan de test spécifique de la technologie ou de la migration et un (1) examen de la topologie de test du plan de test et des résultats des tests du client. Fournir des commentaires et des recommandations sur les meilleures pratiques.
    - Évaluation de la stratégie de validation des laboratoires et des tests de solutions : comprend un (1) plan de test spécifique de la solution et un (1) examen de la topologie de test du plan de test et des résultats des tests du client. Fournir des commentaires et des recommandations sur les meilleures pratiques.

Livrable

- Rapport d'évaluation générale de la validation des laboratoires et des tests
- Test de migration des produits et des technologies, et rapport d'évaluation de la validation des laboratoires et des tests
- Rapport d'évaluation de la validation des laboratoires et des tests de solutions

1.1.7. Validation de l'adoption et de la migration technologique

La validation de l'adoption et de la migration technologique aide les clients à planifier, à exécuter et à produire des rapports sur l'adoption de nouveaux cycles de test technologique. Cisco fournit des conseils pour tester la migration du matériel, des logiciels et de l'architecture, y compris la validation des mises à jour logicielles et des méthodes de procédure (MOP). Les tests sont réalisés dans un laboratoire Cisco avec le matériel et les outils de test applicables. Cas type d'adoption de la technologie.

Architectures prises en charge

- Réseau de base
- Centre de données et nuage
- Collaboration
- Sécurité
- Services de mobilité des fournisseurs de services

Solutions prises en charge

- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
    - Routage et commutation
    - Systèmes informatiques
    - Commutation de centres de données
- Secure Agile Exchange (SAE)
    - Routage et commutation
    - Systèmes informatiques
    - Commutation de centres de données

- Orchestration et automatisation de centre de données
- Réseau central de transmission par paquets
- Orchestration et automatisation de centre de données
- Sécurité du nuage

- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Responsabilités de Cisco

- Créer et documenter le plan de service d'adoption ou de migration technologique.
- Élaborer un plan de test
- Effectuer les essais décrits dans le plan de test ayant fait l'objet d'une entente entre Cisco et le client.
- Fournir un soutien qui peut comprendre, sans toutefois s'y limiter, ce qui suit :
  - Automatisation des tests – définir ou augmenter la portée des scénarios de tests automatisés.
  - Préparation et exécution des tests – exécution du plan de test et préparation du rapport de test.

Livrables

- Plan de mise à l'essai
- Rapport de test

1.1.8. Tests d'automatisation et d'intégration en continu

Le service de tests d'automatisation et d'intégration en continu fournit des conseils pour le développement de scénarios de tests automatisés pour les clients qui désirent revoir leurs scénarios de test manuels pour les faire migrer vers des scénarios de test automatisés afin d'accélérer la migration de nouvelles technologies et le déploiement de nouveaux services informatiques. Cisco utilise une bibliothèque de tests et un cadre d'automatisation pour développer les scénarios de test du client.

Architectures prises en charge

- Réseau de base
- Centre de données et nuage
- Collaboration
- Sécurité
- Services de mobilité des fournisseurs de services

Renseignements supplémentaires à recueillir

- Plan de test, conditions requises et objectifs pour le scénario de test et l'automatisation.

Responsabilités de Cisco

- Mettre au point à distance les scénarios de tests automatisés en fonction du plan de test fourni par le client.
- Passer en revue les scénarios de tests automatisés avec le Client.
- Installer et configurer le cadre de validation de l'automatisation (Cisco Automation Validation Framework) sur la plateforme du client, dans son laboratoire de validation.
- Fournir au client l'accès aux ressources désignées de la bibliothèque de tests d'automatisation Cisco pour effectuer des tests d'automatisation pendant toute la durée de ce service, comme indiqué dans le devis.

- Fournir les mises à jour et les services de maintenance pour l'environnement d'automatisation de Cisco.
- Exécuter les tests et fournir le rapport de test si cela est spécifié dans le devis.
- Intégrer la bibliothèque de tests automatisés Cisco au modèle CI/CD du client, si cela est spécifié dans le devis.

Livrables

- Scénarios de tests automatisés
- Rapport de test (si spécifié dans le devis)

Responsabilités du client

- Fournir la plateforme informatique spécifiée pour le serveur du cadre de validation de l'automatisation de Cisco.
- Passer en revue les scénarios de tests automatisés fournis par Cisco.
- Installer et préparer la plateforme informatique requise, comme demandé par Cisco, pour l'exécution de l'environnement d'automatisation de tests fourni par Cisco.
- Exécuter des tests d'automatisation selon le plan de test automatisé.
- Fournir à Cisco la liste du personnel, chez le client, qui aura des privilèges d'accès au répertoire de tests d'automatisation de Cisco.
- Fournir à Cisco des ressources et des renseignements détaillés pour mettre au point l'intégration du répertoire de tests d'automatisation de Cisco avec le modèle de CI/CD du client, si cela est indiqué dans le devis.

1.1.9. Validation de l'intégration continue du cycle de test

La validation de l'intégration continue du cycle de test offre des services de Conseil et de test de validation pour les clients nécessitant une simulation de réseau continue dans un laboratoire Cisco pour réduire les risques et accélérer le déploiement des nouvelles technologies, des logiciels, du matériel mises à jour de sécurité et autres modifications apportées.

Architectures prises en charge

- Réseau de base
- Centre de données et nuage
- Collaboration
- Sécurité
- Services de mobilité des fournisseurs de services

Renseignements supplémentaires à recueillir

- Le plan de test du client qui doit être automatisé

Responsabilités de Cisco

- Passer en revue le plan de test du client.
- Fournir des services qui peuvent comprendre, entre autres, les activités suivantes :
    - Automatisation des tests – fournir les cas de test automatisé.
    - Exécution des essais – exécuter le plan d'essai.

Livrables

- Soutien aux essais
- Plan de test (si spécifié dans le devis)

1.1.10. Soutien à la validation des tests sur site

La validation des tests sur site permet aux clients d'adopter de nouvelles technologies, de mettre en œuvre la validation de principe ou de valider la migration vers de nouvelles architectures chez le client.

Architectures prises en charge

- Réseau de base
- Centre de données et nuage
- Collaboration
- Sécurité
- Services de mobilité des fournisseurs de services

Solutions prises en charge

- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage
- Multicloud

Responsabilités de Cisco

- Configurer les outils de test et d'automatisation fournis par le client ainsi que les méthodes d'automatisation de test de la solution en matière d'infrastructure, de configuration, d'intégration et de points de regroupement pour le déploiement de la validation et des tests, y compris des considérations sur les protocoles, la sécurité et la gestion.
- Offrir un service de consultation et des conseils concernant les besoins d'automatisation des tests.
- Effectuer des tests en fonction du plan de test.
- Fournir au client un soutien sur site concernant les problèmes trouvés pendant la phase de test du client.

Livrables

- Rapport d'exécution des tests

Responsabilités du client

- Le client est responsable de fournir l'installation, l'armoire ou le bâti, le câblage du matériel les tests et les outils et licences permettant d'exécuter les tests.
- Fournir une assistance, une maintenance, des mises à jour et la configuration de toutes les solutions tierces.

1.1.11. Tests de l'état de préparation de l'architecture sur site

Le service de test de l'état de préparation de l'architecture sur site permet de vérifier que la conception ou le déploiement de la nouvelle architecture (Greenfield) ou de la technologie du Client est conforme à l'aide de tests effectués sur site ou à partir d'une installation Cisco.

Architectures prises en charge

- Réseau de base
- Centre de données et nuage
- Collaboration
- Sécurité
- Services de mobilité des fournisseurs de services

Renseignements supplémentaires à recueillir

- Les critères d'acceptation pour la validation de la conception du client.

Responsabilités de Cisco

- Créer le plan de test du client.
- Réaliser les tests indiqués dans le plan de test et rapporter les résultats au client.

Livrables

- Plan de mise à l'essai
- Rapport de test

Responsabilités du client

- Accès à l'environnement du site du client.
- Définir les critères d'acceptation

1.2. Ingénierie des fonctionnalités

L'ingénierie des fonctionnalités porte principalement sur l'analyse des avantages, des risques et des méthodes associés à l'adoption de capacités avancées ou améliorées d'application et d'infrastructure, tout en réduisant les perturbations et les risques propres aux activités du client en validant l'état de préparation de la solution.

1.2.1. Évaluation de fonctionnalité avancée

L'évaluation de fonctionnalité avancée aide le personnel d'ingénierie du client à accélérer l'adoption de fonctions technologiques avancées de Cisco qui renforcent le fonctionnement et la résilience de la solution du client. Les ingénieurs de Cisco évaluent et planifient les exigences et les dépendances de la solution afin de déployer des fonctionnalités avancées dans l'environnement du client, tout en atténuant les risques.

Technologies prises en charge

- Commutation de centre de données
- Tetration

Responsabilités de Cisco

- Évaluer la conception actuelle, planifier la mise en œuvre et offrir la formation en ce qui concerne une (1) fonctionnalité avancée que le client déploiera.

- Effectuer l'analyse du système dans un domaine sélectionné de l'infrastructure Cisco du client en ce qui concerne une fonctionnalité avancée précise.
- Analyser les configurations d'infrastructure et les aligner sur les politiques et procédures du client ainsi que sur les meilleures pratiques de Cisco.
- Examiner la conception de l'infrastructure actuelle afin de déterminer les éléments suivants :
    - Exigences d'état de préparation et de conception afin de déployer la fonctionnalité avancée ciblée.
    - Moyens d'exploiter la fonctionnalité avancée ciblée de l'infrastructure disponible dans des domaines comme la virtualisation, la résilience, la disponibilité et l'évolutivité.
- Collaborer avec le client afin d'élaborer une stratégie de migration permettant de mettre en œuvre la fonctionnalité ciblée de l'infrastructure dans l'environnement actuel du client.
- Mener une séance de transmission de connaissances technologiques sur la fonctionnalité avancée ciblée de l'infrastructure.

Livrable

- Rapport d'analyse de la fonctionnalité avancée

Restrictions

** Propre à la commutation de centre de données*

- Se limite à l'évaluation de la conception actuelle, à la planification, à la mise en œuvre et à la transmission de connaissances en ce qui concerne une (1) fonctionnalité avancée que le client déploiera.

1.2.1a. Évaluation de fonctionnalité avancée – Réseau sans fil

Technologies prises en charge

- Réseau sans fil

Responsabilités de Cisco

- Fournir des services de dépannage et d'analyse des systèmes qui peuvent inclure une analyse détaillée des performances de l'infrastructure du réseau sans fil du client à l'aide des outils et des techniques d'analyse des performances du réseau local sans fil (WLAN) de Cisco; l'analyse des performances et de la sécurité du WLAN peut inclure, entre autres, les activités suivantes :
    - Mesure de la couverture réelle des signaux du réseau sans fil.
    - Identification du niveau global des interférences et des sources précises pouvant avoir une répercussion négative sur les performances du réseau sans fil.
    - Analyse de l'utilisation du réseau, de la réception du signal RF (radiofréquences) du réseau et des mesures d'efficacité du réseau sans fil.
    - Dépannage du réseau local sans fil ou saisie et analyse de paquets pour des problèmes concernant le réseau local sans fil, au besoin.
    - Analyse de la conception et de la configuration de la sécurité du réseau sans fil.

Livrable

- Rapport d'analyse de la fonctionnalité avancée

Restrictions

** Propre au réseau sans fil*

- Une analyse de performance sur site de l'environnement WLAN du client est limitée à un maximum de dix (10) points d'accès (AP) ou de 25 000 pieds carrés.

1.2.2. Planification et mise en œuvre de l'assistance pour la migration

Le soutien de la planification et de la mise en œuvre de la migration aide le personnel technique du client à accélérer la mise à jour des solutions Cisco tout en atténuant les risques pour l'infrastructure et la stabilité du service.

Les ingénieurs de Cisco évaluent l'environnement de migration de la solution du client ou les exigences de mise à niveau et offrent du soutien pour évaluer les changements de conception de solution, les dépendances ainsi que les processus et la documentation concernés. Cisco peut également concevoir et vérifier des cas de test qualifiés dans un environnement de laboratoire, et offrira un soutien à distance sur appel durant les périodes de changement de client planifiées, comme l'indique le devis.

Technologies prises en charge

- Routage et commutation
- Gestion et orchestration de réseau
- Commutation de centre de données
- Orchestration et automatisation de centre de données
- Infrastructure centrée sur les applications
- Communications unifiées
- Service à la clientèle
- Collaboration vidéo
- Réunions et messagerie infonuagiques
- Solution de collaboration hébergée
- Réseau central de transmission par paquets
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
- Virtual Packet Core
  - Réseau central de transmission par paquets
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Gestion et orchestration de réseau
  - Politique de sécurité et accès

Exclusion

** Propre à l'orchestration et à l'automatisation de centre de données*

- Cisco CloudCenter (CCC) n'est pas pris en charge.

Renseignements supplémentaires à recueillir

- Carte des dépendances de l'application ou de la solution, propriétaires d'applications et administrateurs système.

Responsabilités de Cisco

- Découvrir et analyser l'environnement du client (inventaire, configurations et versions, schémas de trafic).

Remarque : Pour obtenir une description des outils et méthodes de collecte de données de Cisco qui sont utilisés, consultez le document Comment Cisco fournit des services, dont il est question dans les Conditions générales de BCS.

- Offrir un soutien et des conseils consultatifs au client pour faciliter la compréhension des changements nécessaires aux mesures correctives; Cisco n'apportera aucun changement ni aucune modification à l'environnement du client.
- Déterminer le potentiel, les risques ou les problèmes de l'intégration et fournir des recommandations concernant la migration de la solution et la réduction des risques.
- Si Cisco le juge nécessaire, effectuer des travaux de vérification limités ou qualifiés dans un laboratoire Cisco afin de valider les questions et les recommandations.
- Fournir des conseils et une assistance consultative au client avec le développement de changements de correction qualifiés et approuvés, et les valider dans un laboratoire Cisco.
- Aider le client à évaluer les processus de contrôle des modifications à la documentation et formuler des recommandations à ce sujet.

Responsabilités exclues

** Propre à l'infrastructure centrée sur les applications*

- Cisco n'est pas responsable du mappage des dépendances des applications.

Autres responsabilités

** Propre à la gestion et à l'orchestration du réseau, ainsi qu'à l'orchestration et à l'automatisation de centre de données*

- Examiner la liste requise des événements généraux, des modifications par phase et des activités afin de proposer de nouvelles solutions d'orchestration de services.
- Examiner la documentation des méthodes de procédure (MOP) concernant la connectivité et les tests avant et après la mise en service.
- Examiner les modèles principaux de configuration pour les types de sites ou de dispositifs représentatifs.
- Examiner les procédures de test de la solution prête à l'utilisation.

** Propre à l'infrastructure centrée sur les applications et à la commutation de centre de données*

- Examiner la documentation des méthodes de procédure (MOP) concernant la connectivité et les tests avant et après la mise en service.

** Propre aux communications unifiées, au service à la clientèle, à la collaboration vidéo, aux réunions et à la messagerie en nuage ainsi qu'à la solution de collaboration hébergée*

- Fournir des recommandations sur la migration ou la mise en œuvre de la solution, ce qui comprend notamment, sans toutefois s'y limiter, ce qui suit :
    - Procédures écrites, détaillées et adaptées aux exigences du client sur la migration ou la mise en œuvre du matériel et des logiciels.
    - Estimation de niveau d'effort nécessaire associé aux tâches de migration ou de mise en œuvre.
    - Recommandations concernant les procédures de gestion du changement.
    - Documentation sur les logiciels et le matériel concernant toutes les composantes qui dépendent de la solution.
    - Aide fournie au client dans la rédaction ou la révision de plans de test afin de confirmer l'approbation de la migration ou de la mise en œuvre.
    - Aide fournie au client dans la rédaction ou la révision de plans d'intervention de la mise en œuvre.

Livrable

- Rapport de recommandation sur la planification et la mise en œuvre de la migration

Restriction

** Propre à l'infrastructure centrée sur les applications*

- Cisco fournira un rapport sur la planification et la mise en œuvre des solutions de migration si Cisco le juge nécessaire.

** Spécifique à NFVI et MSX*

- La planification et la prise en charge de la migration doivent adhérer à la stratégie recommandée de mise à jour logicielle publiée par Cisco.

1.3. Gestion des connaissances

La gestion des connaissances aide l'ingénierie à améliorer la conception technique et les connaissances en développement et en déploiement grâce à des séances de transfert de connaissances pour l'ingénierie, des séances spécialisées et des ateliers de formation technique.

Remarque : Pour obtenir une description détaillée de la bibliothèque des apprentissages des Services opérationnels essentiels Cisco et des Services de gestion des connaissances de formation de Cisco : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Operations.pdf

1.3.1. Séance de transfert de connaissances pour l'ingénierie

Le service de séance de transfert de connaissances pour l'ingénierie permet le transfert de connaissances techniques sur des sujets mutuellement acceptables et relatifs à la conception et à la livraison d'architectures Cisco, de fonctionnalités de produits et de technologies déployés dans l'environnement du client. Les séances sont axées sur les meilleures pratiques en matière de conception, d'automatisation, d'analyse, de déploiement et d'adoption de solutions Cisco. Les séances de transferts de connaissances ne sont pas des formations officielles et ne remplacent pas les cours de Cisco.

