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

Services pour les opérations

Ce document contient la description détaillée des capacités et des livrables associés aux services opérationnels essentiels Cisco pour les opérations.

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 LES OPÉRATIONS

Les Services opérationnels essentiels Cisco **pour les opérations** de Cisco englobent les capacités et les livrables à l'appui de la disponibilité, de la performance, de la conformité à la sécurité et de la gestion de l'infrastructure et de l'environnement d'applications Cisco. Les livrables décrits dans le volet Services pour les opérations sont présentés en fonction des fonctionnalités et des technologies, solutions ou architectures prises en charge.

CAPACITÉS ET LIVRABLES DES SERVICES POUR LES OPÉRATIONS

Les capacités et les livrables du volet Services pour les opérations aident les clients avec l'optimisation des opérations et de la gestion de l'infrastructure réseau et des technologies d'application.

1. ANALYSES OPÉRATIONNELLES

Les analyses opérationnelles aident le client en fournissant des observations et des recommandations sur les lacunes système, logicielles et opérationnelles qu'il faut corriger pour optimiser la performance, la disponibilité et la sécurité du réseau et de l'architecture des applications de Cisco.

NAV. SECT.

La section **Analyses opérationnelles** inclut les composants de service suivants, qui sont tous marqués d'un signet pour faciliter la navigation :

1.1. Observations sur la plateforme

Le service d'observations sur la plateforme permet de révéler les lacunes et les risques potentiels qu'il faut corriger pour optimiser la disponibilité, la stabilité et la performance de l'infrastructure et de l'environnement d'application de Cisco. Le service aide aussi à évaluer l'efficacité de l'environnement Cisco afin de planifier les changements actuels et futurs en fonction de l'évolution des exigences et des impératifs opérationnels du client.

Le service comprend la collecte et l'analyse des données des environnements vérifiés ou post-déploiement qui nécessitent un examen planifié régulier ou supplémentaire, selon les besoins et les préoccupations du client.

Exclusions

** Propre au réseau sans fil*

- Les réseaux Cisco Meraki ne sont pas pris en charge.

** Propre aux systèmes informatiques*

- CiscoHyperFlex® n'est pas pris en charge.

** Propre à la commutation de centre de données*

- La plateforme de contrôle des applications (Application Control Engine ou ACE) de Cisco n'est pas prise en charge.

** Propre à l'automatisation, à l'intégration et à la gestion*

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

** Propre à la politique de sécurité et à l'accès*

- Le Centre de gestion FirePower™ (Firepower Management Center ou FMC) et le moteur ISE (Identity Services Engine) ne sont pas pris en charge.

1.1.1. Observation sur la plateforme de type 1 – Rapports générés manuellement ou par l'outil de collecte de données de Cisco

Le service d'observations sur la plateforme de type 1 fournit les rapports suivants :

- Meilleures pratiques en matière de configuration de type 1
- Étapes importantes du cycle de vie du matériel de type 1
- Analyse diagnostique de type 1
- Avis de problème constaté de type 1 (s'il y a lieu)
- Rapport de vérification de type 1

1.1.1a. Meilleures pratiques en matière de configuration de type 1

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

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 Cisco (Network Function Virtualization Infrastructure ou NFVI)
  - Routage et commutation
  - Systèmes informatiques
- Virtual Packet Core
  - Systèmes informatiques
  - Commutation de centres de données
  - Réseau central de transmission par paquets
- Secure Agile Exchange (SAE)
  - 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
  - Systèmes informatiques
  - Commutation de centres de données
  - Orchestration et automatisation de centre de données
  - Sécurité du nuage

Livrables

- Rapport sur les meilleures pratiques en matière de configuration de type 1

Restrictions

** Propre au routage et à la commutation*

- Le questionnaire et la feuille de travail sont les seules méthodes de collecte de données prises en charge pour la collecte d'informations destinées au rapport sur les meilleures pratiques en matière de configuration.
- Un (1) rapport sur les meilleures pratiques en matière de configuration peut contenir jusqu'à cinq (5) configurations de périphérique.

** Propre au réseau optique*

- Un (1) rapport sur les meilleures pratiques en matière de configuration peut contenir jusqu'à cinquante (50) configurations de périphérique.
- Le champ d'application du rapport sur les meilleures pratiques en matière de configuration se limite aux seuils de puissance optique.

** Propre au réseau central virtuel de transmission par paquets*

- Pour une solution de Réseau central virtuel de transmission par paquets, un (1) rapport sur les meilleures pratiques en matière de configuration contient jusqu'à cinq (5) configurations de périphérique.

1.1.1b. Étapes importantes du cycle de vie du matériel de type 1

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Infrastructure vidéo des fournisseurs de services
- Accès par câble de prochaine génération

Solutions prises en charge

- WAN défini par logiciel
  - Routage et commutation
- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données

Livrables

- Rapport sur les étapes importantes du cycle de vie du matériel de type 1

Restrictions

** Propre au routage et à la commutation*

- Le questionnaire et la feuille de travail sont les seules méthodes de collecte de données prises en charge pour la collecte d'informations destinées au rapport sur les étapes importantes du cycle de vie du matériel.
- Un (1) rapport sur les étapes importantes du cycle de vie du matériel contient jusqu'à cent (100) périphériques.

** Propre au réseau optique*

- Un (1) rapport sur les étapes importantes du cycle de vie du matériel contient jusqu'à cinquante (50) périphériques.

1.1.1c. Analyse diagnostique de type 1

Technologies prises en charge

- Réseau optique
- 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
- Infrastructure vidéo des fournisseurs de services
- Accès par câble de prochaine génération

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données
  - Réseau central de transmission par paquets

Responsabilités de Cisco

- Analyser les données diagnostiques des périphériques du client pour déceler les risques potentiels.

Responsabilités supplémentaires de Cisco

** Spécifique au réseau central de transmission par paquets, solution de Réseau central virtuel de transmission par paquets, à l'exclusion des systèmes informatiques et de la commutation de centre de données*

- Analyser les données des journaux système pour formuler des recommandations basées sur les éléments suivants :
- La corrélation entre les événements des journaux système, les données sur l'intégrité du réseau mobile de transmission par paquets et les mesures de base

** Propre au réseau optique*

- Analyser les données des journaux système pour formuler des recommandations basées sur les éléments suivants :
- Les alertes et les conditions, les ressources système et l'environnement de l'étagère.

Livrables

- Rapport d'analyse diagnostique et de recommandations de type 1

Restrictions

** Propre au réseau optique*

- Un (1) rapport d'analyse diagnostique et de recommandations contient jusqu'à cinquante (50) périphériques.
- Le champ d'application du rapport d'analyse diagnostique et de recommandations se limite aux données d'alerte et de circuit, aux activités d'utilisateur, au provisionnement et à la maintenance des données d'accès.

1.1.1d. Avis de problème constaté de type 1 (s'il y a lieu)

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- 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
- Infrastructure vidéo des fournisseurs de services
- Accès par câble de prochaine génération

Solutions prises en charge

- WAN défini par logiciel
  - Routage et commutation
- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données
  - Réseau central de transmission par paquets

Livrables

- Rapport d'analyse d'avis de problème constaté et de recommandations de type 1

Restrictions

** Propre au routage et à la commutation*

- Le questionnaire et la feuille de travail sont les seules méthodes de collecte de données prises en charge pour la collecte d'informations destinées au rapport d'analyse d'avis de problème constaté et de recommandations.
- Un (1) rapport d'analyse d'avis de problème constaté et de recommandations contient jusqu'à cent (100) périphériques.

** Propre au réseau optique*

- Un (1) rapport d'analyse d'avis de problème constaté et de recommandations contient jusqu'à cinquante (50) périphériques.

1.1.1e. Rapport de vérification de type 1

Technologies prises en charge

- Réseau optique
- 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
- 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

- Communications unifiées
- Collaboration vidéo
- Service à la clientèle
- Infrastructure vidéo des fournisseurs de services
- Accès par câble de prochaine génération

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- 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 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
- 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
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Responsabilités de Cisco

- Analyser les informations, ce qui peut comprendre, sans toutefois s'y limiter, ce qui suit :
- Performances et recommandations de réglages.
- Analyse de l'utilisation des ressources aux fins de planification.
- Recommander des domaines nécessitant une analyse complémentaire, comme l'architecture et la conception ou de l'alignement des politiques et des normes.

Autres responsabilités

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

- Recueillir des informations sur les pratiques de travail du client quant au maintien de l'architecture ACI.
- Faire l'alignement sur l'architecture de pointe applicable.

Responsabilités exclues

** Propre aux systèmes informatiques et à la commutation de centre de données*

- L'analyse et le rapport de vérification n'abordent pas ce qui suit :
  - Stabilité, performances et recommandations de réglages.
  - Analyse de l'utilisation des ressources aux fins de planification.

Livrables

- Rapport de vérification de type 1

Responsabilités du client

- Remplir le questionnaire ou la feuille de calcul de vérification de la plateforme, s'il y a lieu.
- Exécuter toutes les étapes préalables à la vérification exigées par Cisco pour que toutes les données soient accessibles lors de la vérification.
- Aviser de tout retard lié aux modifications planifiées au cours de la procédure de vérification.

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 rapport de vérification de type 1 est limité à ce qui suit :
  - Jusqu'à un (1) ensemble de solutions ou un (1) système complexe (par exemple, la plateforme de services d'identité [ISE], le système de contrôle d'accès sécurisé [ACS] de Cisco ou les déploiements 802.1x).
  - Jusqu'à vingt (20) périphériques.

** Propre à la commutation de centre de données*

- Un (1) rapport de vérification de type 1 limité aux commutateurs de la série Cisco Nexus par instance de centre de données.

** Propre au réseau optique*

- Un (1) rapport de vérification de type 1 peut contenir jusqu'à cinquante (50) périphériques.
- Le champ d'application du rapport de vérification de type 1 se limite à l'adressage IP, au réseau de communications de données (DCN) et à l'utilisation de canal du multiplexage par répartition en longueur d'onde dense (DWDM).

** Propre aux systèmes NFVI, SAE, MSX*

- Le rapport de vérification de type 1 est limité à ce qui suit :
  - Analyse de l'utilisation des ressources de l'utilisation du processeur, de la mémoire, de l'état des services exécutés à des fins de planification.

1.1.2. Observations sur la plateforme de type 2 – Fonctionnalités d'expert-conseil et d'analyses hébergées en nuage de Cisco

Exclusions

** Propre aux systèmes informatiques*

- Les serveursUCS de sérieC qui ne sont pas connectés à l'interconnexion de la trame ne sont pas pris en charge par les livrables de type 2 du service d'analyses et d'observations sur la plateforme.

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

- Le réseau de transmission par paquets Ultra (UPC) de Cisco n'est pas pris en charge par les livrables le service d'observations sur la plateforme, type 2.