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Gestion et orchestration de réseau
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Infrastructure centrée sur les applications
- Orchestration et automatisation de centre de données
- Tetration
- Communications unifiées
- Service à la clientèle
- Collaboration vidéo
- Réunions et messagerie infonuagiques
- Solution de collaboration hébergée
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services
- Calcul en périphérie de réseau de l'IDO et informatique géodistribuée
- Réseautique industrielle et collaboration

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Virtual Packet Core
  - Réseau central de transmission par paquets
- Infrastructure de virtualisation des fonctions de réseau Cisco (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
- Réseau étendu défini par logiciel
  - Routage et commutation
  - Gestion et orchestration de réseau
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Gestion et orchestration de réseau
  - Politique de sécurité et accès
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage

Responsabilités de Cisco

- Consulter le client pour déterminer les exigences et les sujets des séances de transfert de connaissances au moins quarante-cinq (45) jours à l'avance; les séances de transfert de connaissances sont :
  - Relatifs aux produits et technologies Cisco déployés dans le réseau de production du client.
  - Tenues à distance par un spécialiste en ingénierie des services Cisco en utilisant la conférence Web virtuelle pour une durée maximale de quatre (4) heures sans exercice et sans matériel de cours imprimé.
  - Tenues en fonction du nombre de séances spécifié dans le devis du client.

Autres responsabilités

** Propre aux communications unifiées, à la collaboration vidéo, au service à la clientèle et aux réunions et à la messagerie infonuagiques*

- Enregistrer toutes les séances de transfert de connaissances.
- Partager les enregistrements des séances avec le client aux fins de consultation future.

** Propre au réseau central de transmission par paquets*

- Pour le Réseau central virtuel de transmission par paquets, ce livrable prend en charge les composantes logicielles du système d'exploitation RedHat et de RedHat OpenStack.

Livrable

- Diapositives de la séance de transfert de connaissances, s'il y a lieu.

Responsabilités du client

- Coordonner et planifier les séances de transfert de connaissances avec le chef de projet de Cisco au début de chaque trimestre.
- Réunir des participants qui connaissent les produits Cisco associés à la solution du client.
- Réunir à tout moment un maximum de dix (10) participants, sauf si le client et Cisco en ont convenu autrement.

Restrictions

** Propre à la solution de collaboration hébergée*

- Pour le service HCS Standard : le nombre de séances de transfert de connaissances sera limité à deux (2).
- Pour le service HCS Premium : le nombre de séances de transfert de connaissances sera limité à quatre (4).

1.3.2. Séance de transfert de connaissances spécialisées

Le service de séance de transfert de connaissances spécialisées est un transfert de connaissances structuré comportant des exercices pratiques (s'il y a lieu) sur des sujets prédéfinis et relatifs à la conception et à la livraison d'architectures, de fonctionnalités et de technologies Cisco déployées dans l'environnement du client. Les séances sont axées sur les meilleures pratiques en matière de conception, de programmabilité, de configuration, d'automatisation et de validation de l'intégration des solutions Cisco. Les séances de transferts de connaissances spécialisées ne sont pas des formations officielles et ne remplacent pas les cours sur les services éducatifs de Cisco ou du portail Learning@Cisco.

1.3.2a. Séance de transfert de connaissances spécialisées

Technologies prises en charge

- Infrastructure centrée sur les applications

Renseignements supplémentaires à recueillir

- Aperçu des produits et des technologies Cisco déployés du client relativement aux sujets de la séance.

Responsabilités de Cisco

- Fournir des renseignements sur les principes fondamentaux, la configuration, les techniques de base de dépannage, les méthodologies de migration et les cas d'utilisation prédéfinis de programmabilité de l'infrastructure centrée sur les applications (ACI), ainsi que la configuration pour les éléments suivants :
  - Structure logique d'un locataire d'infrastructure ACI
  - Modèle de politique d'infrastructure ACI
  - Connectivité externe
  - Intégration de domaine de gestionnaire de machine virtuelle (VMM)
  - Services des couches 4 à 7
- Les séances sont animées par un spécialiste en ingénierie des services Cisco ou un partenaire de Cisco, comme déterminé par Cisco.
- Donner des conférences et un exercice pratique.
- Organiser une séance d'un maximum de cinq (5) jours à l'intention d'un maximum de (16) participants dans un bureau de Cisco.

Livrable

- Diapositives de la séance de transfert de connaissances spécialisées, s'il y a lieu.

1.3.2b. Séance de transfert de connaissances spécialisées pour Cisco CloudCenter

Technologies prises en charge

- Orchestration et automatisation de centre de données

Remarque : Les responsabilités du service de séance de transfert de connaissances spécialisées suivantes ne s'appliquent qu'à Cisco CloudCenter.

Responsabilités de Cisco

- Fournir une ou plusieurs des séances suivantes, comme spécifiées dans le devis :
- Présentation de Cisco CloudCenter :
- Séance d'un (1) jour, fournie à distance.
- Modélisation des services et des applications de Cisco CloudCenter :
- Séance de trois (3) jours, fournie à distance avec exercice pratique.
- Administration de Cisco CloudCenter :
- Séance de deux (2) jours, fournie à distance avec exercice pratique.
- Une séance ne peut avoir qu'un maximum de dix (10) participants.

Livrable

- Diapositives de la séance de transfert de connaissances spécialisées, s'il y a lieu.

Responsabilités du client

- Au moins quarante-cinq (45) jours avant la séance, fournir une liste des participants, leur rôle et leur fonction par rapport à l'objet de la séance.

- Coordonner et planifier les séances de transfert de connaissances spécialisées avec le chef de projet de Cisco.
- Le client est responsable de tous les coûts supplémentaires d'une séance de transfert de connaissances spécialisées fournie à distance sur le site du client.

1.3.2c. Séance de transfert de connaissances spécialisées sur les tests de validation de l'automatisation et de l'intégration

Le service de séance de transfert de connaissances spécialisées porte sur les tests de validation de l'automatisation et de l'intégration relatifs aux produits et technologies Cisco déployés dans l'environnement du client.

Architectures prises en charge

- Réseau de base
- Centre de données et nuage
- Collaboration
- Sécurité
- Services de mobilité des fournisseurs de services

Responsabilités de Cisco

- Présentation du cadre d'automatisation des tests ROBOT pour le test d'acceptation et le développement basé sur les tests d'acceptation.
- Indiquer les meilleures pratiques de Cisco en matière de développement d'automatisation et d'utilisation de la bibliothèque de tests automatisés Cisco.
- Cisco fournira dix (10) exemples de test pour les exercices pratiques du client.
- Fournir une (1) formation de cinq (5) jours pour un maximum de dix (10) participants chez client, pendant la phase de mise en œuvre du client.

Livrable

- Diapositives de la séance de transfert de connaissances spécialisées, s'il y a lieu.

Responsabilités du client

- Au moins quarante-cinq (45) jours avant la séance, fournir une liste des participants, leur rôle et leur fonction par rapport à l'objet de la séance.

2. CONFORMITÉ ET CORRECTION

Le service de conformité et de correction évalue les objectifs et les obligations du client relativement aux normes internes et externes de conformité et fournit une analyse des résultats, des observations utiles, des recommandations et de la correction accélérée.

Le client demeure responsable de l'ensemble de ses obligations réglementaires, juridiques et sectorielles de conformité relevées dans la présente description de service. Cisco fournira les évaluations, formulera des recommandations basées sur ses pratiques et se chargera des tâches de correction selon les instructions du client.

Navigation par section

La section **Conformité et correction** inclut les capacités et les livrables de services suivants, qui sont tous marqués d'un signet pour faciliter la navigation :

2.1. Conformité de la configuration

La conformité de la configuration fournit au client une méthode automatisée pour identifier les appareils non conformes dans le contexte des modèles de configuration de politique du client et des normes industrielles. Le soutien à la configuration et au changement de logiciel prend en compte les modifications de configuration planifiées du client, les mises à jour logicielles et fournit du soutien pour la fenêtre de modification programmée. La configuration, le logiciel et les livrables du service de conformité réglementaire et de correction aident le client à maintenir un rythme accéléré de mesures correctives. Le client reste responsable de déterminer les mesures de correction à entreprendre et si ces efforts répondent aux exigences du client.

2.1.1. Conformité à la procédure de configuration

Le service Conformité à la politique de configuration aide le client en fournissant des informations sur la conformité de la configuration à la politique définie par le client associée au regroupement des périphériques réseau.

Technologies prises en charge

- Routage et commutation
- Sécurité de réseau

Renseignements supplémentaires à recueillir

- Regroupement des périphériques réseau et des modèles de configuration connexes.
- Modèle de configuration standard pour un groupe précis de périphériques réseau.

Livrable

- Rapport sur la conformité à la politique de configuration

Restriction

** Propre à la sécurité du réseau*

- La conformité à la politique de configuration est prise en charge uniquement pour Cisco Adaptive Security Appliance (ASA).

2.1.2. Assistance à la configuration et aux modifications logicielles

Le service d'assistance à la configuration et aux modifications logicielles permet d'analyser et d'examiner les modifications proposées et le document de la méthode de procédure du client pour les opérations liées à la période de modification planifiée. L'assistance à distance est planifiée pour la mise en œuvre par le client de la configuration et des modifications logicielles.

2.1.2a. Assistance à la configuration et aux modifications logicielles

Renseignements supplémentaires à recueillir

- En relation avec les modifications proposées ou planifiées du client :
  - Stratégie de test liée aux modifications, plans de test et résultats de test.
  - Processus de contrôle et planification des modifications

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Gestion et orchestration de réseau
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Infrastructure centrée sur les applications
- Orchestration et automatisation de centre de données
- Tetration
- Communications unifiées
- Service à la clientèle
- Collaboration vidéo
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services
- Calcul en périphérie de réseau de l'IDO et informatique géodistribuée
- Réseautique industrielle et collaboration

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Réseau à optimisation autonome (SON)
  - Politique de mobilité et accès
- Infrastructure de virtualisation des fonctions de réseau Cisco (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
- Réseau étendu défini par logiciel
  - Routage et commutation
  - Gestion et orchestration de réseau
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Gestion et orchestration de réseau
  - Politique de sécurité et accès
- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données
  - Réseau central de transmission par paquets
- Secure Agile Exchange (SAE)
  - Routage et commutation

- Systèmes informatiques

- Systèmes informatiques
- Commutation de centres de données
- Orchestration et automatisation de centre de données
- Sécurité du nuage

Responsabilités de Cisco

- Collaborer avec le client pour évaluer les effets potentiels de la modification planifiée qui est proposée.
- Formuler des recommandations de modifications au plan de mise en œuvre, à la méthode de procédure et au plan de test du client en fonction des données recueillies auprès du client, de l'analyse des modifications proposées et des meilleures pratiques de Cisco.
- Produire un rapport de vérification et de recommandations relatives à la mise en œuvre de la modification pour consigner les résultats et les recommandations, si Cisco le juge nécessaire.
- Rendre disponible une ressource à distance pour les modifications planifiées essentielles.

Autres responsabilités

** Spécifique au document de MOP pour les technologies suivantes :*

Le routage et la commutation, le réseau optique, les réseaux sans fil, les systèmes informatiques, la gestion et l'orchestration du réseau, les réseaux de stockage, la commutation de centre de données, l'orchestration et l'automatisation de centre de données, le réseau central de transmission de paquets

- Formuler des recommandations de modifications au plan de mise en œuvre, à la méthode de procédure et au plan de test du client en fonction des données recueillies auprès du client, de l'analyse des modifications proposées et des meilleures pratiques de Cisco.
- Fournir au client un document de méthode de procédure pour la plateforme Cisco qui peut inclure les éléments suivants :
    - Procédures à suivre avant et après la mise en œuvre de modifications à la configuration ou au logiciel.
    - Procédures de restauration de la configuration planifiée ou des modifications logicielles.

** Propre aux technologies et à la solution suivantes :*

Gestion et orchestration de réseau, orchestration et automatisation du centre de données, orchestration du service de réseau

- Fournir un plan de mise à niveau documenté, si applicable aux produits de la trousse d'outils.
- Recommander un plan de tests pour les outils mis à niveau.

** Propre à Tetration Analytics™*

- Aider à la mise à niveau de grappe Tetration Analytics; limite d'une (1) mise à niveau par trimestre.
- Aider à la mise à niveau de capteurs; limite d'une (1) mise à niveau par trimestre.

Livrables

- Rapport de vérification et de recommandations relatives à la mise en œuvre de la modification (si Cisco le juge nécessaire)
- Document de MOP (spécifique aux technologies prises en charge).

Remarque : Un document de MOP prend en charge un seul changement de configuration ou de logiciel proposé ou planifié pour une technologie prise en charge et une plateforme Cisco.

Restrictions

- Cisco n'est pas responsable de l'élaboration ou de la mise à l'essai de toute méthode de procédure liée aux modifications planifiées ou proposées du client.
- Cisco n'est responsable du développement d'aucun document de MOP pour les plateformes non-Cisco et les technologies non mentionnées spécifiquement sous les responsabilités supplémentaires de Cisco spécifiques au document de MOP.

** Propre à l'orchestration et à l'automatisation de réseau et à la gestion et l'orchestration de centre de données*

- La personne-ressource ne répond pas à plus de trois (3) questions d'assistance, relevées par le client au cours de la période de modification (généralement au cours d'une fin de semaine), concernant des installations majeures de logiciel, une installation importante sur le site ou des modifications de configuration majeures.

** Propre au document MOP pour les technologies suivantes : routage et commutation, réseau optique, réseaux sans fil, systèmes informatiques, gestion et orchestration du réseau, réseaux de stockage, commutation de centre de données, orchestration et automatisation de centre de données, réseau central de transmission de paquets.*

- La modification de l'analyse d'impact n'est pas effectuée à l'aide d'outils de simulation.
- Les documents de MOP ne sont pas fournis pour les produits logiciels Cisco qui nécessitent des scénarios.
- La vérification des recommandations de Cisco contenues dans le document de MOP est limitée à la vérification des modifications de configuration, des procédures de mise à jour logicielle et de restauration pour un système d'exploitation et une plateforme Cisco similaires dans le cadre des travaux pratiques de Cisco, si Cisco le juge opportun.
- Le document de MOP n'est pas prévu pour la migration d'une plateforme Cisco vers une autre plateforme Cisco.

2.1.2b. Assistance à la configuration et aux modifications logicielles (propres à HCS)

Le service d'assistance à la configuration et aux modifications logicielles n'est propre qu'à la solution de collaboration hébergée de Cisco (HCS) Standard ou Premium, comme indiqué dans le devis.

Technologies prises en charge

- Solution de collaboration hébergée

Pour HCS Standard :

Responsabilités de Cisco

- Collaborer avec le client pour évaluer les effets potentiels de la modification planifiée qui est proposée.
- Formuler des recommandations de modifications au plan de mise en œuvre, à la méthode de procédure et au plan de test du client en fonction des données recueillies auprès du client, de l'analyse des modifications proposées et des meilleures pratiques de Cisco.
- Rendre disponible une ressource à distance pour les modifications planifiées essentielles.
- Fournir de l'assistance à distance au client afin de résoudre des questions prioritaires ou critiques à propos des modifications au cours d'une activité majeure sur le réseau de production.

Livrable

- Soutien consultatif et conseils seulement

Pour HCS Premium :

Responsabilités de Cisco

- Collaborer avec le client pour évaluer les effets potentiels de la modification planifiée qui est proposée.
- Fournir au client un document de méthode de procédure qui peut inclure les éléments suivants :
    - Procédures de restauration de la configuration planifiée ou des modifications logicielles.
    - Procédures à suivre avant et après la mise en œuvre des modifications.
    - Stratégie d'essai liée aux modifications, plans d'essai et résultats des essais.
    - Analyse de l'incidence des modifications.
    - Processus et calendrier de contrôle des modifications.
- Effectuer les modifications détaillées dans le document de méthode de procédure avec le client.
- Rendre disponible une ressource à distance pour les modifications planifiées essentielles.
- Fournir de l'assistance à distance au client afin de résoudre des questions prioritaires ou critiques à propos des modifications au cours d'une activité majeure sur le réseau de production.

Livrable

- Document de méthode de procédure

2.1.3. Conformité et correction de la configuration

Le service de conformité et de correction de la configuration fournit un moyen automatisé pour aider le client à relever les périphériques réseau qui ne respectent pas la conformité de la configuration et le guide à travers le processus de correction ou de mise à niveau de la norme requise en fonction des recommandations décrites dans le document sur les meilleures pratiques en matière de configuration des Services opérationnels essentiels Cisco ou dans les livrables de la politique sur la conformité de la configuration.

Le service Conformité et correction de la configuration fournit au client une assistance pour la correction ou la mise à jour pour les périphériques réseau ciblés à l'aide de scénarios basés sur les procédures, des conditions préalables et des critères de réussite décrits dans le livrable sur la configuration et le changement de logiciel.