Livrables

Le service d'observations sur la plateforme de type2 fournit les fonctionnalités et les rapports suivants :

- Meilleures pratiques en matière de configuration de type 2
- Type 2 Hardware Lifecycle Milestones
- Analyse diagnostique de type 2
- Avis de problèmes constatés de type 2
- Rapport de vérification de type 2
- Type 2 en option : prise en charge tierce

1.1.2a. Type 2 – Fonctionnalités d'expert-conseil et d'analyses hébergées standard : pratiques exemplaires de configuration

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Réseau de stockage
- Infrastructure centrée sur les applications

- Réseau central de transmission par paquets
- Sécurité de réseau
- Commutation de centres de données
- Politique de mobilité et accès
- Communications unifiées

Solutions prises en charge

- Virtual Packet Core
  - Commutation de centres de données
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil

Livrables

- Meilleures pratiques en matière de configuration de type 2

Restrictions

** Propre au réseau sans fil*

- Fonctionnalité standard de type 2 : les meilleures pratiques en matière de configuration ne sont prises en charge que pour les points d'accès autonomes Cisco.

** Propre à la sécurité du réseau*

- Les meilleures pratiques en matière de configuration de type 2 ne sont prises en charge que pour les appareils Adaptative Security Appliance (ASA) de Cisco.

** Propre aux communications unifiées*

- Fonctionnalité de portail standard de type 2 : les meilleures pratiques en matière de configuration sont prises en charge uniquement pour Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways et Cisco Session Management Edition.

1.1.2b. Type 2 – Fonctionnalités d'expert-conseil et d'analyses hébergées standard : étapes importantes du cycle de vie du matériel.

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Systèmes informatiques
- Commutation de centres de données
- Réseau de stockage
- Sécurité de réseau
- Politique de sécurité et accès
- Communications unifiées

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données

Livrables

- Étapes importantes du cycle de vie du matériel de type 2

Restrictions

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- Les étapes importantes du cycle de vie du matériel de type 2 sont uniquement prises en charge pour Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD) et le moteur ISE (Identity Services Engine).

** Propre aux communications unifiées*

- Les étapes importantes du cycle de vie du matériel de type 2 ne sont prises en charge que pour Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateway et Cisco Session Management Edition pour des points d'extrémité déterminés.

1.1.2c. Type 2 – Fonctionnalités d'expert-conseil et d'analyses hébergées standard : analyse diagnostique

Technologies prises en charge

- Routage et commutation
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Infrastructure centrée sur les applications
- Sécurité de réseau
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- Communications unifiées

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données

Autres responsabilités

** Propre au routage et à la commutation, et à la commutation de centre de données*

- Indique les facteurs de blocage de périphérique pour les périphériques les plus touchés.

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

- Les observations diagnostiques suivantes sont fournies :
- Les événements, les pannes, les vérifications, les déplacements de point de terminaison et l'utilisation de la capacité.

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

- Les ensembles d'observations diagnostiques suivants sont fournis :

Pour l'ensemble de base :

- Résumé de l'intégrité du réseau pour les flux d'appels GTPC, les IRC et les procédures comme Attach, la création de PDP ou de porteur, la mise à jour de zone de routage ou de suivi, les appels, les requêtes de service et les requêtes de transfert, s'il y a lieu.
- Résumé de l'utilisation de l'UCT et de la mémoire des ressources.
- Tendances de sessions et de débit, utilisation des ressources.
- Paquets perdus à cause de la congestion, retransmissions, délais d'attente pour toutes les interfaces et tous les noms de point d'accès (APN).
- Résumé des sessions, des transactions, des flux d'appels de Diameter au niveau des interfaces (s'il y a lieu).
- Résumé des journaux système des X premiers événements, des tendances des événements critiques, des erreurs et des informations de journaux système.

Livrables

- Analyse diagnostique de type 2

Restrictions

** Propre à la sécurité du réseau*

- L'analyse diagnostique de type 2 est prise en charge uniquement pour Cisco Adaptive Security Appliance (ASA).

** Propre aux communications unifiées*

- L'analyse diagnostique de type 2 est prise en charge uniquement pour Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways et Cisco Session Management Edition et pour des points d'extrémité déterminés.

1.1.2d. Type 2– Fonctionnalités d'expert-conseil et d'analyses hébergées standard : avis de problèmes constatés

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès
- Communications unifiées

Solutions prises en charge

- Virtual Packet Core
  - Systèmes informatiques
  - Commutation de centres de données
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Politique de sécurité et accès

Produits livrables

- Analyse d'avis de problèmes constatés et recommandations, type 2

Restrictions

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- Les avis de problèmes constatés de type 2 ne sont pris en charge que pour Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defence (FTD) et le moteur ISE (Identity services Engine).

** Propre aux communications unifiées*

- Les avis de problèmes constatés de type 2 sont pris en charge uniquement pour Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways et Cisco Session Management Edition et pour des points d'extrémité déterminés.

1.1.2e. Rapport de vérification de type 2

Technologies prises en charge

- Routage et commutation
- Systèmes informatiques
- Commutation de centres de données
- Réseau de stockage
- Sécurité de réseau
- Politique de sécurité et accès
- Communications unifiées
- Réseau central de transmission par paquets
- Politique de mobilité et accès

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données

Responsabilités de Cisco

- Analyser les informations, ce qui peut comprendre, sans toutefois s'y limiter, ce qui suit :
- Stabilité, performances et recommandations de réglages.
- Analyse de l'utilisation des ressources aux fins de planification.
- Recommandations liées aux domaines nécessitant une analyse complémentaire, comme l'architecture et la conception ou l'alignement sur les politiques et les normes.

** Propre aux communications unifiées*

- Le rapport de vérification de type 2 est fourni une fois par trimestre, jusqu'à quatre rapports par an.

Responsabilités exclues

** Propre aux systèmes informatiques, à la commutation de centre de données, aux systèmes informatiques virtuels de transmission par paquets et à la commutation de centre de données.*

- L'analyse et le rapport de vérification n'abordent pas ce qui suit :
- Stabilité, performances et recommandations de réglages.
- Analyse de l'utilisation des ressources aux fins de planification.

Livrables

- Rapport de vérification de type 2

Restrictions

** Propre à la commutation de centre de données*

- Un (1) rapport de vérification de type 1 limité aux commutateurs de la série Nexus par instance de centre de données.

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- Le rapport de vérification de type 2 est limité à ce qui suit :
- Jusqu'à un (1) ensemble de solutions ou un (1) système complexe (par exemple, la plateforme de services d'identité [ISE], le système de contrôle d'accès sécurisé [ACS] de Cisco ou les déploiements 802.1x).
- Jusqu'à vingt (20) périphériques.

** Propre aux communications unifiées*

- Les avis de problèmes constatés de type 2 sont pris en charge uniquement pour Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways et des points d'extrémité déterminés.

1.1.2f. Type 2 : Fonctionnalités d'expert-conseil et d'analyses hébergées en option : soutien par des tiers

Le soutien par des tiers aide le Client grâce à une vue d'inventaire des plateformes tierces et des systèmes d'exploitation pris en charge par Cisco par l'entremise des analyses hébergées en nuage de Cisco.

Restrictions

- La prise en charge de SNMP MIB-2 par le fournisseur de l'appareil tiers est nécessaire pour colliger les données d'inventaire. L'exactitude et l'exhaustivité des données collectées par Cisco dépendent de l'assistance du fournisseur tiers pour SNMP MIB-2.

- Cisco n'est pas responsable de l'adéquation et de la fiabilité de toutes les informations collectées ou fournies par un ou plusieurs appareils, site Web ou toute autre source d'informations d'un fournisseur tiers.
- Cisco n'est pas responsable de la disponibilité, des performances, de la sécurité ou de la fiabilité des périphériques tiers pour lesquels le client demande à Cisco de collecter des données à des fins de production de rapports.

Technologies prises en charge

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

Plateformes et systèmes d'exploitation tiers pris en charge

Société	Systèmes d'exploitation	Plateformes prises en charge
Adtran	AOS	Adtran – NetVanta 3200
Alcatel	SROS	Routeurs de services Alcatel 7750
Alteon	AlteonOS	Commutateur d'application Alteon 2208
Arista	EOS	Commutateurs Arista 7050
Aruba	Aruba OS	Contrôleur de réseau sans fil Aruba
BoSS	BoSS	BS470-48T, ERS4550T, BS551048T
Checkpoint	IPSO GAIA	Mur pare-feu Checkpoint IPxxx
Extreme	EXOS	Commutateurs Extreme Summit
Forti	FortiOS	Forti – Analyzer 60D, Manager
F5	TMOS	F5 – VIPRION de la gamme C2400, BIG IP
Huawei	VRP	Commutateurs Huawei S3328
Infoblox	NIOS	Infoblox 1552-A
Juniper	JunOS ScreenOS	Juniper de la gamme M, SRX240 Services Gateway, EX2200 Pare-feu Juniper NetScreen SSG5
NetScaler	NetScalerOS	Citrix NetScaler, NetScaler SDX

Responsabilités de Cisco

- Fournir un inventaire des périphériques tiers du client par l'entremise des analyses hébergées, ce qui peut comprendre les éléments suivants :
  - Le châssis, l'adresse IP, le type d'appareil, le nom de l'appareil, les versions du logiciel/du micrologiciel

Livrables

- Rapport d'inventaire tiers de type 2, en option.

Responsabilités du Client

- Le client est responsable de la résolution des problèmes de données avec les données collectées par Cisco auprès du fournisseur d'appareils tiers.
- Pour que Cisco puisse fournir ce service, le client est responsable de fournir l'expertise sur les plateformes d'un fournisseur tiers, dont notamment :
  - Nomenclature du matériel
  - Fonctionnalités et commandes de configuration

  - Versions du logiciel
  - Méthodes d'accès et identifiants
- Le client doit maintenir et surveiller la disponibilité, les performances, la sécurité et la fiabilité des appareils tiers pris en charge par la méthode de collecte de données de Cisco; il doit en outre s'assurer que les configurations et les versions logicielles sur les appareils tiers déployés dans l'environnement du client soient adéquates ou qu'elles ne contiennent pas de défauts qui sont affectés par les méthodes de collecte de données de Cisco.
- Le client doit contacter le représentant commercial Cisco pour au sujet d'autres plateformes et fonctionnalités tierces qui ne sont pas présentement répertoriées.

1.1.3. Observations sur la plateforme de type 3 – Rapports produits par l'outil d'analyses et d'observations sur le site de Cisco

Le service Observations sur la plateforme de type 3 fournit les fonctionnalités et le rapport suivants :

- Rapport sur les meilleures pratiques en matière de configuration de type 3
- Rapport sur les étapes importantes du cycle de vie du matériel de type 3
- Conseil de sécurité du produit de type 3, rapport d'évaluation de l'impact client
- Rapport d'analyse diagnostique de type 3
- Rapport de vérification de type 3

1.1.3a. Rapport sur les meilleures pratiques en matière de configuration de type 3

Technologies prises en charge

- Routage et commutation
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Accès défini par logiciel
  - Routage et commutation
  - Politique de sécurité et accès
- Réseau central virtuel de transmission par paquets
  - Réseau central de transmission par paquets

Produits livrables

- Rapport sur les meilleures pratiques en matière de configuration de type 3

Restrictions

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- Le rapport des pratiques de configuration de type 3 est uniquement pris en charge pour Cisco Adaptive Security Appliance (ASA).

** Propre au réseau central virtuel de transmission par paquets*

- Le rapport sur les bonnes pratiques en matière de configuration de type 3 est uniquement pris en charge pour la solution Cisco Ultra-M.
- Les commutateurs Cisco Nexus et Catalyst® qui font partie de la solution Ultra-M de Cisco sont pris en charge.

1.1.3b. Rapport sur les étapes importantes du cycle de vie du matériel de type 3

Technologies prises en charge

- Routage et commutation
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Accès défini par logiciel
  - Routage et commutation
  - Politique de sécurité et accès

Produits livrables

- Rapport sur les étapes importantes du cycle de vie du matériel de type 3

Restrictions

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- Le rapport sur les étapes importantes du cycle de vie du matériel de type 3 est uniquement pris en charge pour Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD) et le moteur ISE (Identity Services Engine).

1.1.3c. Avis de problèmes constatés de type 3

Technologies prises en charge

- Routage et commutation
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Accès défini par logiciel
  - Routage et commutation
  - Politique de sécurité et accès

Produits livrables

- Rapport d'analyse d'avis de problème constaté et de recommandations de type 3

Restrictions

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- L'analyse et les recommandations relatives aux avis de problèmes constatés de type 3 sont uniquement prises en charge pour Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD) et le moteur ISE (Identity Services Engine).

1.1.3d. Rapport d'analyse diagnostique de type 3

Solutions prises en charge

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

Livrables

- Rapport d'analyse diagnostique de type 3

Restrictions

** Propre au réseau central virtuel de transmission par paquets*

- Le rapport d'analyse de diagnostic de type 3 est uniquement pris en charge pour la solution Ultra-M de Cisco.
- Les commutateurs Cisco Nexus et Catalyst qui font partie de la solution Ultra-M de Cisco sont pris en charge.

1.1.3e. Rapport de vérification de type 3

Solutions prises en charge

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

Livrables

- Rapport de vérification de type 3

Restrictions

** Propre au réseau central virtuel de transmission par paquets*

- Le rapport de vérification de type 3 est uniquement pris en charge pour la solution Ultra-M de Cisco.
- Les commutateurs Cisco Nexus et Catalyst qui font partie de la solution Ultra-M de Cisco sont pris en charge.

1.2. Gestion du cycle de vie du logiciel (Software Lifecycle management ou SLM)

Le service de gestion du cycle de vie du logiciel aide le client à préparer et à planifier les décisions à propos des versions logicielles à venir comme les fonctionnalités, la compatibilité avec des logiciels tiers et la stabilité des versions en s'alignant sur les objectifs de versions logicielles à avenir du client. Il analyse les pratiques actuelles du client en rapport avec la création et la gestion de normes relatives aux versions des logiciels dans le but d'identifier les risques et de formuler des recommandations afin d'éviter les problèmes potentiels.

Restrictions générales

Les restrictions suivantes s'appliquent spécifiquement aux bogues relevés dans les mises à jour de maintenance logicielle (SMU) de production des livrables de la gestion du cycle de vie du logiciel décrits ci-dessous et à la discrétion de Cisco en ce qui concerne les demandes et la livraison de SMU de production :

- Les mises à jour de maintenance logicielle de production des versions de maintenance prises en charge sont fournies sur demande du client pour les problèmes qui perturbent le service dans l'environnement de production ou au cours de la validation de version de maintenance, et pour lesquels il n'y a aucune solution de contournement possible.
- Les bogues logiciels relevés à l'aide de recommandations logicielles ou des outils de recherche de bogues ne peuvent justifier une demande de SMU de production.
- Cisco examine les bogues logiciels qui touchent les versions de maintenance prises en charge et fait des demandes proactives de SMU de production lorsque Cisco le juge nécessaire.
- Cisco se réserve le droit de garder un contrôle strict sur la livraison des SMU de production.

Exclusion

** Propre au réseau sans fil*

- Le réseau Cisco Meraki n'est pas pris en charge.

** Propre aux systèmes informatiques*

- Cisco HyperFlex n'est pas pris en charge.

** Propre à la commutation de centre de données*

- La plateforme de contrôle des applications (Application Control Engine ou ACE) de Cisco n'est pas prise en charge.

1.2.1. SLM, Type 1 – Rapports générés manuellement ou par l'outil de collecte de données de Cisco

La gestion du cycle de vie du logiciel de type 1 est composée des trois (3) domaines suivants :

- Élaboration de procédure et de processus de gestion logicielle de type 1
- Normes et conformité des versions des logiciels de type 1
- Observations et gestion des risques des logiciels de type 1

1.2.1a. Élaboration de procédure et de processus de gestion logicielle de type 1

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données
- Communications unifiées
- Collaboration vidéo
- Service à la clientèle
- Réunions et messagerie infonuagiques
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- 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
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau
- 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
- WAN 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
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Responsabilités de Cisco

- Collaborer avec le client à la production du document sur la procédure et le processus de gestion de logiciel, qui peut comprendre ce qui suit :
  - Stratégie logicielle, processus, procédure et documents liés aux choix de logiciel.
  - Exigences et objectifs de fonctionnalités.
  - Planification des mises à niveau et déclencheurs de migration, comme les avis, les reports, les fins de commercialisation et les fins de vie de logiciels ainsi que les avis de problème constaté.

Livrables

- Document sur la procédure et le processus de gestion de logiciel de type 1

1.2.1b. Normes et conformité des versions des logiciels de type 1

Le service des normes et de la conformité des versions de logiciels est composé des deux (2) rapports décrits ci-dessous :

- Rapport des normes de version et d'analyse de logiciels de type 1
- Rapport du suivi de la conformité des logiciels de type 1

b-1. Rapport des normes de version et d'analyse de logiciels de type 1.

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Systèmes informatiques
- Commutation de centres de données
- Réseau de stockage
- Infrastructure centrée sur les applications
- Orchestration et automatisation de centre de données
- Communications unifiées
- Service à la clientèle
- Sécurité du nuage
- Collaboration vidéo
- Réunions et messagerie infonuagiques
- Sécurité de réseau
- Politique de sécurité et accès
- Menace avancée
- 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

- WAN défini par logiciel
  - Routage et commutation
- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données
  - Réseau central de transmission par paquets

Responsabilités de Cisco

- Élaborer le rapport des normes de version et d'analyse de logiciels, qui peut comprendre ce qui suit :
  - Recommandations générales de logiciels à tester et à considérer par le client.
  - Description des nouvelles fonctionnalités logicielles et compatibilités matérielles.
  - Bogues logiciels non résolus qui pourraient comporter un risque pour le client et solutions de contournement, si possible.
  - Analyse de mise à niveau de fonctionnalité logicielle, en fonction des données recueillies et de l'analyse des résultats des versions de logiciels relevées, par rapport aux exigences de fonctionnalités logicielles actuelles et futures du client.

Livrables

- Rapport des normes de version et d'analyse de logiciels de type 1.
- Remarque : Une (1) unité de ces livrables ne comprend qu'une (1) plateforme et sa version logicielle.

Restrictions

- ** Propre à l'orchestration et à l'automatisation de centre de données*
- Le rapport des normes de version et d'analyse de logiciels de type 1 n'est pris en charge que pour Cisco CloudCenter.

b-2. Rapport du suivi de la conformité des logiciels de type 1

Technologies prises en charge

- Réseau optique
- Réseau sans fil
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Infrastructure centrée sur les applications
- Orchestration et automatisation de centre de données
- Collaboration vidéo
- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée
- Accès par câble de prochaine génération
- Infrastructure vidéo des fournisseurs de services
- Calcul en périphérie de réseau de l'IDO et informatique géodistribuée

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données

Responsabilités de Cisco

- Établir une base de référence des normes et de la conformité de versions des normes de versions déployées du client par rapport aux normes de versions logicielles recommandées par Cisco.

Restrictions

- ** Propre à l'orchestration et à l'automatisation de centre de données*
- Le rapport du suivi de la conformité des logiciels de type 1 n'est pris en charge que pour Cisco CloudCenter.

Livrables

- Rapport du suivi de la conformité des logiciels de type 1

1.2.1c. Observations et gestion des risques des logiciels de type 1

Le service d'observations et gestion des risques logiciels est composé des deux (2) rapports décrits ci-dessous :

- Avis de sécurité produit de type 1 évaluation de l'impact client
- Étapes importantes du cycle de vie du logiciel de type 1

Type 1 – évaluation de l'impact du client sur la sécurité des produits

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
- 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
- Infrastructure vidéo des fournisseurs de services
- Accès par câble de prochaine génération

Solutions prises en charge

- WAN défini par logiciel
  - Routage et commutation
- Virtual Packet Core
  - Systèmes informatiques
  - Commutation de centres de données
  - 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
- 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
- Managed Service Accelerator (MSX)
  - Routage et commutation
  - Gestion et orchestration de réseau
  - Systèmes informatiques

Responsabilités de Cisco

- Le cas échéant, procéder à l'évaluation de l'impact client pour un avis de sécurité de produit Cisco publié :
- Dresser la liste des périphériques touchés ou potentiellement touchés.
- Fournir une analyse et des recommandations pour gérer les effets possibles de l'avis de sécurité de produit Cisco sur la solution déployée actuelle du Client.
- Formuler des recommandations de version de logiciel comportant un correctif pour l'avis de sécurité de produit Cisco.

Autres responsabilités

** Propre au réseau central virtuel de transmission par paquets*

- Ce livrable prend en charge les composants logiciels du système d'exploitation Red Hat et de Red Hat Openstack.

Livrables

- Avis de sécurité du produit de type 1, rapport d'évaluation de l'impact client

Étapes importantes du cycle de vie du logiciel de type 1

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
- 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
- Infrastructure vidéo des fournisseurs de services
- Accès par câble de prochaine génération

Solutions prises en charge

- WAN défini par logiciel
  - Routage et commutation
- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données

Responsabilités de Cisco

- Effectuer les actions suivantes, s'il y a lieu :
- Relever les périphériques touchés par le report, la fin de commercialisation et la fin de vie du logiciel qui sont applicables aux normes logicielles déployées du client et qui pourraient déclencher une migration.

Livrables

- Rapport sur les étapes importantes du cycle de vie du logiciel de type 1

1.2.2. SLM, Type 2 – Fonctionnalités d'expert-conseil et d'analyses hébergées dans le nuage de Cisco

Exclusions

** Propre aux systèmes informatiques*

- Les serveurs UCS de série C qui ne sont pas connectés à la trame ne sont pas pris en charge par les livrables du service de gestion du cycle de vie du logiciel de type 2.

Restrictions

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- Les fonctionnalités de gestion du cycle de vie du logiciel de type 2 sont prises en charge uniquement pour Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD) et le moteur ISE (Identity services Engine).
- ISE n'est pas pris en charge pour l'analyse de logiciel de type 2 et les normes de version, ni pour les tendances d'adoption de logiciels de type 2.

** Propre aux communications unifiées*

- Les fonctionnalités de gestion du cycle de vie du logiciel de type 2 sont prises en charge uniquement pour Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateway et Cisco Session Management Edition.