Dépendances

Les rapports livrables suivants sont préalables à la création de l'automatisation des modifications de configuration :

- **Observations sur la plateforme :**
    - Rapport sur les meilleures pratiques en matière de configuration
- **2.1 – Conformité de la configuration**
    - Conformité à la procédure de configuration
    - Assistance à la configuration et aux modifications logicielles
    - Rapport de vérification et de recommandations relatives à la mise en œuvre de la modification de Cisco

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Sécurité de réseau

Remarque : Les Conditions générales des Services opérationnels essentiels Cisco – Responsabilités générales de Cisco – Restrictions indiquent les plateformes et les systèmes d'exploitation de Cisco et non-Cisco pris en charge.

Renseignements supplémentaires à recueillir

- Rapport sur les meilleures pratiques en matière de configuration de Cisco.
- Rapport sur la conformité à la politique de configuration de Cisco
- Rapport complet de vérification et de recommandations relatives à la mise en œuvre de la modification de Cisco du client, un préalable à ce livrable.

Responsabilités de Cisco

- Créer des règles et des conditions d'automatisation pour une (1) norme de conformité de la configuration en fonction des procédures, des conditions préalables et des critères de réussite décrits dans le livrable Configuration et changement de logiciel, Examen de la mise en œuvre de la modification Cisco et Rapport de recommandation.
- Corriger les plateformes et les systèmes d'exploitation en fonction des meilleures pratiques décrites dans le rapport sur les meilleures pratiques de Cisco, ou dans le rapport de conformité de la politique de configuration, comme approuvé et mis de l'avant par le client.
- Fournir des rapports de journal de tâche réussie.

Livrable

- Un (1) scénario de conformité et de correction de la configuration par plateforme ou système d'exploitation indiqué dans le devis.

Responsabilités du client

- Compléter et fournir un rapport d'un ou plusieurs des éléments suivants requis pour ce service :
    - Rapport sur les meilleures pratiques en matière de configuration
    - Rapport sur la conformité à la politique de configuration

- Compléter et fournir le rapport suivant à partir du livrable de Cisco sur le changement de configuration et de logiciel, ce qui constitue une condition préalable à ce service :
    - Rapport de vérification et de recommandations relatives à la mise en œuvre de la modification

2.1.4. Conformité et correction du logiciel

Le service de conformité et de correction des logiciels fournit un moyen automatisé d'aider le Client à recenser les périphériques réseau qui ne respectent pas la conformité du logiciel et guide le client au fil du processus de correction ou de mise à niveau de la version du système d'exploitation requise en fonction des versions recommandées actuelles et déployées décrites dans le rapport des normes de version et d'analyse de logiciels et le rapport du suivi de la conformité du logiciel.

Le service de conformité et de correction des logiciels fournit au client un soutien pour les mises à niveau logicielles à l'aide de scénarios pour un seul périphérique ou pour un grand groupe de périphériques en utilisant le MOP et les documents de prévérification et de post-vérification qui contiennent les conditions préalables et les critères de réussite en post-vérification pour tous les types de périphériques.

Dépendances

Les rapports livrables suivants sont des préalables à la création de l'automatisation des mises à niveau :

- **Gestion du cycle de vie des logiciels :**
    - Rapport des normes de version et d'analyse de logiciels
    - Rapport de conformité pour le suivi des logiciels
- **Assistance à la configuration et aux modifications des logiciels :**
    - Rapport de vérification et de recommandations relatives à la mise en œuvre de la modification

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Sécurité de réseau

Remarque : Les Conditions générales des Services opérationnels essentiels Cisco – Responsabilités générales de Cisco – Restrictions indiquent les plateformes et les systèmes d'exploitation de Cisco et non-Cisco pris en charge.

Renseignements supplémentaires à recueillir

- Rapport complet des normes de version et d'analyse des logiciels de Cisco du client
- Rapport complet du suivi de la conformité des logiciels Cisco du client.
- Rapport complet de vérification et de recommandations relatives à la mise en œuvre de la modification de Cisco du client.

Responsabilités de Cisco

- Créer des règles et des conditions de mise à niveau automatisée pour une (1) plateforme ou un (1) système d'exploitation.
- Mettre à niveau le système d'exploitation vers la version recommandée et sous licence comme indiqué dans le rapport des normes de version et d'analyse des logiciels de Cisco.
- Fournir des rapports de journal de tâche réussie.

Livrable

- Un (1) scénario de mise à niveau d'image logicielle par plateforme ou système d'exploitation indiqué dans le devis.

Responsabilités du client

- Compléter et fournir un rapport des éléments suivants requis pour ce service :
    - Rapport des normes de version et d'analyse de logiciels
    - Rapport de conformité pour le suivi des logiciels
    - Rapport de vérification et de recommandations relatives à la mise en œuvre de la modification

2.1.5. Conformité réglementaire et correction

Le service Conformité réglementaire et les mesures correctives offre un moyen automatisé pour aider les clients à identifier les périphériques réseau dont la configuration n'est pas conforme aux normes industrielles (répertoriées ci-dessous).

Les configurations réseau sont vérifiées par rapport aux règles de diverses catégories comme le routage, la commutation, la communication sans fil et la sécurité de ces normes réglementaires, et des résultats agrégés et par périphérique sont fournis.

Le client sera en mesure d'examiner les résultats pour planifier les fenêtres de maintenance en fonction de sa hiérarchisation des exceptions et des périphériques réseau. Les vues du tableau de bord fournissent des renseignements détaillés au personnel d'ingénierie de réseau, aux équipes des opérations, aux vérificateurs et aux dirigeants afin qu'ils puissent consulter les résultats et les tendances des résumés de vérification chaque jour, chaque semaine, chaque mois ou selon un intervalle personnalisé.

Le client demeure responsable de l'ensemble de ses obligations de conformité associées aux normes sectorielles et réglementaires définies dans la présente description de service. Cisco fournira les évaluations, formulera des recommandations basées sur ses pratiques et se chargera des tâches de correction selon les instructions du client.

Dépendances

Le service Conformité réglementaire et correction est fourni avec le logiciel de configuration réseau et de gestion du changement (NCCM) et ne dépend pas des rapports des autres livrables de la présente offre.

Utilisation

Les clients achètent une évaluation des pratiques en matière de conformité pour une ou plusieurs des normes comme HIPAA, ISO 27002, PCI-DSS, guides STIG de la DoD DISA et autres obligations réglementaires relatives aux normes, s'il y a lieu.

Les livrables du service de conformité réglementaire et de correction visent les clients suivants :

- Les clients qui souhaitent utiliser les résultats des livrables des évaluations des pratiques en matière de conformité de Cisco et les mettre en œuvre dans le réseau en fonction du champ d'application décrit ci-dessous.
- Les clients qui souhaitent utiliser les résultats d'une vérification par un ou plusieurs des organismes de réglementation des normes sectorielles indiquées ci-dessus et les mettre en œuvre dans le réseau en fonction du champ d'application décrit ci-dessous.

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Sécurité de réseau

Remarque : Les conditions générales des Services opérationnels essentiels Cisco – Responsabilités générales de Cisco – Restrictions indiquent les plateformes et les systèmes d'exploitation pris en charge.

Responsabilités de Cisco

- Vérifier la conformité des périphériques à l'aide du logiciel Cisco NCCM pour un ou plusieurs des éléments suivants, comme indiqué dans le devis :
  - North American Electric Reliability Corporation (NERC)
  - Directives de sécurité de la NSA
  - Politique de sécurité des routeurs du SANS
  - Liste de vérification du département de la Sécurité intérieure (DHS)
  - Meilleures pratiques en matière de sécurité (loi SAFE)
  - Conformité aux dispositions de la loi HIPAA
  - Conformité à la loi SOX (COBIT)
  - Normes de configuration des guides STIG de la DoD DISA
  - Liste de vérification IOS® de la DISA
  - Tests de performance IOS et CIS PIX
  - Conformité aux dispositions de la loi FISMA
  - Conformité à la publication spéciale 800-171 du NIST
  - Norme ISO/CEI 27002
  - Norme PCI-DSS (Payment Card Industry Data Security Standard, norme sur la sécurité des données pour les industries de carte de paiement)
- Effectuer l'évaluation de la conformité des périphériques afin de déterminer quelles configurations de périphérique du client ne sont pas conformes.
- Créer des règles et des conditions de modification automatisée de configuration d'une (1) plateforme ou d'un (1) système d'exploitation.
- Corriger la plateforme ou le système d'exploitation en fonction de la politique en matière de meilleures pratiques recommandées décrite dans l'évaluation de conformité des périphériques.
- Fournir des rapports de journal de tâche.

Autres responsabilités

** Propre à l'évaluation des normes de configuration des guides STIG de la DoD DISA*

- Effectuer une vérification de la conformité des périphériques par rapport aux politiques réglementaires des guides STIG.
- Les vérifications continues des périphériques de conformité sont effectuées selon un calendrier convenu avec le client (p. ex., hebdomadaire, mensuel ou trimestriel).
- Effectuer une évaluation de la vulnérabilité.

Livrables

- Une (1) vérification de périphérique de conformité basée sur une ou plusieurs des vérifications ci-dessus, tel que spécifié dans le devis.

** Propre à l'évaluation des normes de configuration des guides STIG de la DoD DISA*

- En plus des livrables ci-dessus, les livrables suivants sont fournis :
    - Rapports de vérification continue de la conformité
    - Résumé du rapport d'évaluation relative au guide STIG de la DoD DISA

2.2. Évaluation des pratiques de conformité

L'évaluation des pratiques de conformité évalue les exigences en matière de sécurité ou de conformité réglementaire du Client, cerne d'éventuelles lacunes et fournit des recommandations en matière de correction, en fonction des pratiques de Cisco, que peut pendre en compte le Client. Le client reste responsable des décisions liées à la mise en œuvre des pratiques de conformité.

Architecture prise en charge

- Sécurité

Le service d'évaluation de la conformité est composé d'un ou de plusieurs des types d'évaluation de conformité pris en charge par les technologies ci-dessus.

- Évaluation de l'alignement de la structure sur la norme ISO 27001
- Évaluation de l'alignement de la structure sur la norme ISO 27002
- Évaluation de la conformité aux normes HIPAA et HITECH
- Évaluation de la conformité à la norme PCI-DSS
- Conformité en matière de sécurité – Autre exigence normative ou réglementaire
- Évaluation de la conformité au guide technique de mise en œuvre de la sécurité (Security Technical Implementation Guide ou STIG)

2.2.1. Évaluation de l'alignement de la structure sur la norme ISO 27001

Cisco va effectuer une évaluation des pratiques de conformité de l'alignement actuel du client sur les exigences de contrôle de la norme ISO 27001 et formuler des recommandations de Cisco et une feuille de route en préparation à la certification ISO 27001.

Renseignements supplémentaires à recueillir

Documents obligatoires

- Champ d'application du système de gestion de la sécurité de l'information
- Politique et objectifs en matière de sécurité de l'information
- Méthodologie d'évaluation et de traitement des risques
- Déclaration d'applicabilité
- Plan de traitement des risques
- Rapport d'évaluation des risques
- Définition des rôles et des responsabilités de sécurité
- Inventaire des ressources
- Utilisation acceptable des ressources
- Politique de contrôle d'accès
- Procédures opérationnelles de gestion des TI
- Principes d'ingénierie de système sécurisé
- Politique de sécurité du fournisseur
- Procédure de gestion des incidents
- Planification de la continuité des activités
- Obligations juridiques, réglementaires et contractuelles

Dossiers obligatoires

- Dossiers relatifs à la formation, aux compétences, à l'expérience et aux qualifications
- Résultats de la surveillance et des mesures
- Programme d'évaluation interne
- Résultats des vérifications internes
- Journaux des activités des utilisateurs, des exceptions et des événements de sécurité
- Résultats de l'analyse de la gestion
- Résultats des mesures correctives

Documents non obligatoires (mais généralement fournis)

- Procédure de contrôle des documents
- Contrôles de la gestion des dossiers
- Procédure de vérification interne
- Procédure pour les mesures correctives
- Politique sur l'utilisation de votre propre appareil
- Politique relative à l'appareil cellulaire et au télétravail
- Politique de classification des renseignements
- Politique relative au mot de passe
- Politique d'élimination et de destruction
- Procédures à suivre pour travailler dans les zones sécurisées
- Politique de bureau propre et d'écran vide
- Politique de gestion du changement
- Politique de sauvegarde
- Politique de transfert des renseignements
- Analyse de l'impact sur l'entreprise
- Plan d'exécution et de tests
- Plan de maintenance et d'examen
- Stratégie de continuité des activités

Responsabilités de Cisco

- Fournir une présentation de la norme ISO 27001 et du processus général pour obtenir la certification.
- Déterminer le champ d'application de la certification ISO :
  - Définir les processus, les systèmes connexes et les équipes d'assistance dans le cadre du champ d'application.
  - Déterminer si les contrôles de l'annexe A peuvent être considérés comme étant hors du champ d'application.
- Effectuer une évaluation approfondie de l'alignement actuel sur les exigences de la norme ISO 27001.

Livrables

- Rapport d'évaluation relatif à la norme ISO 27001
- Résumé du rapport d'évaluation relatif à la norme ISO 27001

2.2.2. Évaluation de l'alignement de la structure sur la norme ISO 27002

Cisco procédera à une évaluation des pratiques de conformité visant à appuyer l'évaluation de l'efficacité de la sélection et la conception des contrôles et à déterminer la conformité du Client dans chaque domaine de la norme ISO 27002:2013. Cisco se chargera également de mener des examens approfondis de l'efficacité d'un échantillon de contrôles et d'examens de site physique des opérations de centre de données et des TI afin de contribuer à l'évaluation de l'efficacité opérationnelle des contrôles.

Responsabilités de Cisco

- Procéder à un examen de l'efficacité du contrôle aux fins suivantes :
  - Valider la documentation sur la sélection et la conception des contrôles.
  - Évaluer l'efficacité opérationnelle des contrôles.

  - Relever les lacunes posant un risque lié à la sécurité de l'information.
  - Relever les risques systémiques potentiels des activités des TI.
- Effectuer un examen approfondi de l'efficacité par rapport aux échantillons de contrôles avec l'une des deux méthodes suivantes :
  - Examiner la preuve de l'exécution et de l'achèvement des contrôles.
  - Observation de l'opération du contrôle.
- Effectuer une inspection physique de site afin d'observer la mise en œuvre des contrôles dans les centres de données, les activités des TI et les zones de gestion du siège social du client.

Livrables

- Rapport d'évaluation relatif à la norme ISO 27002
- Résumé du rapport d'évaluation relatif à la norme ISO 27002

2.2.3. Évaluation de la conformité aux normes HIPAA et HITECH

Cisco effectuera une évaluation des pratiques de conformité afin de contribuer à déterminer la conformité aux obligations des règles de sécurité de la loi HIPAA (Health Insurance Portability and Accountability Act) et aux exigences pertinentes supplémentaires de la loi HITECH (Health Information Technology for Economic and Clinical Health Act). L'évaluation du niveau de conformité aux règles de sécurité des lois HIPAA et HITECH permet d'évaluer l'efficacité de la sélection et de la conception des contrôles. Cisco concentrera ses efforts sur les résultats et la cartographie des efforts de correction que recommande Cisco afin de fournir un rapport qui inclut une feuille de route sur le degré de conformité aux règles de sécurité des lois HIPAA et HITECH.

Renseignements supplémentaires à recueillir

- Processus de vérification internes.
- Processus opérationnels et transactions qui utilisent des données protégées sur la santé (electronic Protected Health Information, ePHI).
- Documentation sur la sélection et la conception des contrôles conformes aux lois HIPAA et HITECH.

Responsabilités de Cisco

- Déterminer le champ d'application de l'évaluation en fonction des éléments suivants :
  - L'emplacement physique des sites et les contrôles qui s'appliquent à chaque emplacement.
  - Les applications et infrastructures qui stockent et traitent les données protégées sur la santé.
- Effectuer un examen de l'efficacité des contrôles et une inspection du site physique pour :
  - Valider la documentation sur la conception des contrôles.
  - Examiner l'efficacité opérationnelle des contrôles.
  - Étudier les processus de contrôle non documentés ou découvrir de la documentation supplémentaire pour l'évaluation.
- Effectuer un examen de l'efficacité opérationnelle de la mise en œuvre des contrôles par rapport à l'échantillon de contrôles des exigences des lois HIPAA et HITECH à l'aide d'une (1) des trois (3) méthodes suivantes :
  - Examiner la preuve de l'exécution et de l'achèvement des contrôles.
  - Observation de l'opération du contrôle.

- Évaluation du contrôle dans le cadre d'un rapport de conformité (ROC) de l'industrie des cartes de paiement (PCI) ou toute autre évaluation pertinente.

- Effectuer une inspection physique de site afin d'observer la mise en œuvre des contrôles dans les centres de données, les activités des TI et les zones de gestion du siège social du client.