Le service de gestion du cycle de vie du logiciel de type 2 est composé des trois (3) domaines suivants :

- Élaboration de procédure et de processus de gestion du logiciel de type 2
- Normes et conformité des versions des logiciels de type 2
- Observations et gestion des risques des logiciels de type 2

1.2.2a. Élaboration de procédure et de processus de gestion logicielle de type 2

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Communications unifiées
- Sécurité de réseau
- Politique de sécurité et accès

Responsabilités de Cisco

- Collaborer avec le client à la production du document sur la procédure et le processus de gestion de logiciel, qui peut comprendre ce qui suit :
  - Stratégie logicielle, processus, procédure et documents liés aux choix de logiciel.
  - Exigences et objectifs de fonctionnalités.
  - Planification des mises à niveau et déclencheurs de migration, comme les avis, les reports, les fins de commercialisation et les fins de vie de logiciels ainsi que les avis de problème constaté.

Livrables

- Document sur la procédure et le processus de gestion des logiciels de type 2

Responsabilités du client

- Communiquer les pratiques actuelles et la documentation relative à l'établissement, la conformité et la gestion des normes sur les versions de logiciels et les déclencheurs de migration logicielle.

1.2.2b. Normes et conformité des versions des logiciels de type 2

Le service des normes et de la conformité des versions des logiciels de type 2 est composé des fonctionnalités et du rapport décrits ci-dessous :

- Normes de version et d'analyse de logiciels de type 2
- Type 2 Software Track Conformance
- Tendances de l'adoption de logiciels de type 2

Type 2 – Normes de version et d'analyses de logiciels

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Réseau de stockage
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès
- Communications unifiées
- Réseau central de transmission par paquets
- Politique de mobilité et accès

Solutions prises en charge

- Virtual Packet Core
  - Réseau central de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Politique de sécurité et accès

Remarque : Les plateformes qui ne sont pas prises en charge par les analyses en nuage hébergées sont prises en charge par le rapport des normes de versions et d'analyses logicielles.

Responsabilités de Cisco

- L'analyse des suivis et des normes de version logicielle déployées spécifiques au client.
- Recommandations générales de logiciels à tester et à considérer par le client.
- La description des nouvelles fonctionnalités logicielles.
- Identifier les bogues logiciels non résolus qui pourraient comporter un risque pour le client et identifier les solutions de contournement, si possible.
- L'analyse de mise à niveau de fonctionnalité logicielle des versions spécifiées par rapport aux exigences en fonctionnalités logicielles actuelles et futures du client.

Livrables

- Rapport des normes de versions et d'analyses de logiciels de type 2
- Une (1) quantité de ces livrables n'inclut qu'une (1) plateforme et sa version logicielle.

Restrictions

** Spécifiques aux réseaux sans fil, aux systèmes informatiques, aux réseaux de stockage, à la commutation de centres de données et aux systèmes informatiques virtuels de transmission par paquets*

- Normes de version et d'analyse de logiciels fournies par un rapport.

Type 2 – Conformité pour le suivi des logiciels

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Communications unifiées
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Politique de sécurité et accès

Responsabilités de Cisco

- Aider le client à créer des groupes de versions de logiciels qui feront l'objet d'un suivi.
- Établir une base de référence des normes et de la conformité de versions des normes de versions déployées du client par rapport aux normes de versions logicielles recommandées par Cisco.

Livrables

- Type 2 – Conformité pour le suivi des logiciels

Restrictions

** Propre au réseau sans fil*

- La fonctionnalité de suivi de la conformité des logiciels de type 2 n'est pas disponible pour les périphériques de point d'accès de réseau local sans fil Cisco.

Type 2 – Fonctionnalité en option : Tendances pour l'adoption des logiciels

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Sécurité de réseau
- Politique de sécurité et accès

Responsabilités de Cisco

- Tendances de mise à niveau de versions de logiciels observées dans la base d'installations du client.

Livrables

- Type 2 – Fonctionnalité en option : Tendances pour l'adoption des logiciels

1.2.2c. Observations et gestion des risques des logiciels de type

Le service d'observations et gestion des risques logiciels de type 2 est composé des fonctionnalités décrites ci-dessous :

- Avis de sécurité produit de type 2, évaluation de l'impact client
- Étapes importantes du cycle de vie du logiciel de type 2
- Avis de bogues critiques de type 2
- Avis de mise à jour de maintenance logicielle de type 2
- Fonctionnalité en option de type 2 : suivi de bogues de versions de logiciels

c-1. Avis de sécurité produit de type 2, évaluation de l'impact client

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Réseau de stockage
- Communications unifiées
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Virtual Packet Core
  - Systèmes informatiques
  - Commutation de centres de données
- Accès défini par logiciel
  - Routage et commutation
  - Réseau sans fil
  - Politique de sécurité et accès

Responsabilités de Cisco

- Le cas échéant, procéder à l'évaluation de l'impact client pour un avis de sécurité de produit Cisco publié :
  - Dresser la liste des périphériques touchés ou potentiellement touchés.
- Fournir une analyse et des recommandations pour gérer les effets possibles de l'avis de sécurité de produit Cisco sur la solution déployée actuelle du Client.
- Formuler des recommandations de version de logiciel comportant un correctif pour l'avis de sécurité de produit Cisco.

Livrables

- Avis de sécurité produit de type 2, évaluation de l'impact client

Étapes importantes du cycle de vie du logiciel de type 2

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Réseau sans fil
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Réseau central virtuel de transmission par paquets
  - Systèmes informatiques
  - Commutation de centres de données

Responsabilités de Cisco

- Relever les périphériques touchés par le report, la fin de commercialisation et la fin de vie du logiciel qui sont applicables aux normes logicielles déployées du client et qui pourraient déclencher une migration.

Livrables

- Étapes importantes du cycle de vie du logiciel de type 2

Type 2 – Fonctionnalité en option d'avis de bogues critiques

Technologies prises en charge

- Routage et commutation
- Sécurité de réseau
- Politique de sécurité et accès
- Communications unifiées
- Réseau central de transmission par paquets
- Politique de mobilité et accès

Solutions prises en charge

- Accès défini par logiciel
  - Routage et commutation
  - Politique de sécurité et accès
- Réseau central virtuel de transmission par paquets
  - Réseau central de transmission par paquets

Responsabilités de Cisco

- Fournir des avis de bogues critiques qui notifient le client de la découverte, du changement d'état ou de la résolution de bogues critiques des versions de logiciel de préférence suivies par le client.

Livrables

- Type 2 – Fonctionnalité en option d'avis de bogues critiques
- Une (1) quantité de ces livrables n'inclut qu'une (1) plateforme et sa version logicielle.

Restrictions

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

- Fonctionnalité de type 2 : la notification de bogues critiques est prise en charge uniquement pour Cisco Ultra-M avec Cisco Virtualized Infrastructure Manager.

Type 2 – Fonctionnalité en option d'avis de mise à jour de maintenance logicielle

Technologies prises en charge

- Routage et commutation

Responsabilités de Cisco

- Fournir des avis de mises à jour de maintenance logicielle qui notifient le client de la disponibilité d'un correctif ou d'une mise à jour de maintenance d'un bogue, d'une fonctionnalité ou d'une version de logiciel spécifique.

Livrables

- Type 2 – Fonctionnalité en option d'avis de mise à jour de maintenance logicielle
- Une (1) quantité de ces livrables n'inclut qu'une (1) plateforme et sa version logicielle.

Type 2 – Fonctionnalité en option suivi de bogues de versions de logiciels

Technologies prises en charge

- Routage et commutation
- Sécurité de réseau
- Politique de sécurité et accès
- Communications unifiées
- Réseau central de transmission par paquets
- Politique de mobilité et accès

Solutions prises en charge

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

Responsabilités de Cisco

- Fournir périodiquement des observations et un suivi des bogues critiques de normes de versions de logiciels spécifiques.

Livrables

- Fonctionnalité en option de type 2 : suivi de bogues de versions de logiciels

1.2.3. SLM type 3 – Rapports produits par l'outil d'analyses et d'observations sur le site de Cisco

Restrictions

** Propre à la sécurité du réseau, à la politique de sécurité et à l'accès*

- Les rapports de gestion du cycle de vie du logiciel de type 3 sont pris en charge uniquement pour Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD) et le moteur ISE (Identity services Engine).

Le service de gestion du cycle de vie du logiciel de type 3 est fourni par l'outil d'analyses et d'observation sur place de Cisco et est composé des trois (3) domaines suivants :

- Élaboration de procédure et de processus de gestion des logiciels de type 3
- Normes et conformité des versions des logiciels de type 3
- Observations et gestion des risques des logiciels de type 3

1.2.3a. Élaboration de procédure et de processus de gestion logicielle de type 3

Technologies prises en charge

- Routage et commutation
- Sécurité de réseau
- Politique de sécurité et accès

Responsabilités de Cisco

- Collaborer avec le client à la production du document sur la procédure et le processus de gestion logicielle, qui peut comprendre ce qui suit :
  - Stratégie logicielle, processus, procédure et documents liés aux choix de logiciel.
  - Exigences et objectifs de fonctionnalités.
  - Planification des mises à niveau et déclencheurs de migration, comme les avis, les reports, les fins de commercialisation et les fins de vie de logiciels ainsi que les avis de problème constaté.

Livrables

- Document sur la procédure et le processus de gestion des logiciels de type 3

1.2.3b. Normes et conformité des versions des logiciels de type 3

Le service des normes et de la conformité des versions de logiciels de type 3 est composé des rapports décrits ci-dessous :

- Rapport du suivi de la conformité de logiciels de type 3
- Rapport des normes de version et d'analyse de logiciels de type 3

Technologies prises en charge

- Routage et commutation
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Accès défini par logiciel
  - Routage et commutation
  - Politique de sécurité et accès

Responsabilités de Cisco

- Établir une base de référence des normes et de la conformité de versions des normes de versions déployées du client par rapport aux normes de versions logicielles recommandées par Cisco.
- Élaborer le rapport des normes de version et d'analyse des logiciels, qui peut inclure :
  - Recommandations générales de logiciels à tester et à considérer par le client.
  - Description des nouvelles fonctionnalités logicielles et compatibilités matérielles.

- Bogues logiciels non résolus qui pourraient comporter un risque pour le client et solutions de contournement, si possible.
- Analyse de mise à niveau de fonctionnalité logicielle, en fonction des données recueillies et de l'analyse des résultats des versions de logiciels relevées, par rapport aux exigences de fonctionnalités logicielles actuelles et futures du client.

Livrables

- Rapport du suivi de la conformité de logiciels de type 3
- Rapport des normes de version et d'analyse de logiciels de type 3
- Remarque : Un (1) rapport des normes de version et d'analyse des logiciels de type 3 ne comprend qu'une (1) plateforme et sa version logicielle.

1.2.3c. Observations et gestion des risques des logiciels de type 3

Le service d'observations et gestion des risques logiciels de type 3 est composé des rapports décrits ci-dessous :

- Conseil de sécurité du produit de type 3, rapport d'évaluation de l'impact client
- Étapes importantes du cycle de vie du logiciel de type 3

Technologies prises en charge

- Routage et commutation
- Commutation de centres de données
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Accès défini par logiciel
  - Routage et commutation
  - Politique de sécurité et accès

Responsabilités de Cisco

- Le cas échéant, procéder à l'évaluation de l'impact client pour un avis de sécurité de produit Cisco publié :
  - Dresser la liste des périphériques touchés ou potentiellement touchés.
- Fournir une analyse et des recommandations pour gérer les effets possibles de l'avis de sécurité de produit Cisco sur la solution déployée actuelle du Client.
- Formuler des recommandations de version de logiciel comportant un correctif pour l'avis de sécurité de produit Cisco.
- Évaluer les périphériques touchés par le report de logiciels, les logiciels en fin de commercialisation et les logiciels en fin de vie qui sont applicables aux normes logicielles déployées du client et qui pourraient déclencher une migration.

Livrables

- Conseil de sécurité du produit de type 3, rapport d'évaluation de l'impact client
- Étapes importantes du cycle de vie du logiciel de type 3

1.3. Observations sur la disponibilité

Les informations sur la disponibilité prévoient les problèmes liés aux périphériques grâce à des algorithmes automatisés en temps réel et basés sur des facteurs, des résultats corrélés et des recommandations pour résoudre les problèmes afin de profiter de la disponibilité.

Le service d'informations sur la disponibilité se compose des caractéristiques décrites ci-dessous :

- Gestion automatisée des erreurs
- Facteur de stabilité de l'appareil

1.3.1. Gestion automatisée des défaillances

Le service de gestion automatisée des erreurs analyse les journaux système des périphériques à l'aide des règles et des algorithmes de Cisco pour détecter les erreurs de logiciel, de matériel et de configuration du réseau et fournir au client des informations pour l'aider à résoudre le problème. Les tendances historiques et les algorithmes prédictives peuvent identifier les pannes imminentes. La surveillance des journaux se fait presque en temps réel, ce qui permet de détecter des séquences signalant si une erreur est survenue ou est sur le point d'arriver. Lors de la détection, le système peut collecter les données du périphérique nécessaires pour résoudre le problème, ce qui peut mener à l'émission d'un avis ou à l'ouverture d'un dossier auprès du service d'assistance de Cisco.

Technologies prises en charge

- Routage et commutation

Responsabilités de Cisco

- Expliquer le déploiement du système et les exigences opérationnelles.
- Configurer et déployer la machine virtuelle de gestion automatisée des erreurs sur le réseau du client pour traiter les journaux système et faire des demandes d'assistance.
- Informer le client d'un ou de plusieurs des éléments suivants lorsque la détection des défaillances s'est produite :
  - Notification des défaillances détectées
  - Toutes les données collectées
  - Étapes de la résolution recommandées
  - Demandes d'assistance
- Mettre à jour les données des périphériques gérés sur le serveur de gestion automatisée des erreurs en fonction des renseignements fournis par le client (aussi souvent qu'une fois par semaine).

Livrables

- Rapport trimestriel sur les erreurs détectées et l'état des demandes de service

Responsabilités du client

- Fournir le déploiement et l'environnement d'exécution précisé pour la machine virtuelle du serveur de gestion automatisée des erreurs de Cisco.
- Fournir au serveur de gestion automatisée des erreurs de Cisco un accès de communication avec les périphériques en service afin de permettre la collecte des données de configuration et d'état.
- Fournir au serveur de gestion automatisée des erreurs de Cisco un accès de communication chiffrée aux serveurs hébergés par Cisco, et ce, aux fins de la gestion des demandes d'assistance et de mises à jour logicielles du serveur de gestion automatisée des erreurs.
- Fournir à Cisco la liste de tous les périphériques réseau en service et leurs identifiants d'accès, et mettre rapidement à jour cette liste en cas de modification; ces données peuvent être fournies par l'intermédiaire de l'API au périphérique Cisco Network Collector (s'il y a lieu) ou envoyées au personnel de Cisco dans un enregistrement électronique formaté.
- Configurer les appareils en service pour qu'ils envoient des messages syslog à un serveur syslog. Configurer le serveur Syslog pour transmettre les événements Syslog à la machine virtuelle de gestion des erreurs automatisée.
- Fournir un accès au serveur de messagerie pour le serveur de gestion automatisée des erreurs. Fournir les adresses pour les notifications transmises par courrier électronique.
- Intégrer le système de gestion des alarmes à la gestion automatisée des erreurs de Cisco à l'aide de l'API Rest, si vous le souhaitez; Cisco n'effectuera pas cette tâche.

1.3.2. Facteurs de stabilité des appareils

Les facteurs de stabilité des appareils collectent des informations en temps réel et aident le client à fournir des recommandations pour limiter les facteurs qui affectent la santé et la stabilité des périphériques les plus touchés.

Technologies prises en charge

- Systèmes informatiques UCS

Responsabilités de Cisco

- Le facteur de stabilité de l'appareil collecte des informations en temps quasi réel et fournit des recommandations pour réduire le risque d'atteinte à la stabilité pour les périphériques les plus touchés.
- Les observations suivantes sont fournies :
  - État général des pratiques exemplaires en matière d'infrastructure informatique
  - Définition dynamique, hiérarchisation et agrégation des scores et des tendances de la stabilité au niveau des composants
  - Définition des anomalies et composants touchés.
  - Résultats corrélés et recommandations visant à améliorer la stabilité de l'infrastructure.

Livrables

- Compilation des données réunies au moyen des facteurs de stabilité de l'appareil et examens périodique par l'expert-conseil de Cisco.

Responsabilités du client

- Indiquer un environnement de déploiement et d'exécution spécifique pour le logiciel du facteur de stabilité du périphérique. Les moteurs de collecte de données des facteurs de stabilité de l'appareil sont distincts du CSPC.
- Fournir à Cisco la liste des appareils et les informations d'accès pour tous les périphériques pris en charge par le logiciel de facteur de stabilité des périphériques, et mettre à jour cette liste rapidement lorsque des modifications sont apportées à cette liste.

1.4. Évaluation des technologies

Le service d'évaluations des technologies définit les lacunes et aide le Client en formulant des recommandations pour l'optimisation de la capacité, de la fiabilité, de la performance générale ou de la sécurité des technologies de Cisco.

1.4.1. Évaluation de la résilience

Le service d'évaluation de la résilience évalue la résilience et la disponibilité pour permettre un réseau et des services d'application sécuritaires, fiables et de grande qualité. L'évaluation est axée sur les améliorations de la résilience et de la disponibilité à l'architecture et aux opérations des technologies Cisco.

Technologies prises en charge

- Routage et commutation
- Réseau optique
- Commutation de centres de données
- Infrastructure vidéo des fournisseurs de services

Solutions prises en charge

- WAN défini par logiciel
  - Routage et commutation

Renseignements supplémentaires à recueillir

- Base de référence de la disponibilité actuelle et effets des interruptions de service.

Responsabilités de Cisco

- Produire des recommandations d'améliorations axées principalement sur la disponibilité et la résilience; les améliorations peuvent notamment comprendre ce qui suit :
  - Modifications de la conception et de la configuration.
  - Fonctionnalités de surveillance.
- Fournir une feuille de route et convenir d'une priorité pour l'amélioration de la résilience.

Livrables

- Rapport d'évaluation de la résilience

Restrictions

Les restrictions suivantes sont propres à la technologie indiquée.

- **Routage et commutation :**
  - L'évaluation de la résilience couvre uniquement les périphériques de routage et de commutation Cisco (jusqu'à 5 000 périphériques Cisco).
  - Les cycles de vie du matériel et des logiciels Wi-Fi Cisco, ainsi que les meilleures pratiques de sécurité et de gérabilité sont incluses dans l'analyse. Les configurations particulières de Wi-Fi et les études de radiofréquences (RF) ne sont pas couvertes par l'évaluation de la résilience du routage et de la commutation; ces activités sont incluses dans les livrables liés à l'évaluation des radiofréquences du réseau local sans fil.
  - Les cycles de vie du matériel et du logiciel de pare-feu Cisco et d'équilibreur de charge sont inclus dans l'analyse, mais pas les règles de pare-feu et d'équilibrage de charge.
  - Les configurations de VoIP sont hors du champ d'application.
  - Les équipements fournis par des tiers sont en dehors du champ d'application.
  - L'évaluation de la résilience effectue l'analyse et formule des recommandations portant sur l'infrastructure réseau existante et ne fait aucune recommandation fondée sur une conception future du réseau.
  - L'évaluation de la résilience ne fait aucune analyse des performances du réseau, ni analyse d'applications, ni évaluation de l'utilisation de la bande passante du réseau.
- **Infrastructure vidéo des fournisseurs de services :**
  - L'évaluation de la résilience de l'infrastructure vidéo des fournisseurs de services est axée sur l'évaluation de la disponibilité pour l'utilisateur final et n'évalue pas la disponibilité de l'ensemble du réseau.
- **Réseau optique :**
  - Un (1) rapport d'évaluation de la résilience contient jusqu'à cinquante (50) périphériques.
  - Le champ d'application de l'évaluation de la résilience se concentre sur les schémas de protection et l'acheminement de secours sur le plan du matériel uniquement. La résilience de l'alimentation, du circuit et de la capacité du nœud de la capacité et les produits tiers sont hors du champ d'application.

1.4.2. Évaluation de la sécurité des périphériques de réseau

L'évaluation de la sécurité des périphériques réseau aide le Client à analyser les configurations des périphériques pour contribuer à détecter les lacunes de sécurité et produit des recommandations pour corriger les lacunes cernées dans les configurations.

Technologies prises en charge

- Sécurité de réseau
- Sécurité du nuage
- Politique de sécurité et accès
- Menace avancée

Renseignements supplémentaires à recueillir

- Modèles de sécurité des périphériques du client, configuration des périphériques et politiques.

Responsabilités de Cisco

- Passer en revue les besoins et les objectifs de sécurité des périphériques du Client.
- Évaluer jusqu'à 350 configurations de périphérique Cisco; un maximum de dix (10) de ces périphériques peuvent être des pare-feu. Au maximum deux (2) grappes FTD.
- Analyser la configuration des périphériques, en se concentrant sur le renforcement de la sécurité des périphériques individuels.
- Analyser les règles de pare-feu pour détecter les problèmes de configuration courants.