Livrables

- Rapport d'évaluation du degré de conformité aux règles de sécurité des lois HIPAA et HITECH, y compris la feuille de route sur le degré de conformité aux règles de sécurité des lois HIPAA et HITECH.
- Résumé du rapport d'évaluation du degré de conformité aux règles de sécurité des lois HIPAA et HITECH

2.2.4. Évaluation de la conformité à la norme PCI-DSS

Cisco effectuera une évaluation par blocs de temps des pratiques de conformité par rapport à la norme de sécurité actuelle de la PCI (par exemple, DSS 3.1) pour fournir des renseignements sur le degré actuel de conformité à cette norme d'un environnement des données du titulaire de la carte (CDE).

Renseignements supplémentaires à recueillir

- La documentation sur la sélection et la conception des contrôles conformes à la norme PCI-DSS.

Responsabilités de Cisco

- Élaborer un plan tactique et stratégique pour effectuer les corrections nécessaires en fonction des résultats de l'évaluation, y compris les recommandations.

Livrable

- Rapport d'évaluation du niveau de conformité à la norme PCI-DSS

Restriction

- Le champ d'application de l'évaluation du niveau de conformité à la norme PCI-DSS couvre un échantillon de périphériques convenus par le client et Cisco et n'est pas une analyse de rapport de conformité (ROC) complète de tous les périphériques.

2.2.5. Conformité en matière de sécurité – Autre exigence normative ou réglementaire

Cisco effectuera une évaluation des lacunes de conformité par rapport à une norme de sécurité ou à une exigence réglementaire précise convenue entre les parties.

Responsabilités de Cisco

- Déterminer le champ d'application de l'évaluation en fonction de la norme de sécurité ou de l'exigence réglementaire et des éléments suivants :
  - Environnement technologique et processus opérationnels du client.
  - L'emplacement physique des sites et les contrôles qui s'appliquent à chaque emplacement.
- Effectuer un examen de l'efficacité du contrôle d'une seule norme de sécurité ou exigence réglementaire aux fins suivantes :
  - Examiner les politiques et les normes.
  - Valider la sélection et de la conception des contrôles.

- Valider le processus de contrôle.
- Attester de la documentation.
- Effectuer une inspection physique de site afin d'observer la mise en œuvre des contrôles dans les centres de données, les activités des TI et les zones de gestion du siège social du client, si Cisco juge cette inspection applicable à l'exigence.

Livrable

- Rapport d'évaluation du degré de conformité

2.2.6. Évaluation de la conformité au guide technique de mise en œuvre de la sécurité (Security Technical Implementation Guide ou STIG)

Le service d'évaluation de la conformité au guide STIG fournit une évaluation du degré de conscience de la situation et de la conformité à l'aide de politiques basées sur des exigences de conformité gouvernementales (p. ex., les guides STIG relatifs à l'infrastructure réseau de l'Agence des systèmes d'information du Département de la Défense [DoD DISA]) pour aider à évaluer les menaces à l'infrastructure du client. Cisco effectuera une évaluation des pratiques de conformité à l'aide d'un moteur de conformité qui répertorie les configurations du client, les examine par rapport aux politiques décrites ci-dessus et produit un rapport détaillé des vulnérabilités et un résumé destiné aux cadres.

Renseignements supplémentaires à recueillir

Documents obligatoires

- Objectifs, politiques et considérations relatives à la sécurité
- Rapport d'évaluation et plan d'atténuation des risques
- Déclaration d'applicabilité
- Définitions des rôles et des responsabilités en matière de sécurité
- Procédure de gestion des incidents
- Inventaire des ressources
- Utilisation acceptable des ressources
- Politique de contrôle d'accès
- Procédures opérationnelles de gestion des TI
- Principes d'ingénierie de système sécurisé
- Planification de la continuité des activités
- Obligations juridiques, réglementaires et contractuelles

Dossiers obligatoires

- Dossiers relatifs à la formation, aux compétences, à l'expérience et aux qualifications
- Résultats de la surveillance et des mesures
- Programme d'évaluation interne
- Résultats des vérifications internes
- Journaux des activités des utilisateurs, des exceptions et des événements de sécurité
- Résultats de l'analyse de la gestion
- Résultats des mesures correctives
- Nombre et types de périphériques

Documents non obligatoires (mais généralement fournis)

- Procédure de contrôle des documents
- Contrôles de la gestion des dossiers
- Procédure de vérification interne
- Procédure pour les mesures correctives
- Politique sur l'utilisation de votre propre appareil
- Politique relative à l'appareil cellulaire et au télétravail
- Procédures à suivre pour travailler dans les zones sécurisées
- Politique de bureau propre et d'écran vide
- Politique de gestion du changement
- Politique de sauvegarde
- Politique de transfert des renseignements
- Analyse de l'impact sur l'entreprise

- Politique de classification des renseignements
- Politique relative au mot de passe
- Politique d'élimination et de destruction
- Plan d'exécution et de tests
- Plan de maintenance et d'examen
- Stratégie de continuité des activités

Responsabilités de Cisco

- Réaliser une vérification de la conformité par rapport aux politiques réglementaires des guides STIG. Les vérifications continues de la conformité sont effectuées selon un calendrier convenu avec le client (p. ex., hebdomadaire, mensuel ou trimestriel).
- Effectuer une évaluation approfondie de la vulnérabilité.
- Formuler des recommandations afin de corriger les vulnérabilités révélées par l'évaluation.

Livrables

- Rapports de vérification continue de la conformité
- Rapport d'évaluation relative au guide STIG de la DoD DISA
- Résumé du rapport d'évaluation relative au guide STIG de la DoD DISA

3. SOUTIEN AUX APPLICATIONS

Le soutien à l'application aide le client lors de l'analyse des avantages, des risques et des méthodes d'intégration et de prise en charge des capacités avancées ou mises à niveau de l'application ou de l'infrastructure, tout en tentant de réduire au minimum les interruptions et les risques de l'entreprise du client.

Navigation par section

La section **Soutien à l'application** décrit les capacités de services suivantes, qui sont toutes associées à un signet pour faciliter la navigation :

3.1. Soutien aux applications personnalisées

Le soutien aux applications personnalisées vise à aider le client dans la planification, la configuration et le soutien des applications personnalisées et des processus automatisés.

3.1.1. Assistance à l'administration du site et des systèmes

Le service d'assistance à l'administration des sites et des systèmes est conçu pour les administrateurs de site du client qui sont responsables de la configuration, de l'administration et de la maintenance de la plateforme de gestion du nuage, de l'automatisation des processus informatiques et de la mise en œuvre des systèmes d'orchestration.

Technologies prises en charge

- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données
- Tetration

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
- Réseau étendu défini par logiciel
  - Gestion et orchestration de réseau
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage

Exclusion

** Propre à l'orchestration et à l'automatisation de centre de données*

- Cisco CloudCenter (CCC) n'est pas pris en charge.

Responsabilités de Cisco

- Fournir un soutien à distance au client pour les activités courantes suivantes :
  - Surveiller les environnements :
    - Effectuer des contrôles quotidiens de l'intégrité du système (fichiers journaux, archives et temps de réponse).
    - Fournir de manière proactive une notification en cas d'erreur, de dégradation, d'activité inhabituelle ou suspecte aux personnes appropriées.
    - Surveiller l'exploitation des serveurs, de la mémoire, des processeurs, du stockage local et des paramètres de débit.
    - Créer des rapports hebdomadaires sur le niveau de service.
  - Entretenir les environnements :
    - Appliquer des correctifs et des mises à niveau.
    - Élaborer et tenir à jour des plans et des processus d'entretien quotidiens, hebdomadaires ou mensuels.
    - Redémarrer le système au besoin.
    - Collaborer avec l'équipe chargée des opérations matérielles pour la maintenance du serveur physique, comme prévu.

- Maintenir le système et les autorisations de sécurité.
- Inspecter les paramètres et les versions des logiciels.
- Vérifier la cohérence entre les environnements.
- Gérer les problèmes liés au déploiement (migration des objets de la phase de développement à la production, en passant par le test).

- Élaborer et documenter les processus de gestion des opérations et du système (modèles de déploiement, gestion des utilisateurs, contrôles d'accès).

** Propre à Tetration*

- Créez jusqu'à deux (2) tableaux de bord de Tetration Analytics comportant au maximum de quatre (4) sections chacune, à l'aide des données de Tetration Analytics.

Livrable

- Document sur le processus de gestion des opérations et des systèmes

3.1.2. Soutien au protocole NDP (Neighbor Discovery Protocol) de SON

Le service de soutien au protocole NDP offre une configuration proactive des nouveaux sites cellulaires voisins du client. Cisco aide le client à analyser, à mettre au point et à soutenir les configurations de modules de SON.

Solutions prises en charge

- Réseau à optimisation autonome
  - Politique de mobilité et accès

Renseignements supplémentaires à recueillir

- Exigences de configuration du SON

Responsabilités de Cisco

- Analyser les rapports de trafic du SON (veille stratégique) du client.
- Aider le client à configurer les paramètres relatifs aux politiques du module de relation de voisinage automatique (ANR) du SON.
- Aider le client à configurer le module d'optimisation automatique des paramètres (APO).
- Assurer le suivi des activités RAN liées aux éléments du nouveau réseau.

Livrable

- Soutien consultatif et conseils seulement

3.2. Soutien adapté pour l'intégration

Le soutien adapté pour l'intégration vise à aider les clients à accélérer l'intégration des applications personnalisées et des flux de travail à l'aide de scénarios et d'interfaces de programmation d'applications (API).

3.2.1. Assistance à l'intégration de la solution de gestion

L'assistance à l'intégration de la solution de gestion vise à aider le personnel technique du client à accélérer l'adoption et l'intégration des plateformes de gestion et d'orchestration des logiciels ou des plateformes tierces avec les applications relatives au flux de travail du client.

Les ingénieurs de Cisco évaluent les exigences actuelles et futures de l'automatisation des applications du flux de travail, valident les modifications apportées à l'intégration des fonctions et répondent aux questions et aux problèmes des clients concernant les interfaces API standard publiées.

Technologies prises en charge

- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données
- Réseau central de transmission par paquets

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
- Réseau étendu défini par logiciel
  - Gestion et orchestration de réseau
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage

Remarque : Les Conditions générales des Services opérationnels essentiels Cisco – responsabilités générales de Cisco – Restrictions indiquent les plateformes de Cisco prises en charge. L'assistance offerte aux plateformes tierces sera précisée dans le devis.

Renseignements supplémentaires à recueillir

- Principes de la gestion et de l'orchestration de la clientèle, objectifs, exigences et priorités en matière d'automatisation des applications du flux de travail, intégration des applications, y compris les API standard planifiées et mises en œuvre de Cisco.

Responsabilités de Cisco

- Diagnostiquer les problèmes du client en utilisant ou en mettant en place des API standard de gestion et d'orchestration de Cisco.

- Conseiller le personnel du client sur l'utilisation et les fonctionnalités des API standard de Cisco dans le cadre de l'automatisation générale du flux de travail de gestion et d'orchestration.
- Évaluer et confirmer si les mesures d'intégration des applications exploitent efficacement les API standard de Cisco.

Livrable

- Soutien consultatif et conseils seulement

Restrictions

** Propre à la gestion et à l'orchestration du réseau, à l'orchestration et à l'automatisation du centre de données, à l'orchestration des services réseau, au réseau WAN défini par le logiciel et à l'analyse et à l'assurance des fournisseurs de services.*

- Les éléments suivants sont exclus :
    - Conception, développement, déploiement et soutien des applications relatives au flux de travail du client.
    - Mise à l'essai des applications relatives au flux de travail du client.
    - Assistance/soutien pour les API de logiciels ne provenant pas de Cisco.

3.2.2. Prise en charge de l'API pour l'intégration des plateformes client

La prise en charge des API pour l'intégration des plateformes du client permet aux clients d'utiliser des API standard publiées.

3.2.2a. Assistance à l'intégration des API dans l'infrastructure ACI

L'assistance à l'intégration des interfaces de programmation d'applications (API) dans l'infrastructure centrée sur les applications (ACI) comprend un soutien pour l'intégration dans VCenter des API standard publiées et pour les trousses d'appareils des couches 4 à 7 (L4-7) autorisées et prises en charge par Cisco.

Technologies prises en charge

- Infrastructure centrée sur les applications

Renseignements supplémentaires à recueillir

- Conception et configuration de l'intégration des API

Responsabilités de Cisco

- Apporter un soutien au client pour les étapes de déploiement et d'intégration basées sur l'intégration des API standards publiées au serveur VCenter de VMware à l'aide des trousses de périphériques des couches L4 à L7 approuvés par Cisco.

Livrable

- Soutien consultatif et conseils seulement

Responsabilités du client

- Franchir l'étape d'assistance permanente à la conception, laquelle est un préalable à la présente étape.
- Collaborer avec les fournisseurs de l'écosystème sur la configuration et la conception de services particuliers.

4. PROTECTION DE LA SÉCURITÉ

La sécurité comprend des stratégies de sécurité proactives, une planification, des conseils relatifs à la mise en œuvre, de la formation, des simulations et une aide pour la résolution de problèmes du client.

Navigation par section

La section **Protection de la sécurité** décrit les capacités et les livrables de services suivants, qui sont tous associés à un signet pour faciliter la navigation :

4.1. Évaluations de la sécurité

Les évaluations de sécurité permettent de trouver des vulnérabilités techniques au sein des systèmes informatiques et de l'infrastructure de soutien.

4.1.1. Évaluation de la sécurité physique

L'évaluation de la sécurité physique consiste à mettre à l'épreuve une installation du client, en tentant d'exploiter les faiblesses des contrôles de sécurité physiques afin d'évaluer l'efficacité de telles défenses et d'améliorer la formation liée à la sensibilisation à la sécurité. Le principal objectif du test est d'obtenir l'accès au matériel important et aux zones sécurisées. L'évaluation de la sécurité physique sera effectuée sur place dans une installation à sécurité minimale du Client, qui ne possède pas de mesures de sécurité poussées (sas, identificateurs biométriques ou gardes armés).

Architecture prise en charge

- Sécurité

Responsabilités de Cisco

- **Collecte d'observations et planification :**
  - Utiliser les techniques de renseignement de sources ouvertes (OSINT) pour obtenir des renseignements sur la cible physique et sur le personnel concerné.
  - Effectuer une analyse du site relative au mécanisme et aux procédures de contrôle d'accès de l'emplacement.
  - Définir les défenses de sécurité face au contournement.
  - Définir les utilisateurs et les administrateurs du système.
  - Élaborer un plan pour atteindre les objectifs de la mission.
  - Concevoir une trousse d'attaques physiques sur mesure à utiliser lors des phases opérationnelles et post-opérationnelles.

- **Phase opérationnelle :**
    - Essayer de pénétrer le périmètre de chaque emplacement physique à l'aide de plusieurs techniques, par exemple :
        - Créer un faux identifiant et un faux objectif provisoire pour justifier la présence sur le site.
        - Essayer d'obtenir un accès physique aux installations ou aux zones données (p. ex., passage en double).
        - Créer de faux badges ou de fausses cartes professionnelles, s'il y a lieu.
        - Essayer d'obtenir un accès physique en s'attaquant aux systèmes de contrôle physiques (p. ex., crochetage de serrures, clonage de RFID).
        - Élaborer une infrastructure d'attaque pour surveiller les connexions à partir de périphériques infectés par un cheval de Troie.
        - Intégrer les périphériques USB, les CD et les petits périphériques informatiques infectés par un cheval de Troie dans des zones à trafic utilisateur élevé.
        - Surveiller les connexions des périphériques USB, des CD et des petits périphériques pendant la période des tests.
        - Se faire passer pour un client, un employé ou un fournisseur du client.
        - Essayer de convaincre le personnel de réaliser des tâches au nom du testeur (p. ex., ouvrir des portes et des serrures).
        - Tenter d'obtenir l'accès à du matériel ou à des périphériques définis par le client.
        - Essayer de contourner les contrôles de sécurité physiques et d'en exploiter les faiblesses.
        - Essayer d'éviter les systèmes physiques de détection et de surveillance tels que les caméras et les alarmes de porte.
- **Phase post-opérationnelle :**
    - Essayer d'accéder aux autres emplacements à accès restreint.
    - Essayer d'obtenir un accès au matériel sensible.
    - Intégrer des périphériques non autorisés, comme des implants, des enregistreurs de frappe et des périphériques USB, si cela est pertinent.
    - Essayer d'extraire du matériel ou de l'équipement, avec l'autorisation du client.
    - Documenter l'accès et le chemin d'accès aux objectifs définis.

Livrable

- Rapport d'évaluation de la sécurité physique

Responsabilités du client

- Fournir les adresses et les indications nécessaires pour rejoindre et déterminer l'emplacement physique à tester.
- Repérer les zones sécurisées.
- Fournir une assistance pour obtenir l'accès à tous les emplacements physiques nécessaires pour commencer à réaliser les tests sur les emplacements physiques visés par le service.
- Fournir les détails sur tous les risques associés à chaque emplacement physique (p. ex., gardes armés, risques sanitaires).