Livrables

- Rapport d'évaluation de la sécurité des périphériques réseau

Restrictions

Les types de système d'exploitation pris en charge pour l'évaluation de la sécurité des périphériques réseau sont les suivants :

- Systèmes d'exploitation compatibles :
  - Cisco IOS
  - Cisco IOS XR
  - Cisco NX-OS
  - Cisco IOS-XE
  - Cisco ASA / ASASM
  - Cisco FWSM
  - Cisco PIX
  - Cisco FTD
  - Cisco WSA
  - Cisco CAT-OS

1.4.3. Évaluation de la sécurité de la solution de collaboration

L'évaluation de sécurité de la solution de collaboration fournit aux clients un rapport d'évaluation de la sécurité, des recommandations et une analyse des risques de cinq éléments essentiels de la solution :

- **Infrastructure de réseau collaboratif** : segmentation du réseau et réseaux locaux virtuels, qualité de service, listes de contrôle d'accès, matériel et logiciel, DHCP, DNS, TFTP et NTP.
- **Identification et gestion des accès :** autorisations, gestion des comptes, journalisation des accès, gestion des modifications de configuration
- **Contrôle des appels** : Cisco Unified Communications Manager (CUCM), passerelles vocales, liaisons ligne principale SIP, Cisco Unified Border Element (CUBE), plan de numérotation, signalisation et supports.
- **Terminaux** : téléphones IP Cisco Unified, téléphones logiciels, points d'extrémité vidéo, terminaux et les périphériques se connectant au réseau IP.
- **Applications** : les applications utilisateurs comme CUCM, la messagerie unifiée, les téléconférences, la vidéo, le service à la clientèle et les outils personnalisés qui améliorent les capacités des systèmes de communication IP.

Architecture prise en charge

- Collaboration

Renseignements supplémentaires à recueillir

** Propre à la sécurité de la solution de collaboration*

- Infrastructure UC, qui peut comprendre les éléments suivants :
  - Historique détaillé des appels de CUCM.
  - Rapport sur le plan de numérotation et rapport des journaux
  - Analyse du routage des appels de CUCM
  - Protection de la signalisation et des supports
  - Points terminaux
  - Applications
  - Passerelle vocale, données de la ligne principale SIP / CUBE
- Infrastructure de service client, qui peut comprendre les éléments suivants :
  - Serveur du système d'exploitation Windows
  - Serveur MS SQL
  - Pare-feu et de ports de Windows
  - Antivirus
  - Accès à distance
- Infrastructure de collaboration vidéo, qui peut comprendre les éléments suivants :
  - Applications vidéo
  - Contrôle des appels

- Conférences
- Points d'extrémité vidéo

- Collaboration en périphérie

Responsabilités de Cisco

La portée de l'évaluation de la sécurité de la collaboration inclura une ou les deux zones suivantes spécifiées dans le devis :

- Fraude touchant les appels interurbains
- Déni de service téléphonique (TDO)

Valider les besoins du client

- Vérifier les terminaux de la solution de collaboration sélectionnés par le client ainsi que ses préoccupations en matière de sécurité.
- Confirmer l'emplacement des serveurs d'application et d'hébergement ainsi que les préoccupations du client en matière de sécurité.
- Valider le modèle de déploiement de la solution de collaboration (physique et logique) et les exigences de sécurité (s'il y a lieu).
- Vérifier les connexions fédérées ou les applications interentreprises exécutées sur le réseau.
- Vérifier la liaison du réseau téléphonique public commuté (SIP) et la sécurité appliquée, s'il y a lieu.

Évaluation de la sécurité

- Évaluer l'efficacité des contrôles de sécurité du réseau qui servent à protéger la solution de collaboration du client.
- Réaliser une analyse des risques logiciels sur les terminaux et les serveurs d'applications collaboratifs.
- Analyser et comparer les politiques de sécurité du client avec les pratiques exemplaires en matière de sécurité de la solution de collaboration de Cisco.
- Réaliser des analyses de CUCM et des passerelles téléphoniques ou des lignes principales SIP, s'il y a lieu.

Livrables

- Rapport d'évaluation de la sécurité de la solution de collaboration
- Résumé du rapport d'évaluation de la sécurité de la solution de collaboration

Responsabilités du client

- Aucune modification majeure n'est apportée à l'infrastructure de collaboration pendant l'évaluation de la sécurité qui, en fonction de la complexité de l'environnement, peut durer jusqu'à quatre (4) semaines.

1.4.4. Évaluation de vérification des radiofréquences

Le service d'évaluation de vérification des radiofréquences (RF) étudie l'environnement des radiofréquences, fournit une analyse et formule des recommandations pour l'optimisation de la couverture et des performances des radiofréquences.

Technologies prises en charge

- Réseau sans fil

Renseignements supplémentaires à recueillir

- Mesures des interférences internes et externes à un moment donné.

Responsabilités de Cisco

- Valider les performances et la couverture des radiofréquences du réseau local sans fil en les comparant à la documentation de la conception du réseau local sans fil.

- Étudier la couverture, les interférences, les performances générales et la configuration réseau de l'environnement des radiofréquences.

Livrables

- Document de vérification des radiofréquences

1.4.5. Évaluation des radiofréquences de réseau local sans fil

Le service d'évaluation des radiofréquences de réseau local sans fil examine la propagation du signal des radiofréquences pour optimiser le placement du point d'accès sans fil. Cisco effectue une analyse sur site afin de recueillir et d'évaluer les détails du site, y compris les considérations physiques et environnementales, l'alimentation électrique CA/CC, le câblage, la synchronisation réseau, les périphériques et l'accès à distance.

Technologies prises en charge

- Réseau sans fil

Responsabilités de Cisco

- Effectuer une analyse de la couverture, des interférences, des performances générales et de la configuration réseau de l'environnement des radiofréquences sur le site.
- Effectuer une étude critique des radiofréquences pour déterminer le placement optimal du point d'accès.
- Formuler des recommandations à propos de la modification et des améliorations à apporter au site en effectuant des analyses qui comprennent notamment ce qui suit :
  - Analyse de la couverture des radiofréquences.
  - Analyse des interférences.
  - Analyse du spectre des radiofréquences (facultative).

Livrables

- Rapport d'analyse du site

2. COMPÉTENCE OPÉRATIONNELLE

Le service de compétence opérationnelle aide le client en lui fournissant des recommandations d'améliorations afin que gagnent en maturité les processus, les mesures, les outils et les ressources opérationnelles qui permettent d'améliorer les compétences et les connaissances liées aux technologies de Cisco.

NAV. SECT.

La section **Compétence opérationnelle** inclut les capacités et les livrables suivants :

2.1. Gestion des instruments

Le service de gestion des instruments aide le client dans l'analyse des objectifs de gestions par rapport aux capacités et fonctionnalités actuelles, évalue les effets des nouvelles exigences et formule des recommandations pour aligner la conception de la solution de gestion sur les priorités, les buts et les objectifs.

2.1.1. Examen des instruments de gestion

Le service d'examen des instruments de gestion aide le personnel des opérations à réaliser les objectifs commerciaux et opérationnels actuels et futurs de gestion de réseau en intégrant les meilleures pratiques de Cisco en matière d'architecture et d'opérations.

Les spécialistes en ingénierie de Cisco évaluent les exigences de conception techniques et architecturales de la solution du client (capacité, résilience, efficacité, extensibilité), effectuent une évaluation des capacités et des risques actuels et formulent des recommandations pour aider le client à réaliser ses objectifs commerciaux et opérationnels. Cisco optimise la visibilité et le contrôle de l'environnement informatique du client pour une (1) architecture.

Technologies prises en charge

- Gestion et orchestration de réseau

Solutions prises en charge

- WAN défini par logiciel
  - Gestion et orchestration de réseau

Responsabilités de Cisco

- Mettre l'accent sur les domaines qui peuvent inclure la gestion des événements, la gestion des incidents, la gestion des problèmes, la gestion du changement, la gestion des services, la gestion des ressources et de la configuration, la gestion du catalogue des services de TI, la gestion de la performance et de la capacité, la gestion de la sécurité, la gestion des connaissances, l'automatisation et l'orchestration ainsi que la facturation et la rétrofacturation.
- Analyser les exigences, les pratiques actuelles et les capacités du client par rapport aux meilleures pratiques recommandées par Cisco.
- Analyser l'effet des nouvelles exigences sur l'infrastructure de gestion du réseau et l'assistance opérationnelle en place.
- Fournir une assistance pour l'harmonisation de la conception des instruments de gestion avec l'évolution de l'architecture du réseau.
- Mettre à jour la documentation actuelle de conception des instruments de gestion du réseau.

Autres responsabilités

** Propre au service de gestion et d'orchestration du réseau*

- Examiner et formuler des recommandations concernant ce qui suit :
  - Choix et la configuration du protocole de gestion
  - Choix et configuration des applications des instruments de gestion du réseau en place.
  - Questions de sécurité.

Livrables

- Rapport d'examen des instruments de gestion

2.1.2. Évaluation de la planification et de la préparation du déploiement des outils de gestion

Le service de l'évaluation de la planification et de la préparation du déploiement des outils de gestion aide le personnel des opérations du client à préparer la maintenance après mise en œuvre de la solution logicielle de gestion. Cisco valide les plans et les processus de mise en œuvre, vérifie les scénarios de test et les résultats et offre des conseils au client à propos des effets sur les processus opérationnels.

Technologies prises en charge

- Gestion et orchestration de réseau
- Réseau central de transmission par paquets
- 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 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
- WAN défini par logiciel
  - Gestion et orchestration de réseau
- Accès défini par logiciel
  - 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

Responsabilités de Cisco

- Valider les plans et processus de mise en œuvre de la solution du Client.
- Valider les objectifs, les plans, les résultats et les problèmes relatifs au test de la solution du client.
- Formuler des recommandations d'amélioration au client à propos des capacités et de l'état de préparation du processus opérationnel.

Livrables

- Soutien consultatif et conseils seulement

2.2. Gestion des mesures

Le service de gestion des mesures aide le client à examiner les objectifs et les exigences en matière de mesures, à évaluer l'efficacité des mesures actuelles par rapport aux capacités recommandées quant aux mesures et aux outils et fournit des étapes pour élaborer la définition, l'harmonisation, la mesure et les rapports des IRC pour améliorer la visibilité et le processus décisionnel.

2.2.1. Définition, mise en œuvre et rapport des IRC

Le service de définition, de mise en œuvre et de rapport des indicateurs de rendement clés (IRC) aide le client à définir et à mettre en place un cadre pour mesurer les facteurs clés de succès et les IRC de la solution logicielle de gestion de Cisco et du système. Le champ d'application des IRC peut comprendre des indicateurs fonctionnels, comme la gestion du provisionnement de service, de défaillances, de performance et de configuration, ainsi que des indicateurs de performance, comme les capacités de mémoire, de traitement et de base de données.

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
- Accès défini par logiciel
  - Gestion et orchestration de réseau
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau

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

- Évaluer les IRC potentiellement nécessaires au client en se basant sur les IRC recommandés par Cisco.
- Définir les sources de collecte de données, le processus, les possibilités d'automatisation et les seuils cibles des IRC.
- Définir la propriété fonctionnelle, la propriété des processus et la fréquence des examens des IRC.

Livrables

- Rapport sur le cadre des IRC

Responsabilités du client

- Fournir les priorités et les exigences en matière de facteurs clés de succès et d'IRC.

2.2.2. Vérification des IRC et recommandations

Le service de vérification des IRC et de recommandations recueille et analyse les IRC de la solution Cisco sur une période donnée pour déceler des problèmes dans la gestion des défaillances, de la performance, des capacités et de la configuration qui sont directement liés à la stabilité et la disponibilité de la solution du Client. Le devis des services précisera la ou les solutions Cisco prises en charge.

Technologies prises en charge

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

Solutions prises en charge

- Solution Cisco Policy (Cisco Policy Solutions ou CPS) :
- Self-Optimizing Network (SON)
  - Politique de mobilité et accès
- Accès défini par logiciel
  - Gestion et orchestration de réseau
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau

Responsabilités de Cisco

- Produire le rapport de vérification des IRC et de recommandations :
- Pour la solution Cisco Policy Suite (CPS) :
  - S'il y a lieu, sur les interfaces Gx et Gy, les IRC suivants seront inclus au rapport :
  - Demande de contrôle du crédit – taux de réussite, d'abandon et d'erreur.
  - Demande de réautorisation – taux de réussite, d'abandon et d'erreur.
  - S'il y a lieu, sur l'interface Sy, les IRC suivants seront inclus au rapport :
    - Demande de limite des dépenses – taux de réussite.
    - Notification de l'état des dépenses – taux de réussite.
    - Demande de fin de session – taux de réussite.
- Pour la solution SON de Cisco :
  - Analyse des problèmes principaux et recommandations connexes :
    - Produire des rapports mensuels sur les problèmes principaux, y compris les taux de coupure les plus élevés.
    - Optimiser les paramètres SON pour ces problèmes afin d'améliorer les IRC.
    - Recommander des solutions préliminaires pour les problèmes principaux.
  - Rapports SON : Rapports sur les IRC et Boomer :
    - Les rapports de collision Boomer et Primary Scrambling Code (PSC) seront fournis à la demande du client.
    - Rapport d'activité pour application pour montrer les actions SON.
    - Mesures des IRC des contrôleurs de réseau à distance et du réseau.
    - Nombre des activités des nouvelles cellules voisines par la solution SON.
- Pour Cisco Prime® Access Registrar :
  - S'il y a lieu, les éléments suivants seront inclus dans le rapport :
    - IRC des systèmes
    - Compteurs définis
    - Compteurs Radius
    - IRC de Rest

Produits livrables :

- Rapport de vérification des IRC et de recommandations

2.2.3. Tendances et rapports des IRC

Le service d'établissement des tendances et des rapports des IRC aide le client en fournissant des recommandations pour l'amélioration de la solution logicielle de gestion de Cisco et des processus, des tendances et des écarts des IRC par rapport à la base de référence. Le service planifié est effectué à une fréquence convenue avec le client (la recommandation est d'une fois par trimestre).

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
- Accès défini par logiciel
  - Gestion et orchestration de réseau
- Analyses et assurance des fournisseurs de service
  - Gestion et orchestration de réseau

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

- Analyser les tendances des IRC du client afin de relever les écarts par rapport aux cibles de référence.
- Évaluer plusieurs points de vue comme la conception, la capacité, l'assistance et les opérations.

Livrables

- Rapport d'évaluation des IRC

2.2.4. Développement d'un programme sur les mesures de sécurité

Cisco aidera le client à élaborer un programme de mesures de sécurité, qui comprend l'analyse et la création d'un catalogue de mesures de sécurité et des tableaux de bord initiaux selon les besoins et les exigences du client.

Cisco utilisera les normes reconnues pour les mesures et les mesures de sécurité, notamment la norme ISO 27004 : Technologies de l'information – Techniques de sécurité – Gestion de la sécurité de l'information – Mesures. Cisco utilise des approches combinées pour assurer l'élaboration d'un programme de mesures de sécurité, notamment des ateliers de formation, des séances de travail individuelles ou de groupe, et un examen des objets. Les livrables qui en découlent comprennent des recommandations d'améliorations stratégiques et tactiques du programme de mesures, ainsi que des mesures et des tableaux de bord spécifiques élaborés tout au long de l'exécution.

Architecture prise en charge

- Sécurité

Responsabilités de Cisco

- Examiner la maturité du programme actuel de mesures de l'information et des TI du client.
- Animer des ateliers d'introduction aux indicateurs de sécurité pour des ressources opérationnelles et techniques pour :
- Donner un aperçu des indicateurs du secteur.
- Donner un aperçu des applications spécifiques d'indicateurs de sécurité de l'information et informatique.
- Donner un aperçu de la norme ISO 27004 et des autres normes et cadres appropriés d'indicateurs de sécurité.
- Expliquer la méthodologie Goal-Question-Metric ou GQM (approche par les buts).
- Aborder des exemples spécifiques d'indicateurs de sécurité et d'études de cas.
- Aborder et définir les questions et les mesures de sécurité principales qui doivent être régulièrement traitées et signalées.
- Analyser les résultats des ateliers et l'applicabilité à un engagement global.
- Comparer le programme actuel aux recommandations et aux exigences de la norme ISO 27004 et d'autres cadres de mesure.
- Animer des ateliers GQM pour les ressources opérationnelles et techniques afin d'élaborer et d'améliorer le catalogue de mesures du client, qui peuvent inclure les activités suivantes :
- L'utilisation de techniques GQM pour définir et explorer des scénarios de mesures stratégiques spécifiques pour les mesures de sécurité nouvelles ou existantes des clients.
- Analyser les résultats GQM et les intégrer au catalogue des mesures.
- Formuler des recommandations pour les tableaux de bord des cadres et des gestionnaires ainsi qu'une feuille de route pour la maturité des mesures.

Livrables

- Rapport de recommandations de mesures de sécurité

2.3. Gestion des opérations

La gestion des opérations aide le Client à évaluer le risque de lacunes opérationnelles et à corriger ces dernières. Cisco et le client collaboreront avec le centre d'assistance technique Cisco (TAC) et les unités opérationnelles appropriées pour résoudre les dossiers Cisco de priorité 1 (P1) et de priorité 2 (P2) ouverts.

2.3.1. Soutien technique en cas d'escalade

Le service de soutien technique en cas d'escalade améliore le processus de gestion des incidents et des problèmes du client en fournissant du soutien aux activités de restauration du service du centre d'assistance technique de Cisco pour les incidents non planifiés.

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Gestion et orchestration de réseau
- Orchestration et automatisation de centre de données
- Tetration
- 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
- Accès par câble de prochaine génération
- Calcul en périphérie de réseau de l'IDO et informatique géodistribuée

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

Responsabilités de Cisco

- Effectuer une évaluation technique avec escalade du centre d'assistance technique de Cisco en suivant les procédures, les diagnostics et les processus d'escalade appropriés du centre d'assistance technique de Cisco.
- Collaborer avec le centre d'assistance technique de Cisco relativement à l'environnement Cisco du client pour aider le centre d'assistance technique et les unités commerciales appropriées de Cisco à résoudre l'incident.
- Aider le client en lui fournissant une assistance à distance pour traiter les dossiers P1 et P2 ouverts.
- Aider le client à analyser les problèmes récurrents et les causes premières, en fournissant notamment une assistance consultative en vue d'élaborer un plan d'action visant à prévenir, pallier et minimiser les effets opérationnels des problèmes.

Autres responsabilités

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

- Le chef de projet de Cisco affectera un spécialiste en ingénierie qui assurera le suivi et la résolution à distance des problèmes liés aux composants de la solution de collaboration Cisco des dossiers P1 et P2 seulement.

Livrables

- Soutien consultatif et conseils seulement

Responsabilités du client

- Permettre à Cisco de communiquer avec les utilisateurs ayant joint le service d'assistance ou le centre de résolution du client pour obtenir de l'aide concernant des problèmes ou des questions liés au service ou aux composants de la solution Cisco.
- Informer les services de Cisco de l'ouverture d'un billet nécessitant une intervention et fournir le numéro de dossier attribué par le centre d'assistance technique de Cisco.

Remarque : Le client n'escaladera pas de problèmes ou de questions connexes tant que le centre d'assistance technique de Cisco n'aura pas effectué de diagnostic.

- Collaborer avec le centre d'assistance technique de Cisco pour résoudre et clore le problème ou le dossier et ne faire intervenir les experts-conseils en réseautique de Cisco que dans les dossiers P1 et P2 critiques, si nécessaire.

Restrictions

- Les éléments suivants ne sont pas fournis dans le cadre du service de soutien technique en cas d'escalade :
- Le spécialiste en ingénierie des services de Cisco n'apporte aucune modification à l'environnement de production du client.
- Le service ne couvre pas les priorités P3 et P4 du centre d'assistance technique de Cisco.
- Il doit y avoir une présence sur le site pour l'assistance au dossier du centre d'assistance technique de Cisco.
- Ces livrables ne remplacent pas le centre d'assistance technique de Cisco, la gestion des opérations High-Touch de Cisco, l'assistance technique High-Touch de Cisco ou toute autre forme de service ou de soutien technique, y compris l'assistance technique d'un tiers.
- Les services techniques de Cisco, le centre d'assistance technique de Cisco ainsi que tous les services suivants auxquels le client peut souscrire, comme l'assistance technique High-Touch, la gestion des opérations High-Touch et les services techniques ciblés, sont responsables de l'escalade et de la résolution des dossiers, ainsi que de mobiliser et de faire intervenir les ressources appropriées, comme les unités opérationnelles de Cisco et des fournisseurs tiers, en plus de fournir des mises à jour sur l'état du dossier et les communications relatives à celui-ci et à sa clôture.

2.3.2. Gestion de l'équipement

La gestion des ressources aide le client avec des recommandations de meilleures pratiques Cisco pour la gestion des ressources et des contrats en fonction de l'inventaire des clients, la production de rapports sur les déplacements, les ajouts, les modifications et les suppressions (MACD) des ressources, ainsi que la surveillance de la couverture des ressources et des droits.

La gestion des ressources comporte deux niveaux :

- Standard
- Supérieur

La gestion des ressources de niveau supérieur (Premium) offre un niveau d'engagement et de personnalisation supérieur au niveau standard.

Solutions prises en charge

- Cisco Expert Care

Renseignements supplémentaires à recueillir

- Informations sur l'inventaire et le contrat de service du client.

- Enregistrement du client du numéro de série qui a été supprimé et remplacé par une autorisation de retour de matériel (RMA).

Responsabilités de Cisco

- Fournir les responsabilités communes suivantes :
- Fournir des rapports sur l'inventaire du client, notamment les éléments suivants :
  - Les modifications pour traiter la couverture des services de l'inventaire, la co-résiliation, et l'emplacement.
- Fournir un processus documenté pour les déplacements, les ajouts, les modifications et les suppressions de ressources informatiques.
- Indiquer le niveau de gestion des ressources standard ou niveau Premium, comme spécifié sur le devis :

• Gestion de l'équipement	• Niveau standard	• Niveau supérieur (Premium)
Niveau d'engagement du client		
1.1 – Allocation d'une ressource	• Attribuée	• Attribuée
Emplacement de la ressource	• Distant	• Distant
Visites sur place	• Sans objet	• Quatre fois l'an
2.0 – Établissement et maintien d'un parc de machines installées (Installed Base ou IB) consolidé		
2.1 – Ressource et qualification de l'entité commerciale	• Pris en charge	• Pris en charge
2.2 – Établissement et maintien d'un parc de machines installées de référence	• Pris en charge	• Pris en charge
2.3 – Fréquence des mises à jour	• Chaque mois	• Chaque mois
3.0 – Rapprochement / maintenance		
3.1 – Identification et correction des écarts de données	• Pris en charge	• Pris en charge
4.0 – Production de rapports, analyses et évaluations des activités		
4.1 – Production d'un rapport de référence du parc de machines installées	• Pris en charge	• Pris en charge
4.2 – Évaluation des activités	• Deux fois l'an, à distance	• Quatre fois l'an, sur place
4.3 – Production de rapports et analyses	• Standard	• Sur mesure
4.4 – Évaluation des activités et conseils	• Standard	• Sur mesure

Livrables

- Les livrables fournis sont basés sur le niveau de service de gestion des ressources Standard ou Premium comme spécifié dans le devis.