- Fournir une lettre d'autorisation écrite à remettre au personnel de sécurité :
    - Indiquer les noms des consultants dans la lettre.
    - Indiquer l'équipement ou le matériel pouvant être retiré du site dans la lettre.
- Intervenir rapidement si les autorités locales arrêtent le personnel de Cisco.
- Informer toutes les parties concernées des activités de test et les coordonner avec celles-ci (p. ex., la gestion des bâtiments et les agents de sécurité).
- Obtenir une autorisation de réalisation des tests auprès des propriétaires de l'immeuble si l'emplacement physique est partagé ou loué.

4.1.2. Test d'intrusion dans les réseaux

Le test d'intrusion dans le réseau consiste à mener des tests externes ou internes sur un seul réseau du client afin d'aider le client à repérer les vulnérabilités exploitables et celles présentant un risque élevé; il s'agit d'une occasion d'évaluer l'efficacité des investissements en matière de sécurité dans le cadre d'une attaque simulée.

Architecture prise en charge

- Sécurité

Responsabilités de Cisco

- Effectuer une collecte d'observations nécessaires, de la manière suivante :
    - Effectuer une analyse de périmètre des protocoles, services, systèmes d'exploitation (SE) et autres technologies.
    - Repérer les défenses de sécurité à contourner.
    - Repérer les utilisateurs et administrateurs du système.
    - Déterminer les composants du système.
    - Créer un aperçu de la surface d'attaque.
- Modéliser les menaces, détecter les vulnérabilités et analyser la surface d'attaque comme suit :
    - Effectuer des analyses automatisées et manuelles.
    - Utiliser, s'il y a lieu, des techniques de test à données aléatoires ou de rétro-ingénierie.
    - Rechercher les menaces applicables aux logiciels et aux actifs de systèmes.
    - Hiérarchiser les attaques en fonction des objectifs de l'analyse.
- Effectuer les activités opérationnelles suivantes, s'il y a lieu :
    - Tirer parti des faiblesses de conception et d'architecture à l'aide du reniflage du réseau et en lançant des attaques de l'intercepteur.
    - Compromettre les composants du système en exploitant les failles du logiciel au moyen de débordements de mémoire tampon, d'exécutions de codes à distance, de scénarios intersites, d'injections SQL et d'autres attaques par injection de commande.
    - Tester les failles opérationnelles liées aux pratiques de gestion des correctifs, de gestion de la configuration et de déploiement des systèmes.
    - Exploiter les faiblesses des utilisateurs en tentant de deviner ou de craquer leurs mots de passe.

- Contourner les contrôles de sécurité en échappant aux pare-feu, aux systèmes de détection des intrusions, aux antivirus, aux contrôles d'accès, aux protections cryptographiques et aux systèmes de prévention de perte de données.

- Effectuer les activités post-opérationnelles suivantes, s'il y a lieu :
  - Exploiter les vulnérabilités découvertes pour établir une menace persistante.
  - Exploiter les vulnérabilités découvertes pour obtenir des droits d'accès supplémentaires.
  - Rechercher des identifiants et des données sensibles, comme des renseignements nominatifs et des numéros de carte de crédit.
  - Essayer de rediriger les attaques vers des cibles supplémentaires.
  - Essayer d'extraire des données, avec l'autorisation du client.
- Mener les activités suivantes liées au rapport :
  - Éliminer les faux positifs, si possible.
  - Analyser l'incidence possible sur l'entreprise.
  - Étudier et élaborer des stratégies pour remédier aux problèmes.

Livrable

- Document sur les tests d'intrusion dans le réseau

Restrictions :

- Les tests compteront jusqu'à 256 adresses IP externes ou 400 adresses IP internes.

4.1.3. Évaluation de la sécurité des solutions sans fil

L'évaluation de la sécurité des solutions sans fil consiste à évaluer le déploiement de l'environnement sans fil du client afin de repérer les vulnérabilités dans un immeuble du client. Les vulnérabilités de sécurité peuvent être démontrées en exploitant les vulnérabilités découvertes après l'approbation du client.

Architecture prise en charge

- Sécurité

Renseignements supplémentaires à recueillir

- Nombre de points d'accès sans fil 802.11 a/b/g/n/ac, identifiant SSID, état de configuration de la diffusion avec identifiant SSID, type d'authentification et chiffrement.

Responsabilités de Cisco

- Évaluer les risques associés aux périphériques sans fil en essayant de déterminer les éléments suivants :
  - Clients servant de passerelle entre les réseaux sans fil et le réseau de l'entreprise, si les identifiants sont fournis.
  - Clients sans fil qui se connectent généralement aux réseaux sans fil non sécurisés.
  - Configuration d'authentification faible (p. ex., validation de certificat désactivée).
- Évaluer le déploiement sans fil général, notamment :
  - Administration.
  - Segmentation et connectivité du réseau.

- Configuration des points d'accès.
- Authentification et chiffrement.

- Détecter et valider les vulnérabilités.
- Classer les vulnérabilités en fonction des risques associés.

Livrable

- Rapport d'évaluation sur la sécurité des solutions sans fil

Responsabilités du client

- Fournir à Cisco une autorisation d'exploitation des vulnérabilités détectées, s'il y a lieu.

Restrictions

- Cisco organisera une évaluation de la sécurité des solutions sans fil au sein d'un emplacement unique.
- Cisco énumérera au maximum cinq (5) instances de réseau sans fil identifiées par SSID, et évaluera le déploiement de l'environnement sans fil pour déterminer les vulnérabilités.

4.1.4. Évaluation des intrusions dans l'application

L'évaluation des intrusions dans l'application consiste à mener des tests visant à repérer les vulnérabilités de la couche d'application dans une application de taille moyenne conçue par le Client. Cependant, les tests peuvent aussi révéler des vulnérabilités dans les dépendances immédiates de l'application. L'évaluation commencera par la définition de la surface d'attaque directe au sein de l'application. La surface d'attaque sera analysée pour la détection de vulnérabilités grâce à des techniques de test manuelles et automatisées. Un code source peut être utilisé pour augmenter l'efficacité des tests. Une fois les renseignements d'authentification fournis, Cisco réalisera des tests en mode authentifié.

Architecture prise en charge

- Sécurité

Renseignements supplémentaires à recueillir

- Documents sur l'application, diagrammes et données d'accès (p. ex., noms de domaine, URL et adresses IP)
- Détails pour utiliser pleinement l'application (p. ex., code d'exemple, documentation sur les API)
- Comptes d'utilisateurs pour chaque rôle à tester
- Code source des applications à évaluer
- Processus de débogage et versions de production du logiciel ciblé

Responsabilités de Cisco

- Effectuer un examen afin de repérer les problèmes de sécurité pertinents, notamment les classes de vulnérabilités suivantes :
  - Vulnérabilités d'injection (injection de commande, injection SQL)
  - Vulnérabilités aux attaques par scénario intersites et par injection basée sur des scénarios
  - Falsification de requêtes intersites (CSRF)

- Vulnérabilités liées à la gestion de la mémoire
- Vulnérabilités liées à la validation d'entrée et de sortie
- Vulnérabilités liées à la gestion des séances
- Vulnérabilités liées au contrôle d'accès
- Vulnérabilités liées à la canonisation du chemin
- Utilisation inefficace ou insuffisante du chiffrement
- Déni de service lié à l'application
- Propagation d'observations sensibles
- Stockage sécurisé de secrets
- Vulnérabilités liées au traitement général des données
- Vulnérabilités liées à la référence d'objets
- Conception ou logique pouvant provoquer des failles de sécurité
- Failles relatives à la configuration
- Failles de sécurité des communications
- Problèmes applicables non mentionnés explicitement ci-dessus, mais couverts par les normes pertinentes (Top 10 de l'OWASP, Top 25 des erreurs de programmation les plus dangereuses selon l'institut SANS)

- Effectuer une analyse à l'aide d'un éventail de techniques permettant de repérer les vulnérabilités en matière de sécurité le plus rapidement possible, en adoptant les stratégies de base suivantes lors de l'évaluation :
  - Recensement de la surface d'attaque : tentative de détection des fonctionnalités de l'application grâce à la traversée automatisée de l'arborescence du site et à la permutation des variantes courantes sur les conventions de nomenclature populaires.
  - Injection automatisée d'erreurs : envoi automatisé de données malveillantes afin de repérer les vulnérabilités liées à la sécurité sur le chemin de requête.
  - Injection manuelle d'erreurs : envoi manuel de données malveillantes afin de repérer les vulnérabilités liées à la sécurité sur le chemin de requête.
  - Test de vulnérabilité connue : repérage des vulnérabilités sur la plateforme d'hébergement (serveur Web, conteneur de servlet) à l'aide, principalement, de techniques d'analyse automatisée.
  - Compréhension du code : analyse manuelle du code source des chemins de code relatifs à la sécurité (si le code est disponible).
  - Repérage des risques de vulnérabilités : analyse automatisée permettant de repérer des schémas de vulnérabilité connus, suivie d'une analyse manuelle pour valider toute vulnérabilité suspectée (si le code est disponible).
  - Corrélation de données : recherche de vulnérabilités, élimination des faux positifs et étude de la portée des résultats.

Livrable

- Rapport d'évaluation des intrusions dans l'application

Responsabilités du client

- Fournir à Cisco un accès de niveau administrateur aux systèmes évalués ou mettre à sa disposition des membres du personnel capables d'effectuer les tâches administratives en cas de problèmes techniques.
- Déterminer les modules cibles spécifiques et leur capacité (s'il y a lieu).
- Fournir un accès aux environnements de test et de production (s'il y a lieu).
- Prendre en charge tous les frais associés à l'augmentation de l'utilisation des ressources sur les systèmes tiers (comme les fournisseurs infonuagiques) nécessaires à la réalisation des tests.
- Informer toutes les tierces parties concernées et obtenir leur autorisation pour la réalisation des tests.

Restrictions

- Cisco effectuera une évaluation des intrusions dans l'application pour une seule application, sur une plateforme donnée.
- L'application doit comprendre au maximum 250 000 lignes de code.
- L'évaluation portera sur un maximum de soixante (60) entrées d'application (p. ex., les appels RPC, les demandes http POST ou les messages de services Web traités par l'application) avec une moyenne de quinze (15) paramètres par entrée, pour un maximum de six (6) rôles d'utilisateur.

4.1.5. Équipes Red Team et Purple Team

Les équipes Cisco Red Team et Purple Team effectuent des tests pour accéder au réseau et aux systèmes du client. La simulation de tentatives d'intrusion peut effectuer de la surveillance du niveau de sécurité et de la gestion de la sécurité et permet de déterminer si les défenses du client peuvent empêcher ou détecter les menaces modernes.

Définitions et relation entre les équipes :

L'équipe Cisco Red Team fait office d'entité externe pour tester l'efficacité des contrôles de sécurité en place. Pour ce faire, elle surveille le comportement des agresseurs de la vie réelle dans la manière dont ils ciblent et attaquent une entité.

L'équipe Purple Team est une combinaison de membres des équipes Red Team et Blue Team travaillant en collaboration pour exécuter une attaque réelle ou sélectionner des phases d'attaque, et analyser chaque action pour aider le client à déterminer comment identifier et contrer les attaques.

Le client (Blue Team) est l'entité de sécurité interne qui défend une entreprise contre les attaques malveillantes en tentant d'identifier et de bloquer une attaque au moment où elle se produit. Généralement distincte des équipes de sécurité « normales ».

Architecture prise en charge

- Sécurité

Renseignements supplémentaires à recueillir

- Les segments de réseau et la liste des appareils inclus et exclus de l'évaluation des fonctionnalités de sécurité déployées.
- Les méthodes et les cibles des attaques exclues.
- Exigences réglementaires concernant la protection des données de l'application.

- Objectif(s) de la recherche de données après l'activité.
- Scénarios pour la filtration de données et la modification du code.

Responsabilités de Cisco

- Collecte d'informations et détection des vulnérabilités lorsque Cisco peut :
    - Tirer parti de la l'information sur les menaces pour identifier les scénarios d'attaque les plus pertinents.
    - Utiliser des techniques de collecte d'information à code libre (Open Source Information Gathering Techniques ou OSINT) pour identifier les personnes, les processus et les technologies les plus exposés.
- Exécuter des activités d'exploitation sur les environnements vulnérables où Cisco peut :
    - Compromettre les composants du système en exploitant les failles de mise en œuvre dans le logiciel au moyen de débordements de mémoire tampon, d'exécutions de codes à distance, d'attaques sur les éléments dynamiques, d'injections de code et d'autres attaques.
    - Exploiter les failles opérationnelles liées aux pratiques de gestion des correctifs, de gestion de la configuration et de déploiement des systèmes.
    - Exploiter les faiblesses des utilisateurs par ingénierie sociale, en tentant de deviner ou de craquer leurs mots de passe.
    - Exploiter les faiblesses de conception et d'architecture dans les réseaux sans fil et dans la sécurité physique.
    - Contourner les contrôles de sécurité comme les pare-feu, les systèmes de détection des intrusions, les antivirus, les contrôles d'accès, les protections cryptographiques et les systèmes de prévention de perte de données.
- Effectuer des activités post-exploitation au sein des environnements exploités lorsque Cisco peut :
    - Utiliser les emprises présentes au sein de la structure afin d'établir une menace persistante.
    - Utiliser les emprises présentes en place au sein de la structure afin d'obtenir des droits d'accès supplémentaires.
    - Se déplacer latéralement au sein des systèmes compromis.
    - Effectuer une recherche de données sensibles et de renseignements d'identification (p. ex. : renseignements nominatifs, numéros de carte de crédit).
    - Exécuter des attaques par filtration de données et modification de code, tel qu'approuvé par le client.
- Les opérations de sécurité des équipes Purple Team et Red Team peuvent comprendre les éléments suivants :
    - Évaluation des fonctionnalités de sécurité déployées sur les appareils et les segments de réseau inclus dans l'évaluation.
    - Simulations ciblées et répétées des tactiques des agresseurs.
    - Ajuster les tactiques des attaques en fonction des commentaires du client.

Livrable

- Les livrables du service peuvent inclure le ou les éléments suivants :
- Rapport de l'équipe Red Team de Cisco
- Rapport de l'équipe Purple Team de Cisco

Responsabilités du client

- Fournir une assistance Cisco en cas d'échec d'une étape requise, qui peut consister à fournir un accès privilégié ou à désactiver temporairement un contrôle de sécurité.
- Donner l'approbation à Cisco une (1) semaine à l'avance pour l'exécution des attaques par filtration de données et modification de code et des simulations répétées des tactiques des agresseurs.
- Donner l'autorisation écrite pour effectuer les tests, selon les besoins de Cisco.
- Pour l'équipe Cisco Purple Team, fournir un accès Cisco au représentant du client pour une (1) semaine maximum pour chaque appareil et chaque segment de réseau soumis aux tests.
- Pour l'équipe Cisco Purple Team, configurer et fournir l'accès local et distant de Cisco à un environnement de test adéquat.
- Pour l'équipe Cisco Purple Team, donner à Cisco des informations de contrôle de sécurité de prévention et de détection.
- Les équipes Red Team du client et de Cisco devront partager réciproquement les informations relatives aux attaques et à la défense.

Restrictions

- La simulation pourra se limiter aux vecteurs d'attaque à distance, comme les attaques contre les ordinateurs et les utilisateurs du client exposés sur Internet.
- La simulation pourra se limiter aux vecteurs d'attaque sur site, comme les attaques contre les ordinateurs et les utilisateurs du client sur les sites du client.
- Pour l'équipe Purple Team, la portée de la simulation se limite à un seul périphérique en cours de test dans un segment de réseau unique, sauf si Cisco et le client en conviennent autrement.

4.1.6. Évaluation du piratage psychologique

L'évaluation du piratage psychologique vise à définir les membres du personnel du Client qui ont besoin d'une formation supplémentaire de sensibilisation à la sécurité ou à obtenir les mesures de réussite généralisées anonymes de la formation de sensibilisation à la sécurité (c.-à-d., des résultats anonymes). Les tests peuvent utiliser des mécanismes de communication, à l'écrit ou à l'oral, tels que les courriels, la messagerie instantanée, le téléphone et la télécopie pour convaincre les personnes de compromettre la sécurité dans un environnement contrôlé. L'évaluation du piratage psychologique sera effectuée à distance, dans un ou plusieurs emplacements.

Architecture prise en charge

- Sécurité

Renseignements supplémentaires à recueillir

- Piratage psychologique (à l'écrit) :
  - Fournir une liste des noms et des adresses de courriel cibles.
  - Indiquer les personnes ciblées ayant signalé une tentative de piratage psychologique, au besoin.
- Piratage psychologique (à l'oral) :
  - Fournir une liste des noms et des numéros de téléphone cibles.
  - Indiquer les personnes ciblées ayant signalé une tentative de piratage psychologique, au besoin.

Responsabilités de Cisco

- Effectuer un test de piratage psychologique (à l'écrit) :
    - Fournir au client les adresses IP source des serveurs de messagerie utilisés pour l'exécution de la campagne.
    - Recenser les utilisateurs très exposés à l'aide des méthodes OSINT.
    - Élaborer jusqu'à quatre (4) campagnes d'hameçonnage visant à convaincre les utilisateurs cibles de ce qui suit :
    - Révéler les identifiants d'accès.
    - Exécuter des tâches pour le compte du testeur.
    - Visiter les sites Web contrôlés par l'attaquant.
    - Ouvrir des fichiers fournis par l'attaquant.
    - Élaborer et personnaliser l'infrastructure d'attaques, qui peut inclure les éléments suivants :
        - Créer des sites Web personnalisés.
        - Concevoir ou déployer des pseudo-logiciels malveillants, des commandes de système principal et des serveurs de contrôle.
    - Réaliser une campagne d'hameçonnage qui peut inclure des communications contenant les éléments suivants :
        - Messages visant à convaincre les utilisateurs d'ouvrir des fichiers, de cliquer sur des liens ou d'effectuer des actions pour le compte du testeur.
        - Liens vers des sites Web contrôlés par l'attaquant.
        - Pièces jointes et fichiers contenant des pseudo-logiciels malveillants.
        - Liens vers des sites Web imitant des sites Web d'entreprise pour collecter des identifiants.
        - Liens vers des formulaires Web qui demandent à l'utilisateur de soumettre des données sensibles.
        - Identités falsifiées de personnes de confiance.
    - Surveiller et enregistrer les réponses des utilisateurs.
- Effectuer un test de piratage psychologique (à l'oral) :
    - Déterminer les numéros de téléphone ou périphériques vocaux à haut risque en utilisant les méthodes OSINT.
    - Essayer d'usurper l'identité des personnes de confiance du client, notamment les clients, les employés et les fournisseurs du client.
    - Essayer de demander à un maximum de vingt (20) personnes de fournir des renseignements sensibles, comme :
        - Identifiants d'accès.
        - Renseignements confidentiels.
        - Données financières.
        - Renseignements nominatifs des clients ou d'autres employés.
        - Renseignements sensibles définis par le client.
    - Essayer de convaincre le personnel d'effectuer des actions au nom de l'appelant.
    - Documenter les tentatives de piratage psychologique réussies.

Livrable

- Rapport sur le piratage psychologique

Responsabilités du client

- Pour le test de piratage psychologique (à l'écrit) :
    - Approuver les scénarios de piratage psychologique, s'il y a lieu.
    - Configurer les serveurs, les passerelles et les filtres de courriel pour accepter les courriels provenant du serveur de courriel de test de Cisco, quel que soit le taux de transmission ou le contenu.
    - S'assurer que les personnes qui ne devraient pas recevoir de courriels d'hameçonnage sont clairement identifiées.
- Piratage psychologique (à l'oral) :
    - Approuver les scénarios de piratage psychologique, s'il y a lieu.
    - S'assurer que les personnes qui ne devraient pas recevoir d'appels téléphoniques sont clairement identifiées.

Restrictions

- Pour le test de piratage psychologique (à l'écrit) :
    - Un maximum de cinq cents (500) adresses de courriel seront fournies par le client ou trente (30) adresses découvertes par Cisco, mais dans ce cas, les adresses de courriel autorisées par le client pourront être vulnérables aux attaques par hameçonnage.
    - Jusqu'à quatre (4) campagnes d'hameçonnage seront menées.
- Cisco effectuera des tentatives de communication avec quinze (15) employés au maximum pour le piratage psychologique à l'oral.

4.2. Développement d'un programme de sécurité

L'élaboration d'un programme de sécurité vise à aider les clients à mettre en place un ensemble de stratégies, de connaissances, de capacités et de processus organisationnels, ainsi que des mesures pour atteindre leurs objectifs en matière d'affaires et de sécurité.

4.2.1. Assistance en matière de planification et de stratégie de sécurité

L'assistance pour la planification et la stratégie de sécurité consiste à offrir des conseils stratégiques et tactiques par l'entremise d'une série de réunions ou d'ateliers sur un sujet de sécurité choisi par le client, puis d'organiser un atelier d'une durée maximale de trois (3) jours afin de travailler sur les phases d'incubation et d'élaboration de la stratégie. Les sujets peuvent notamment porter sur ce qui suit : les technologies et l'architecture de sécurité, le nuage, les solutions Cisco TrustSec® et Identity, le programme de sécurité, la conformité et les risques associés à la gouvernance de la sécurité, la sécurité des systèmes d'automatisation et de contrôle, la sécurité des systèmes mobiles, le télétravail, la gestion, le centre de données et la sécurité des solutions de collaboration.

Architecture prise en charge

- Sécurité

Responsabilités de Cisco

- Informer le client sur le service et les options du service.
- Organiser un atelier de planification préalable pour le client.

- Organiser un atelier de planification pour le client.
- Résumer le contenu et les recommandations issues de l'atelier.
- Faire un retour sur l'atelier.
- Organiser une réunion après l'atelier.
- Résumer le contenu de la réunion suivant l'atelier et les recommandations finales en découlant.

Livrable

- Compte-rendu des travaux

Restrictions

- L'atelier peut s'étendre sur trois (3) jours.
- Chaque unité d'assistance pour la planification et la stratégie de sécurité comprend :
    - Jusqu'à trois (3) domaines de difficultés majeures.
    - Jusqu'à trois (3) réunions ou une (1) journée entière de réunion préalable à l'atelier.
    - Jusqu'à trois (3) jours pour un atelier sur site, hors site ou par Cisco TelePresence.
    - Jusqu'à trois (3) réunions de suivi ou une (1) journée entière de réunion postérieure à l'atelier.
    - Jusqu'à quatre (4) participants Cisco simultanés.

4.2.2. Évaluation des risques liés à la sécurité de l'information et élaboration d'un programme

Architecture prise en charge

- Sécurité

Renseignements supplémentaires à recueillir

- La structure organisationnelle des risques de TI, le nombre de membres de l'équipe et le champ de vision
- Les processus opérationnels critiques, les processus de TI et les dépendances connues à l'application
- Les contrôles des risques associés à l'entité et le processus de gouvernance
- Les attentes des parties prenantes, les facteurs de succès pour contrer le risque informatique, la perception des gens, les problèmes ou les préoccupations à l'égard du processus actuel
- Les facteurs culturels qui influencent le risque informatique

4.2.2a. Évaluation des risques liés à la sécurité de l'information

L'évaluation des risques liés à la sécurité de l'information vise à déterminer, évaluer et recommander des mesures pour atténuer les risques stratégiques et opérationnels liés à la sécurité qui peuvent toucher les activités du Client. L'évaluation des risques permettra d'examiner les stratégies commerciales et informatiques et de déterminer les risques liés à la sécurité de l'information pour l'entreprise, qui menacent la mise en œuvre des stratégies définies. L'évaluation visera à déterminer les risques critiques par un mélange d'analyses stratégiques, d'examen de la documentation, d'entrevues, d'observations du contrôle et d'évaluation simplifiée des risques. L'évaluation des risques permet d'évaluer les contrôles actuels des risques et de chercher à déterminer les risques résiduels. En fonction des priorités de l'entreprise et de la

connaissance de la tolérance aux risques que Cisco a acquise au fil d'entrevues avec les cadres, Cisco établira un profil personnalisé des risques liés à la sécurité de l'information et une feuille de route des mesures d'atténuation.

Responsabilités de Cisco

- Adapter l'évaluation des risques en fonction des renseignements recueillis sur le contexte commercial.
- Confirmer et accepter le niveau de tolérance aux risques de sécurité de l'information et les critères pertinents d'évaluation des risques commerciaux.
- Effectuer une analyse stratégique des tendances clés, en tenant compte des éléments suivants :
    - Stratégies commerciales, attentes du client et tendances du secteur identifiées par les parties prenantes.
    - Stratégies technologiques pertinentes.
    - Tendances en matière de réglementation et de législation.
    - Tendances pertinentes en matière de sécurité de l'information et de menaces externes.
- Étudier le processus actuel de gestion des risques liés aux TI :
    - Étudier la structure organisationnelle des risques liés aux TI, le nombre de membres de l'équipe et le champ de vision.
    - Étudier la documentation des processus.
    - Étudier l'utilisation de l'automatisation.
    - Étudier l'efficacité de l'exécution par la ou les personnes responsables.
    - Déterminer quels sont les apports et les perceptions des contributeurs en menant des entrevues.
    - Examiner la production de rapports sur l'évaluation des risques informatiques.
    - Étudier les résultats exploitables et les réponses organisationnelles face aux conclusions de l'évaluation des risques informatiques.
- Examiner et tenter de recenser les risques liés à la sécurité de l'information au sein des processus d'affaires et de l'architecture informatique du client, de l'infrastructure et des processus opérationnels qui soutiennent les actifs informatiques essentiels, ce qui comprend l'identification des risques potentiels et l'examen des contrôles actuels au moyen des activités suivantes :
    - Animer des ateliers en groupe sur l'évaluation des risques avec un sous-groupe de parties prenantes pour mettre en évidence et évaluer les risques en fonction de connaissances institutionnelles informelles.
    - Examiner les sources de risques disponibles, telles que les rapports de gestion des problèmes et des incidents et les mesures de rendement du service informatique.
    - Effectuer une analyse des domaines pertinents, ce qui peut comprendre :
        - Gouvernance et supervision de la sécurité de l'information.
        - Politiques, normes et procédures de sécurité de l'information.
        - Classification et gestion des renseignements.
        - Processus de conformité.
        - Évaluation et la gestion des risques.
        - Architecture de sécurité d'entreprise.

- Gestion du rendement et des mesures de la sécurité.
- Sensibilisation et formation.
- Gestion de la vulnérabilité, des correctifs, du changement et des ressources.
- Surveillance de la sécurité et les instruments.
- Gestion des incidents.
- Acquisition, développement et maintenance des logiciels.
- Reprise après sinistre et résilience du système.
- Gestion des risques liés à des tierces parties.
- Gestion de l'identité et de l'accès.
- Sécurité des ressources humaines.
- Sécurité environnementale et physique.
- Sécurité du réseau.
- Sécurité du système.
- Chiffrement et la sécurité des données.
- Sécurité des supports et des appareils mobiles.
- Protection contre les codes malveillants.

- Évaluer les risques :
  - Regrouper et analyser les risques potentiels en fonction du type d'incidence.
  - Évaluer les risques ciblés, les classer selon la probabilité de concrétisation de chaque risque et selon l'incidence potentielle s'ils se produisent.
  - Examiner les risques évalués par rapport aux critères personnalisés de notation des risques afin de les classer par ordre de priorité et de déterminer ceux qui nécessitent une intervention.
- Établir une feuille de route de mesures d'atténuation comprenant :
  - Recommandations liées à la gestion des risques.
  - Améliorations recommandées qui sont associées aux initiatives dans un échéancier.

Livrable

- Rapport de l'évaluation des risques liés à la sécurité de l'information

4.2.2b. Développement d'un programme de gestion des risques liés à la sécurité de l'information

À partir de l'évaluation des risques informatiques du client, Cisco fournira des recommandations sur les possibilités d'amélioration ou d'enrichissement du programme.

Responsabilités de Cisco

- Examiner l'approche, les activités et les commentaires actuels relatifs à l'évaluation des risques informatiques du client et les comparer aux attentes.

- Examiner les processus actuels liés aux risques informatiques :
    - Étudier l'efficacité de l'exécution par la ou les personnes responsables.
    - Déterminer quels sont les apports et les perceptions des contributeurs en menant des entrevues.
    - Étudier les résultats exploitables et les réponses organisationnelles face aux conclusions de l'évaluation des risques informatiques.

Livrable

- Rapport sur l'élaboration d'un programme de gestion des risques liés à la sécurité de l'information

4.2.3. Évaluation des risques liés à des tierces parties et élaboration d'un programme

Le service d'évaluation des risques liés à des tierces parties et d'élaboration d'un programme permet de déterminer les failles de sécurité potentielles dans le programme de gestion des risques liés aux fournisseurs et aux tierces parties du client, lesquelles peuvent exposer le client à certains risques. L'évaluation portera sur les processus du programme, afin d'évaluer l'efficacité des processus d'identification, de gestion, de gouvernance et de surveillance des risques liés aux tierces parties.

L'évaluation couvre tout le cycle de vie des engagements avec des tierces parties, dont la définition des exigences, la diligence et le contrôle raisonnables, la négociation, la transition et la transformation, ainsi que les opérations permanentes et la résiliation. Les problèmes déterminés seront hiérarchisés en fonction des risques, puis signalés. Des recommandations utiles seront fournies avec un plan d'amélioration proposé.

Architecture prise en charge

- Sécurité

4.2.3a. Évaluation des risques liés à des tierces parties

Responsabilités de Cisco

- Évaluer le programme de sécurité du fournisseur du client ou d'une tierce partie sélectionnée afin de repérer les failles de sécurité potentielles pouvant présenter des risques pour le client.
- Mener une évaluation, en tenant compte de l'une des activités suivantes :
    - Effectuer une (1) évaluation complète des risques sur place pour un (1) environnement de fournisseur tiers.
    - Effectuer deux (2) vérifications rapides de conformité à la norme ISO 27002 sur les sites de différentes tierces parties.
    - Effectuer deux (2) évaluations à distance des risques sans gravité associés à différentes tierces parties.

Livrable

- Rapport sur l'évaluation des risques liés à des tierces parties

4.2.3b. Développement d'un programme de gestion des risques liés aux tierces parties

Renseignements supplémentaires à recueillir

- Les stratégies commerciales, les objectifs et les initiatives qui dépendent des tierces parties, ainsi que les éléments connexes de la stratégie globale
- Les relations essentielles avec des tierces parties, ainsi que les services, les technologies et les produits qui en découlent et leur importance dans les processus opérationnels du client
- Les processus de gestion des risques liés aux tierces parties

Responsabilités de Cisco

- Définir la tolérance générale au risque et confirmer les critères pertinents d'évaluation des risques commerciaux.
- Déterminer les processus pertinents de gouvernance, d'achat, de vérification préalable, de gestion des relations, de garantie et de gestion des risques.
- Analyser les domaines pertinents, ce qui peut comprendre :
    - Inventaire des tierces parties.
    - Établissement des priorités.
    - Élaboration des exigences.
    - Évaluation des risques.
    - Planification de la continuité des activités.
    - Exigences fondées sur les risques.
    - Définition du contrat de niveau de service.
    - Normes et modèles de contrat.
    - Critères de négociation et analyse des répercussions.
    - Procédures de vérification préalable.
    - Gestion de la transition et de la transformation.
    - Surveillance de la performance.
    - Processus de sécurité et d'assurance de la conformité.
    - Structures de gouvernance, surveillance et mécanismes de responsabilité.
- Évaluer les relations représentatives :
    - Valider les exigences du client.
    - Définir un échantillon de relations avec les tierces parties selon la hiérarchisation du client et les risques.
    - Effectuer une évaluation approfondie au moyen d'entrevues avec des intervenants internes et des représentants de tierces parties afin de valider les constatations antérieures et de cerner les nouveaux problèmes liés à la qualité de l'exécution, ce qui couvrira :
        - Gouvernance et protection de l'information.
        - Exigences de conformité.
        - Attentes opérationnelles.
- Évaluer la continuité des activités et la résilience opérationnelle :
    - Examiner la gestion du changement.
    - Effectuer une évaluation des risques.
    - Évaluer et hiérarchiser les risques en fonction de la tolérance au risque de l'entreprise et des critères d'évaluation des risques convenus.
    - Définir le profil de risque.

- Élaborer une feuille de route pour l'amélioration du programme de gestion des risques liés à des tierces parties :
    - Élaborer une feuille de route de perfectionnement fondée sur les risques prioritaires, y compris des recommandations d'amélioration réalisables et des états provisoires tangibles.
    - Estimer le coût, le temps et les ressources nécessaires à la mise en œuvre de la feuille de route de perfectionnement, dans la mesure du possible.

Livrable

- Feuille de route pour l'élaboration d'un programme de gestion des risques liés aux tierces parties.

5. ANALYSES D'INGÉNIERIE

Les analyses d'ingénierie proposent des observations, des recommandations et un soutien à la mise en œuvre afin d'améliorer la stratégie relative au service continu et aux applications du client, l'architecture et la conception, la sélection des fonctionnalités, les exigences de configuration, l'intégrité et les performances, ainsi que l'installation ou les mises à jour des produits.

Navigation par section

La section **Analyse d'ingénierie** inclut les capacités et les livrables de services suivants, qui sont tous associés à un signet pour faciliter la navigation :

5.1. Aperçus des applications

Le service d'observations sur les applications se concentre à aider les clients à analyser et à gérer de façon proactive l'utilisation, l'intégrité et les performances de leurs applications et de leurs ressources de manière à atteindre leurs objectifs commerciaux et opérationnels.

5.1.1. Observations sur l'application de collaboration

Le service d'observations sur l'application de collaboration propose des renseignements sur l'utilisation de la solution de collaboration et génère périodiquement des rapports standard. Les rapports fournissent des informations qui peuvent être utilisées pour la planification de la capacité, ce qui favorise l'adoption et optimise l'application et les services de collaboration.

Remarque : Ce livrable ne prend en charge que les déploiements sur site des applications de collaboration.

Architecture prise en charge

- Collaboration

Renseignements supplémentaires à recueillir

- Informations sur la hiérarchie de l'entreprise, qui contiennent le mappage entre les ID des utilisateurs et les services correspondants.
- Informations sur l'emplacement des différentes grappes.

Responsabilités de Cisco

- Fournir le ou les rapports sur l'application de la collaboration qui peuvent contenir les informations suivantes :
    - Inventaire des ressources
    - Utilisation des services, qualité du service et expérience.
    - Base du modèle d'utilisation de la solution de collaboration et tendances par utilisateur, rôle ou fonction.
    - Si des informations sur la hiérarchie de l'entreprise sont mises à disposition, les rapports peuvent être ventilés par fonction ou par service.

Livrable

- Rapport(s) des observations sur l'application de collaboration

5.1.2. Soutien aux analyses sur la collaboration

Le service de soutien aux analyses sur la collaboration de la solution de collaboration hébergée (HCS) fournira au client des recommandations pour évaluer l'intégrité générale de la plateforme, les défauts logiciels connus, les erreurs de configuration et les logiciels obsolètes pour la solution HCS. Des outils de collecte de données récupèrent les données, qui sont ensuite analysées à l'aide de règles, de seuils et de logiques propres au déploiement du client, puis converties en rapports sommaires livrés selon la fréquence convenue.

Technologies prises en charge

- Solution de collaboration hébergée

Responsabilités de Cisco

- Déployer la trousse de production de rapports sur l'intégrité et l'optimisation des services dans l'environnement HCS ainsi que les scénarios d'analyse des journaux nécessaires à la génération de rapports.
- Configurer la génération de rapports et envoyer les rapports par courriel à une fréquence convenue.
- Entretenir les composants du logiciel de création de rapports.
- Organiser un examen trimestriel de l'intégrité et de l'optimisation de la plateforme, dans un format et selon un calendrier convenus par Cisco et le client lors du lancement des services. L'examen doit se limiter à ce qui suit :
    - Examiner les configurations et formuler des recommandations quant à celles qui devraient être optimisées.
    - Évaluer la sécurité et les autres vulnérabilités détectées, et hiérarchiser les mesures correctives.
    - Repérer les défauts logiciels connus et prendre des mesures correctives.
    - Fournir des conseils sur l'installation et la configuration de tout nouveau produit Cisco.

Livrable

- Rapport sur l'intégrité et l'optimisation

Responsabilités du client

- Indiquer les exigences relatives aux rapports.

5.1.3. Renseignements sur les applications du centre de données

Les renseignements sur les applications du centre de données aident les clients à améliorer la résilience, les performances et la sécurité des charges de travail des applications du client en assurant l'analyse des ressources du centre de données.

Les renseignements sur les applications du centre de données offrent les livrables suivants :

- Mappage des dépendances des applications (ADM)
- Soutien à l'analyse des applications
- Politique de liste blanche et directives d'application

Technologies prises en charge

- Tetration

5.1.3a. Soutien pour le mappage des dépendances des applications (ADM)

Le soutien au mappage des dépendances des applications (ADM) aide le client à examiner les dépendances des applications du centre de données, les performances et la sécurité par l'analyse des flux de données et les politiques existantes, la création d'aperçus d'analyse des applications et la prestation de recommandations de mise en grappe ou de regroupement des terminaux.

Renseignements supplémentaires à recueillir

- Information sur les données de gestion de la configuration du client
- Information sur l'hôte et entrées d'annotation

Responsabilités de Cisco

- Le nombre d'applications et de ponts terminaux dans le champ d'application sera précisé dans le devis.
- Charger l'inventaire vers Tetration Analytics et dériver le champ d'application utilisé afin de regrouper les points d'accès et les terminaux pour les applications.
- Effectuer des examens des dépendances des applications avec le client.
- Fournir une analyse des charges de travail des applications.
- Fournir des modèles de configurations de serveur d'équilibrage de charge (SLB) dans des formats canoniques Tetration Analytics.
- Fournir des annotations définies par l'utilisateur pour l'inventaire de l'hôte sous forme de valeurs séparées par des virgules (.CSV).
- Fournir des recommandations relatives aux grappes/groupements pour les terminaux analysés.
- Créer des espaces de travail d'ADM et des aperçus d'application par application analysée.
- Exécuter des analyses de conformité ponctuelles pour les politiques publiées, par application.
- Créer une politique relative à l'ADM comprenant les éléments suivants (s'il y a lieu) :
    - Politiques de liste blanche entre grappes
    - Politiques de microsegmentation
    - Terminaux dans un EPG
    - Analyse de conformité et recommandations
    - Aperçus des applications

Livrable

- Rapport d'exportation sur la politique relative à l'ADM

Responsabilités du client

- Utiliser les modèles Tetration Analytics de serveur d'équilibrage de charge et les étiquettes de routage fournies par Cisco pour générer les configurations requises dans le cadre de l'analyse d'ADM.

Restrictions

- L'analyse de la charge de travail ne doit pas dépasser cinquante (50) terminaux par application découverte avec les capteurs sous tension; par exemple, toute adresse IPv4/IPv6 est un point terminal dans le cadre de l'exécution d'ADM.
- Le client comprend que si le nombre de terminaux par application dépasse la limite de cinquante (50), Cisco réduira le nombre d'applications qu'elle mappera.
- Cisco réalisera jusqu'à trois (3) évaluations d'application par application.
- Cisco créera au maximum deux (2) espaces de travail d'ADM par application analysée.
- Cisco ne fournira pas plus de trois (3) aperçus d'application par espace de travail d'ADM.
- Cisco ne fournira pas plus de quinze (15) exécutions ou versions d'ADM par application analysée.
- Cisco exécutera au maximum trois (3) analyses de conformité ponctuelles pour les politiques publiées, par application.

5.1.3b. Soutien à l'analyse des applications

Le soutien à l'analyse des applications aide les clients en analysant les flux de données, en définissant et en recommandant des mises à jour de politiques et en assurant ou soutien à la mise à jour de leurs politiques d'ADM.

Responsabilités de Cisco

- Analyser les flux de données par rapport à la politique de liste blanche déployée.
- Analyser les politiques de liste blanche définies par l'utilisateur.
- Mettre à jour les politiques, nouvelles ou existantes, afin d'intégrer les nouveaux capteurs à l'espace de travail d'ADM existant.
- Mettre à jour la politique d'ADM en fonction des besoins de l'environnement :
    - Créer un fichier de définition de grappe de base pour les exécutions d'ADM.
    - Mettre à jour la politique des capteurs pour l'UCT et la bande passante.
    - Mettre à jour les fichiers de configuration d'équilibrage des charges dans les espaces de travail d'ADM.
- Réaliser une (1) des analyses suivantes et formuler une recommandation de mise à jour de la politique :
    - Analyse de visibilité des applications
    - Analyse de l'optimisation des ressources du centre de données
    - Analyse de la fiabilité des applications
    - Analyse de l'échelle et de la redondance de centre de données
    - Analyse des anomalies et des valeurs aberrantes
    - Analyse de la structure du réseau
    - Analyse des modèles de trafic
- Travailler avec les principales parties prenantes du client pour évaluer l'incidence des modifications de politique observées et leur atténuation.
- Créer des expériences de la conformité de la politique Tetration publiée.

Livrable

Rapport d'analyse des applications

Restrictions

- Les éléments suivants sont fournis à la fréquence indiquée :
- Chaque mois
    - Mettre à jour la politique d'ADM, analyser les politiques de listes blanches définies par les utilisateurs et le flux de données actuel, analyser les ressources et l'évolutivité de centre de données, la fiabilité des applications, la structure du réseau, les anomalies et valeurs aberrantes et les modèles de trafic.
    - Créer jusqu'à deux (2) expériences de conformité pour jusqu'à une (1) politique Tetration publiée.
- Chaque trimestre
    - Mettre à jour la politique des capteurs pour l'UCT et la bande passante.
    - Créer jusqu'à un (1) fichier de définition de grappe de base pour les exécutions d'ADM.

- Chaque année
    - Mettre à jour les fichiers de configuration d'équilibrage des charges dans les espaces de travail d'ADM.

5.1.3c. Politique de liste blanche et directives d'application

La politique de liste blanche et les directives d'application facilitent la mise en œuvre par le client d'un cadre de politique de liste blanche Tetration qui est intégré à l'application de centre de données, au réseau, aux conceptions de sécurité, aux politiques et aux configurations du client. Cisco fournira une analyse des conclusions et des recommandations générales afin d'aider à remédier aux failles en matière de conception, de politique et de configuration.

Dépendances

- Le client doit disposer de la licence logicielle complémentaire d'application de politique et de segmentation des applications Cisco Tetration pour ce livrable.

Renseignements supplémentaires à recueillir

- Active Directory (AD), système de noms de domaine (DNS) et information sur l'adresse IP du serveur.
- Informations spécifiques à un réseau de centre de données ACI existant :
    - Exigences ACI et document de conception « tel quel »
    - Cadre et stratégie d'adoption de la politique de centre de données
- Renseignements propres au réseau de centre de données non ACI :
    - Exigences et document de conception « tel quel ».
    - Stratégie d'adoption de la politique de centre de données

Responsabilités de Cisco

- Le nombre d'applications et de ponts terminaux dans le champ d'application sera précisé dans le devis.
- Travailler avec le client pour lui faire comprendre son environnement actuel d'infrastructure de centre de données et les conditions requises pour l'application de la stratégie de liste blanche de Tetration au cadre de politique de centre de données du client.
- Cisco doit fournir un cadre de politique de liste blanche et des directives concernant l'application de la politique, notamment :
    - Microsegmentation avec application aux terminaux.
    - Comparaison de la politique de Tetration aux ACL existants concernant les applications comprises dans le champ d'application.
- S'il y a lieu, Cisco fera des recommandations sur les règles de pare-feu existantes ou les contrats ACI en se basant sur les politiques de liste blanche et l'analyse de la politique Tetration qui en résulte. Les recommandations comprendront notamment, sans toutefois s'y limiter, les éléments suivants :
    - Règles ou contrat inutilisés
    - Règles ou contrats sous-utilisés
    - Règles ou contrat absents

- Effectuer une séance d'examen de la conception du client en fonction d'un (1) des éléments suivants :
    - Réseau de centre de données ACI existant
    - Comparaison des exigences du Client avec la conception ACI pour centre de données Cisco, la politique de sécurité et de réseau des applications, le groupement des applications; formulation de recommandations de conception générale pour résoudre les failles relevées à l'aide de ce qui suit :
    - Conception de trame
    - Configurations de locataires/profils des applications/groupe de terminaux
    - Intégration des couches 4 à 7 (pare-feu et équilibreur de charges)
    - Réseau de centre de données non ACI
    - Comparaison des exigences du client avec la conception de centre de données Cisco, la politique de sécurité et de réseau des applications, le groupement des applications; formulation de recommandations de conception générale pour résoudre les failles relevées à l'aide de ce qui suit :
        - Architecture L2/L3 de centre de données
        - Intégration des couches 4 à 7 (pare-feu et équilibreur de charges)
- Évaluer les aspects de la conception et du modèle de déploiement du client, notamment l'emplacement des périphériques, la connectivité physique et logique, ainsi que l'administration réseau selon les meilleures pratiques de Cisco.

Livrable

- Rapport sur la politique de liste blanche et les directives d'application

Responsabilités du client

- Faciliter l'examen d'ACL des pare-feu de tiers avec les fournisseurs tiers.
- Faciliter l'application des politiques des pare-feu de tiers avec les fournisseurs tiers.

Restrictions

- Le cadre de politique de liste blanche et les directives d'application Cisco permettent une microsegmentation avec application à jusqu'à cinquante (50) terminaux par application.
- Cisco participera, au plus, à trois (3) séances d'évaluation de la conception à distance de deux (2) heures, pendant deux (2) semaines avec le client.

5.2. Observations sur le service

Le service d'observations sur le service se concentre à aider les clients à analyser et à gérer de façon proactive l'intégrité et les performances de leurs services et de leurs ressources d'application ou d'infrastructure de manière à atteindre leurs objectifs commerciaux et opérationnels.

5.2.1. Observations sur l'infrastructure ACI

Le service d'observations sur l'infrastructure ACI aide à améliorer l'harmonisation avec les politiques d'application et les meilleures pratiques du client en s'efforçant d'établir de façon proactive l'ordre de priorité de l'utilisation de ressources et d'appuyer les besoins de croissance future.

Technologies prises en charge

- Infrastructure centrée sur les applications
- Sécurité de réseau

Renseignements supplémentaires à recueillir

- Les données recueillies par le contrôleur APIC (Application Policy Infrastructure Controller) comprennent notamment des données du système, des journaux, des ressources matérielles et logicielles et des notes sur l'intégrité.

Responsabilités de Cisco

- Optimiser les performances de la structure en passant en revue les exceptions au moyen de l'analyse des données du système, des journaux et des ressources matérielles et logicielles qu'a recueillis le contrôleur APIC.
- Analyser les anomalies, la relation avec les objets gérés, les déclencheurs et l'incidence sur la fonctionnalité.
- Procéder à une analyse périodique des notes sur l'intégrité générées par le contrôleur APIC et des problèmes ayant une incidence sur ces notes et déchiffrer les codes d'anomalie, la relation avec les objets gérés, les déclencheurs et l'incidence sur la fonctionnalité.

Livrable

- Soutien consultatif et conseils seulement

5.2.2. Analyses des ressources du réseau à optimisation autonome (SON)

Le service d'analyses du réseau à optimisation autonome (SON) assure l'équilibrage et la gestion des ressources du réseau d'accès radio (RAN) à travers les couches et les sites pour aider le client à réduire la congestion et améliorer les IRC du RAN.

Solutions prises en charge

- Réseau à optimisation autonome
  - Politique de mobilité et accès

Renseignements supplémentaires à recueillir

- Objectifs de performance du RAN et seuils des IRC.

Responsabilités de Cisco

- Générer et réviser régulièrement les rapports de congestion cellulaire du SON (veille stratégique), et avoir des discussions avec le client sur les congestions et les objectifs.
- Analyser les rapports cellulaires pour des déclenchements élevés sur l'utilisation de puissance HS et non HS, le code et l'UL H/W pour isoler les cellules encombrées.
- Aider le client à optimiser le RAN mobile à travers les couches et les différents sites cellulaires en tirant parti des modules d'équilibrage de charge interopérateurs (ICLB) et d'équilibrage de charge dynamique (DLB) du SON.

Livrable

- Soutien consultatif et conseils seulement

Responsabilités du client

- Examiner régulièrement les rapports sur la congestion cellulaire.
- Travailler avec un spécialiste en ingénierie-conseil de réseau de Cisco pour configurer et optimiser les modules du SON.

5.3. Performance et capacité

Le service Performance et capacité offre en temps quasi réel des observations prédictives et une corrélation des performances, de la qualité, de la capacité et de l'utilisation pour aider le client à résoudre des problèmes tels que la dégradation du service et une expérience utilisateur sous-optimale.

Le service Performance et capacité fournit les livrables suivants :

- Observations sur la performance et la capacité
- Assistance au réglage des performances
- Analyses des tests de performance
- Analyse des informations sur la performance
- Évaluation de la capacité

5.3.1. Observations sur la performance et la capacité

Le service d'observations sur la performance et les capacités fournit de manière automatisée et en temps quasi réel des analyses des IRC les moins reluisants, de l'utilisation et des tendances, met en corrélation les conclusions et formule des recommandations pour remédier aux problèmes afin de réaliser des gains de performance et de capacité.

Exclusions

** Propre au réseau central de transmission par paquets et à la politique de mobilité et d'accès*

- Le réseau de transmission par paquets Ultra (Ultra Packet Core ou UPC) de Cisco n'est pas pris en charge par les livrables du service Observations sur la performance et la capacité.

Technologies prises en charge

- Politique de mobilité et accès
- Réseau central de transmission par paquets

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Réseau central de transmission par paquets

Responsabilités de Cisco

- Le service Observations sur la performance et la capacité se compose des caractéristiques décrites ci-dessous :
  - Les IRC de performance et de capacité les moins reluisants, ainsi que les tendances observables.
  - Corrélation des IRC de performance et de capacité touchés par les alarmes, l'exploitation des ressources, le journal de système ou les dépassements de seuils.
  - Les comportements de performance à l'aide de tendances historiques et d'algorithmes prédictifs.

Autres responsabilités

** Propre aux technologies prises en charge : réseau central de transmission par paquets et accès et politique de mobilité*

Pour l'ensemble amélioré :

- Comprend des tableaux de bord intelligents de corrélation – IRC, journaux et capacité

Pour l'ensemble Premium :

- Comprend l'ensemble amélioré.
- Fournir une détection d'anomalie basée sur l'apprentissage machine, ainsi que des seuils.
- Mettre à jour les IRC, les tableaux de bord et les algorithmes des analyses prédictives et normative avancées.
- Mettre à jour les API aux fins de leur intégration avec d'autres domaines Cisco (p. ex. liaison IP, GiLAN, routage et commutation) et les nœuds tiers.
- Analyse au niveau de l'abonné en fonction de la consommation des journaux du moteur pour l'utilisation des renseignements commerciaux et des renseignements sur les abonnés.
- Mettre à jour les API aux fins de l'intégration des alertes avec OSS ou NMS.

Livrable

- Fonctionnalité du portail : observations sur la performance et la capacité

5.3.2. Assistance au réglage des performances

Le service Assistance au réglage des performances (Performance Tuning Support ou PTS) permet d'évaluer les écarts par rapport aux objectifs de performance, aux politiques et aux configurations et d'aider le client en lui fournissant des recommandations de réglages pour mettre au point la performance, la sécurité et la résilience.

Technologies prises en charge

- Réseau sans fil
- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Calcul en périphérie de réseau de l'IDO et informatique géodistribuée
- Réseautique industrielle et collaboration

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques
- Réseau étendu défini par logiciel
  - Routage et commutation
  - Gestion et orchestration de réseau
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage

Exclusion

** Propre à l'orchestration et à l'automatisation de centre de données*

- Cisco CloudCenter (CCC) n'est pas pris en charge.

Renseignements supplémentaires à recueillir

- Écarts de performance, exigences relatives aux réglages, stratégies et préoccupations.

Responsabilités de Cisco

- Analyser la mise en œuvre des politiques et l'alignement sur les politiques et procédures de l'entreprise et les meilleures pratiques de Cisco.
- Analyser les fonctionnalités et la configuration du système pour maximiser les performances et la résilience.
- Recommander des domaines pouvant nécessiter une analyse complémentaire, comme l'architecture et la conception, le respect continu des politiques, la gestion de la configuration et la gestion des instruments (si jugé nécessaire par Cisco).

Autres responsabilités

** Propre au réseau sans fil*

- Effectuer la collecte de données sur site et les tests des cas d'utilisation demandés par le client.
- Fournir une (1) séance interactive de réglages avec le client pour mettre en œuvre les recommandations.
- Aider le client avec les tests et la validation des modifications.

Livrable

- Rapport sur le réglage des performances

Restrictions

** Propre à la sécurité du réseau, à la sécurité du nuage, à la politique de sécurité et d'accès et à la menace avancée*

- Le service d'assistance en matière d'adaptation des performances de sécurité (Security PTS) n'est pas conçu pour des systèmes et des solutions complexes comme les environnements ISE de Cisco, les déploiements de contrôle d'accès sécurisé (ACS) de Cisco et les périphériques réseau prenant en charge des déploiements 802.1x complexes.
    - Chaque unité d'assistance au réglage des performances de sécurité comprend jusqu'à un (1) ensemble de solutions ou un (1) type de périphérique de service :
        - Un (1) ensemble de solutions (c'est-à-dire une solution de pare-feu, une solution de RPV, un système de prévention des intrusions [IPS]), qui est composé de ce qui suit :
            - Jusqu'à cinq (5) périphériques avec un ensemble de solutions donné pour la première unité de service Security PTS.
            - Jusqu'à cinq (5) périphériques de plus pour des unités de service Security PTS.
            - Si une nouvelle solution est ajoutée, par exemple, si le service Security PTS comprend des solutions de pare-feu et de RPV, alors deux unités de service Security PTS prennent en charge jusqu'à (10) dispositifs de pare-feu ou de RPV à analyser et à adapter.

        - Jusqu'à quinze (15) périphériques de plus pour des unités de service Security PTS.
            - Si l'ensemble de solutions n'est pas modifié, par exemple, si le service Security PTS inclut une solution de RPV, alors deux unités de service Security PTS prennent en charge jusqu'à (20) dispositifs de RPV à analyser et à adapter.
    - Un (1) type de périphérique de sécurité (c.-à-d., des périphériques de sécurité polyvalents prenant en charge les pare-feu, les RVP et les IPS), qui est composé de ce qui suit :
        - Jusqu'à deux (2) périphériques de sécurité.

** Propre aux systèmes NFVI, SAE, MSX*

- L'assistance aux réglages de performance n'est pas fournie pour les fonctions réseau virtualisées (Virtualized Network Functions ou VNF) tierces.

5.3.3. Analyses des tests de performance

Le service Analyse de test de performance fournit au client un rapport sur les IRC, des seuils, les recommandations pratiques et les améliorations de la performance et de la qualité du réseau.

Technologies prises en charge

- Réseau central de transmission par paquets

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
    - Réseau central de transmission par paquets

Responsabilités de Cisco

- Élaborer un rapport comparatif de test de performance de réseau en fonction de la similarité du nombre de nœuds et du profil de modèle d'appel dans des réseaux de pairs afin d'attirer l'attention et les efforts vers des domaines nécessitant des améliorations en matière de performance de réseau. En fonction des domaines couverts, le rapport peut comprendre ce qui suit :
    - Les IRC du plan de contrôle ou du plan utilisateur.
    - Un examen des observations et des résultats.
    - Des recommandations pratiques pour améliorer la qualité du réseau.

Livrable

- Rapport de test de performance du réseau

5.3.4. Rapports d'observation sur les performances

Le service Rapports d'observation sur les performances offre au client une analyse des IRC des systèmes et des applications les plus problématiques, les corrélations entre les résultats et des recommandations pour corriger les problèmes afin d'améliorer les performances et d'obtenir des gains opérationnels.

Technologies prises en charge

- Réseau central de transmission par paquets

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Réseau central de transmission par paquets

Responsabilités de Cisco

- Élaborer un rapport qui comprendra une liste des indicateurs clés de réseau selon le domaine précisé dans le devis de services; le rapport fournira des vues et des seuils regroupés et peut comprendre les éléments suivants :
  - Vue d'ensemble de la performance du réseau.
  - Identification des IRC et des tendances les plus problématiques.
  - Recommandation de mesures correctives en fonction des indicateurs problématiques détectés.
  - Indication préventive d'indicateurs problématiques.
  - Corrélation avec d'autres sources de données comme les journaux système, les configurations ou les erreurs d'interruption SNMP.
  - La synchronisation des erreurs détectées en fonction des problèmes connus dans la base de connaissances de Cisco.

Livrable

- Rapports d'observation sur les performances

5.3.5. Évaluation de la capacité

L'évaluation de la capacité établit un niveau de référence pour analyser les effets de la croissance actuelle et prévue et fournir au client des recommandations pour l'alignement sur les exigences de capacité.

Technologies prises en charge

- Réseau optique
- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données
- Solution de collaboration hébergée
- Réseau central de transmission par paquets

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Virtual Packet Core
  - Réseau central de transmission par paquets
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Exclusion

** Propre à l'orchestration et à l'automatisation de centre de données*

- Cisco CloudCenter (CCC) n'est pas pris en charge.

Renseignements supplémentaires à recueillir

- Les modifications prévues liées à l'augmentation, à la diminution ou au regroupement des ressources de l'infrastructure et des applications.
- La capacité de bande passante, les tendances d'utilisation des profils de trafic, les dernières mises à niveau et modifications ainsi que les plans futurs.

Responsabilités de Cisco

- Formuler des recommandations pour un déploiement et des configurations optimales en se basant sur les données recueillies et l'analyse des résultats; les recommandations peuvent inclure, sans toutefois s'y limiter, ce qui suit :
    - Architecture de référence mettant en évidence les options d'augmentation de la capacité basées sur les meilleures pratiques de Cisco.
    - Modifications aux réglages pour optimiser l'utilisation des ressources.
    - Meilleures pratiques en matière de surveillance de l'utilisation du réseau et de ses éléments.
    - Limites publiées de l'extensibilité du matériel déployé par Cisco.

Livrable

- Rapport d'évaluation de la capacité

Restriction

** Propre au réseau optique*

- Le champ d'application de l'évaluation de la capacité est limité à la disponibilité des connecteurs, des interfaces et des longueurs d'onde des nœuds qui sont accessibles à distance. La capacité du circuit est hors du champ d'application.

** Propre aux systèmes NFVI, SAE, MSX*

- L'évaluation de la capacité ne prend en charge que les modifications aux réglages qui optimisent l'utilisation des ressources.

6. ORCHESTRATION ET AUTOMATISATION

Le service d'orchestration et d'automatisation fournit de l'aide au client pour l'adoption et le soutien de l'orchestration et de l'automatisation de la prestation de services, des applications et des flux de travail.

Navigation par section

La section **Orchestration et automatisation** décrit les capacités et les livrables de services suivants, qui sont tous associés à un signet pour faciliter la navigation :

6.1. Orchestration des services

L'orchestration du service se concentre sur l'aide aux clients pour planifier, développer, tester, mettre en œuvre, soutenir et améliorer les modèles et flux de travail d'orchestration de service afin d'atteindre leurs objectifs commerciaux et opérationnels.

6.1.1. Prise en charge du développement du modèle de service

Le service de prise en charge du développement du modèle de service aide le client à accélérer le développement et la mise en œuvre de nouveaux modèles de service dans un environnement DevOps itératif.

Cisco collaborera avec le Client en vue d'adopter un cycle de vie DevOps (développement et exploitation) d'analyse, de développement, d'amélioration, de tests et de déploiement des capacités et des modèles d'orchestration de services réseau, d'EMS/NMS d'orchestration de service et de centre de données avec plusieurs interactions/instances.

Technologies prises en charge

- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Responsabilités de Cisco

- Fournir les services à la demande du client, ce qui peut comprendre les services suivants :
  - Analyser et élaborer de nouveaux modèles de service dans un environnement itératif de DevOp.
  - Aider à configurer les périphériques dans le cadre des nouveaux services.
  - Soutien à la mise en œuvre logicielle, comme indiqué dans le devis et dans la section « Autres responsabilités » ci-dessous.
  - Prodiguer des conseils sur la modélisation YANG, FastMap/Java, et la validation NED pour le service NSO.
  - Prodiguer des conseils sur les modèles de configuration, les flux de processus et les flux de provisionnement pour les services suivants : UCS-D, CPO, PSC, Prime Portfolio et autres produits EMS, NMS, de centre de données et en nuage de Cisco.

Autres responsabilités

** Propre aux ensembles de services d'automatisation et à l'automatisation des processus opérationnels.*

- Comme précisé dans le devis.
- Soutien à la mise en œuvre logicielle pour :
    - Mise en œuvre haute disponibilité de la plateforme centrale (facultatif)
    - Mise en œuvre haute disponibilité + récupération après sinistre (facultatif)
    - Mise en œuvre des ensembles de services (facultatif)
    - Environnement de laboratoire (facultatif)
    - Environment de solution (facultatif)

** Propre au domaine en nuages multiples*

Comme précisé dans le devis.

- Mise en œuvre logicielle pour :
    - Composants Nexus et ACI
    - Plateforme de données Hyperflex avec Cisco Intersight
    - Intégration avec un (1) fournisseur de nuage public
    - CSR1000v
    - Suite CloudCenter
    - Cisco Container Platform (CCP) sur Hyperflex
    - Cisco Workload Optimization Manager d'OVA comme suit :
    - Intégration avec Stealthwatch Cloud

Livrable

- Soutien consultatif et conseils seulement

7. EXPERT-CONSEIL SUR PLACE

Un expert-conseil sur place fournit aux clients des services de conseil d'ingénierie pour les initiatives d'ingénierie pour la conception et la livraison des solutions Cisco, les architectures technologiques, l'orchestration et l'automatisation de service, l'analyse de l'infrastructure et des applications, les risques liés à la sécurité opérationnelle et les stratégies de protection.

Navigation par section

La section **Expert-conseil sur place** inclut les capacités et les livrables de services suivants, qui sont tous associés à un signet pour faciliter la navigation :

7.1. Conseiller avisé

Le conseiller de confiance fournit du leadership pour permettre aux clients de bénéficier des Services opérationnels essentiels Cisco pour l'ingénierie en mettant l'accent sur la planification, la coordination et la livraison des capacités requises à l'aide d'approches sur le site et à distance.

7.1.1. Expert-conseil sur site

Le service Expert-conseil sur site est fourni dans le lieu désigné par le client jusqu'à cinq (5) jours par semaine (sous réserve des restrictions de travail locales) pendant les heures de bureau standard.

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Gestion et orchestration de réseau
- Systèmes informatiques
- Tetration
- Orchestration et automatisation de centre de données
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Communications unifiées
- Service à la clientèle
- Collaboration vidéo
- Réunions et messagerie infonuagiques
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services

Solutions prises en charge

- Réseau étendu défini par logiciel
  - Routage et commutation
  - Gestion et orchestration de réseau
- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- Réseau virtuel de transmission par paquets
  - Réseau central de transmission par paquets
- Infrastructure de virtualisation des fonctions de réseau (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Réseau central de transmission par paquets
- Secure Agile Exchange (SAE)
  - Routage et commutation
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Responsabilités de Cisco

- Comprendre les initiatives et les exigences technologiques du client et offrir des conseils et une orientation visant l'atteinte des objectifs du client.
- Aligner les objectifs du client sur les services et les livrables commandés par le client.
- Recueillir les renseignements et les exigences grâce à des réunions avec le client pour la planification, le séquencement et la réalisation des livrables.

Remarque :

- Cisco peut juger nécessaire d'offrir les livrables dans une combinaison de service de consultation sur site et de soutien à distance.
- Les tâches dirigées par le client qui doivent être effectuées par le spécialiste en ingénierie des services avancés de Cisco sont régies selon le service et les livrables commandés par le client et sont soumises à l'approbation de Cisco, qui ne doit pas être refusée sans raison valable.

Autres responsabilités

Gestion et orchestration de réseau, orchestration et automatisation du centre de données, orchestration du service de réseau

- Désigner un spécialiste en ingénierie Cisco pour représenter le client et communiquer les exigences du client à la planification de produit Cisco, y compris le soutien de la solution logicielle et les activités de maintenance continue.

** Propre au réseau sans fil*

- Fournir un soutien proactif sur site pour les événements du Client utilisant une infrastructure de mobilité Cisco gérée pour les utilisateurs finaux et l'accès des spectateurs et des participants.
- Tirer parti de l'infrastructure Cisco Prime® (PI), du moteur MSE et, s'il y a lieu, du portail d'observations sur la mobilité (MIP).
- Analyser les renseignements suivants :
    - Indicateurs de rendement clés (IRC).
    - Seuils de performance de réseau souhaités.
    - Éléments de l'infrastructure réseau et outils de gestion disponibles.
    - Indicateurs de suivi de l'utilisation, du comportement et des analyses du client.
- Effectuer les tâches d'assistance suivantes :
    - Surveiller la performance et l'intégrité globale du réseau sans fil pendant toute la durée de l'événement.
    - Fournir, dans la mesure du possible, des services de dépannage et de soutien liés à l'infrastructure sans fil pendant l'événement.
    - Fournir le client sans fil de base et le dépannage sur demande de l'utilisateur final pendant l'événement, dans la mesure du possible.
- Fournir au personnel du client l'assistance, les capacités ou la documentation suivantes :
    - Fournir un accès au portail MIP de Cisco géré dans le nuage.
    - Fournir les observations ou les recommandations nécessaires avant, pendant et après l'événement.
    - Élaborer le rapport d'observation sur les performances du réseau en fonction des données, des analyses et des renseignements propres au client qui ont été recueillis.
- Fournir un point de contact unique et désigné pour toutes les questions liées à l'événement, et ce, tout au long de l'événement en direct.

- Fournir un soutien aux parties prenantes du client responsables de l'exécution des tâches liées à l'événement.
- Mettre à disposition le personnel et/ou l'accès au site afin que Cisco puisse assurer le soutien dans le cadre de l'événement.

Livrables

- Les livrables pris en charge par le service de consultation sur site sont basés sur ceux du volet Service pour l'ingénierie précisés dans le devis des services commandés par le client, qui peuvent comprendre les composants suivants :

Conception et validation	• Étude de la conception • Assistance permanente à la conception • Développement de la conception • Prise en charge des modifications de conception • Soutien à la validation des tests sur site • Tests sur site de l'état de préparation de l'architecture
Ingénierie des fonctionnalités	• Évaluation de fonctionnalité avancée • Planification et mise en œuvre de l'assistance pour la migration
Gestion des connaissances	• Séance de transfert de connaissances pour l'ingénierie
Conformité de la configuration	• Conformité à la procédure de configuration • Assistance à la configuration et aux modifications logicielles • Conformité et correction de la configuration • Conformité et correction du logiciel
Soutien adapté pour l'intégration	• Assistance à l'intégration de la solution de gestion • Assistance à l'intégration des API dans l'infrastructure ACI
Développement d'un programme de sécurité	• Assistance en matière de planification et de stratégie de sécurité
Observations sur le service	• Observations sur l'infrastructure ACI
Orchestration des services	• Prise en charge du développement du modèle de service

Responsabilités du client

- Donner à Cisco des directives au sujet des activités, des priorités et des projets pour lesquels le client a besoin de l'aide du spécialiste en ingénierie de Cisco.