Responsabilités du client

- Désigner un représentant qui agira comme principale ressource pour la gestion des ressources; ce représentant travaillera avec le gestionnaire de ressources Cisco pour résoudre toute question relative au service de gestion des ressources.

2.3.3. Gestion des Incidents

La gestion des incidents fournit un point de contact unique, un gestionnaire des opérations Cisco High-Touch (« HTOM »), pour la gestion de tous les incidents. Le HTOM a connaissance des processus clients, des organismes d'assistance Cisco, du processus de transmission et des coordonnées du client pour faciliter la restauration des opérations de service client. Pour la gestion des incidents sur site, vous devez acheter ces livrables avec le service d'assistance sur site.

Remarque : Le service de gestion des incidents est fourni avec la surveillance des services et la production de rapports.

Solutions prises en charge

- Cisco Expert Care

Renseignements supplémentaires à recueillir

- Configuration du centre d'exploitation du réseau (Network Operation Center ou NOC) du client, par exemple les groupements de personnel, les outils, les processus de communication et d'escalade, les contacts et les groupes de soutien sur site.

Responsabilités de Cisco

- Faciliter la résolution des problèmes sur une base réactive pour les problèmes techniques signalés à Cisco par le client.
- Gestion des incidents 24 h sur 24, 7 j sur 7 pour les demandes de soutien et la gestion des processus d'escalade pour les dossiers d'un niveau de gravité 1 ou 2 en dehors des heures normales d'ouverture.
- Effectuer le suivi, chez Cisco et chez le client, et identifier des lacunes quant à la réponse à une requête de service.
- Coordonner les organismes de soutien Cisco, le processus d'escalade et des ressources Client pour les demandes de service.
- Effectuez un examen a posteriori de l'incident pour déterminer les recommandations relatives aux actions correctives et aux bonnes pratiques pour améliorer les processus d'assistance opérationnelle.
- Procéder à l'évaluation opérationnelle des processus actuels du client et recommander les bonnes pratiques en matière de gestion des incidents et des événements.

Livrables

- Faciliter la résolution des incidents et des problèmes

2.3.4. Surveillance du service et rapports

La surveillance du service et la production de rapports aident le client grâce à des recommandations concernant les bonnes pratiques opérationnelles, des informations et des indicateurs de performance liés aux incidents en matière d'amélioration de la qualité du service, et des gains de performances au niveau des services et de l'efficacité opérationnelle.

Dépendances

- La surveillance des services et la production de rapports nécessitent l'achat de la solution de gestion des incidents.
- La production de rapports d'analyse des causes premières et des recommandations qui en découlent nécessite l'achat de la solution de gestion des problèmes.

Solutions prises en charge

- Cisco Expert Care

Renseignements supplémentaires à recueillir

- Procédures et processus établis utilisés pour l'assistance.

Responsabilités de Cisco

- Fournir un statut et des rapports, du soutien pour le processus d'escalade et coordonner le retour des pièces nécessitant une analyse d'ingénierie sur site (Engineering Field Analysis ou EFA).
- Vérifier l'état et la progression des niveaux de prestation de services, créer des requêtes de service, effectuer le suivi des actions et traiter les problèmes en suspens.

- Effectuer une revue trimestrielle des livrables et des activités fournis au cours de la période précédente et élaborer le plan d'action pour le prochain trimestre.
- Effectuer régulièrement une évaluation proactive sur l'excellence opérationnelle.
- Créer un profil client pour les besoins opérationnels des services techniques Cisco, incluant les processus, les procédures et l'accès au réseau pour le soutien technique.
- Fournir des rapports sur les incidents liés au service qui peuvent comprendre les éléments suivants, le cas échéant :
- Les requêtes de service Cisco, les erreurs connues, les améliorations opérationnelles postérieures à l'incident, l'analyse des causes premières et les recommandations, les anomalies et les tendances opérationnelles.
- IRC et rapports analytiques axés sur l'analyse afin d'améliorer l'efficacité opérationnelle

Livrables

- Coordination et élaboration de rapports EFA
- Rapport sur les niveaux de prestation de services
- Évaluation de l'état de préparation pour la gestion des incidents
- Rapport d'incident de service
- Rapports d'analyse et de tableau de bord IRC

2.3.5. Gestion des problèmes

La gestion des problèmes permet d'accéder au service d'assistance technique ou d'ingénierie Cisco High-Touch de Cisco qui connait votre environnement réseau.

2.3.5a. Gestion des problèmes – Assistance technique High-Touch

Offre un accès direct de vingt-quatre (24) heures par jour, sept (7) jours par semaine à l'équipe de spécialistes du service d'assistance technique Cisco High-Touch (HTTS). L'équipe HTTS aide à dépanner votre réseau Cisco à la recherche de problèmes complexes et critiques et fournit une assistance pour la résolution des problèmes identifiés. HTTS propose deux options d'assistance : un groupe d'assistance technique High-Touch, ou une équipe dédiée au service d'assistance technique High-Touch.

Dépendances

- Le service de gestion des incidents est requis.

Renseignements supplémentaires à recueillir

- Modifications matérielles actuelles et planifiées du client, mises à niveau logicielles et modifications de configuration, méthodes de procédures (MOP).

Solutions prises en charge

- Cisco Expert Care

Responsabilités de Cisco

- Assurer le suivi des dossiers et le dépannage qui inclut les éléments suivants :
- Fournir un accès direct si disponible, vingt-quatre (24) heures par jour, sept (7) jours par semaine à une équipe HTTS grâces aux coordonnées fournies par Cisco.
- Fournir une fenêtre d'intervention proactive pour le soutien qui inclut notamment :
- Travailler de façon proactive avec le client pour créer la requête de service et programmer la fenêtre de maintenance.
- 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.
- Fourniture d'une assistance à distance en alerte durant la période de maintenance.

Remarque : Les conditions générales et le contrat de niveau de service de Cisco Expert Care concernant le temps de réponse et de reprise sont documentées dans les conditions générales des Services opérationnels essentiels Cisco, section 5 – contrat de niveau de service de Cisco Expert Care.

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 pas responsable du développement des MOP (Methods of Procedure).

Livrables

- Suivi de dossiers et dépannage
- Fenêtre de maintenance proactive

Remarque : Le devis spécifie un service d'assistance technique High-Touch par une équipe générale ou dédiée.

2.3.5b. Gestion des problèmes – Ingénierie High-Touch

Fournit un accès direct à un spécialiste Cisco High-Touch (High-Touch Engineering ou HTE), qui dispose de connaissances techniques et qui est familier avec votre environnement réseau. L'équipe HTE aide à dépanner votre réseau Cisco à la recherche de problèmes complexes et critiques et fournit une assistance pour la résolution des problèmes définis. Pour la gestion des problèmes sur site par High-Touch Engineering, vous devez acheter le Service d'assistance opérationnelle sur site.

Dépendances

- Les livrables de gestion des incidents sont requis pour ce service.
- L'exécution d'une analyse des causes premières par Cisco est tributaire de l'obtention de toutes les informations nécessaires à Cisco en temps opportun.

Renseignements supplémentaires à recueillir

- Modifications matérielles actuelles et planifiées du client, mises à niveau logicielles et modifications de configuration, méthodes de procédures (MOP).

Solutions prises en charge

- Cisco Expert Care

Responsabilités de Cisco

- Assurer le suivi des dossiers et le dépannage qui inclut les éléments suivants :
- Fournir un accès direct au HTE si disponible, pendant les heures de travail standard, en utilisant les coordonnées fournies par Cisco.
- Effectuer une analyse de cause première des problèmes techniques de premier ordre concernant l'infrastructure de réseau.
- Fournir une fenêtre d'intervention proactive pour le soutien qui inclut notamment :
- Travailler de façon proactive avec le client pour créer la requête de service et programmer la fenêtre de maintenance.
- 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.
- Fourniture d'une assistance à distance en alerte durant la période de maintenance.

Livrables

- Rapport d'analyse de cause première
- Gestion des problèmes
- Fenêtre de maintenance proactive

2.3.6. Soutien d'événement planifié de réseau à optimisation autonome (SON) et d'installations

Le service de soutien d'événement planifié de réseau à optimisation autonome (SON) et d'installations offre une assistance proactive aux événements planifiés à grande échelle (des jeux ou des conférences) qui utilisent les ressources de réseau d'accès radio (RAN) du client. Cisco fournit une assistance pour la planification, la mise en œuvre et le soutien des principales configurations des modules d'application SON.

Solutions prises en charge

- Réseau à optimisation autonome
  - Politique de mobilité et accès

Renseignements supplémentaires à recueillir

- Exigences commerciales et techniques de la configuration du module de gestion d'événement de masse (MEH).
- Événement planifié de client/détails sur les installations

Responsabilités de Cisco

- Aider le client à configurer les modules d'application MEH pour répondre à ses besoins en matière d'événement et de réseau sur le site.
- Fournir une assistance proactive en cas de gel ou de réacheminement du réseau et de toute autre activité planifiée de RAN majeure pour la solution SON.
- Examiner les rapports de RAN de client sur le réseau ou le trafic prévu.

Livrables

- Soutien consultatif et conseils seulement

2.4. Gestion des connaissances

Le service de gestion des connaissances aide le Client à améliorer ses connaissances et ses compétences techniques par des séances de transfert de connaissances pour les opérations, par l'accès à la bibliothèque de connaissances techniques et par des ateliers de formation Cisco et des ateliers techniques spécialisés.

2.4.1. Séance de transfert de connaissances pour les opérations

Le service de séance de transfert de connaissances pour les opérations permet le transfert de connaissances techniques sur des sujets mutuellement acceptables et relatifs aux produits et technologies Cisco déployés dans l'environnement du Client. Les séances sont axées sur les meilleures pratiques d'opérations, de réglage, de dépannage, de maintenance et de gestion des solutions Cisco déployées. 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
- 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

- Service à la clientèle
- Collaboration vidéo
- 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
- WAN 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.

Livrables

- 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).

2.4.2. Bibliothèque de formation

La bibliothèque de formation permet d'accéder aux meilleures pratiques de Cisco Services, aux études de cas, aux livres de Cisco Press, aux ressources techniques à la demande, aux cours en ligne et aux exercices pratiques interactifs.

Les deux bibliothèques suivantes sont disponibles :

- Bibliothèque de connaissances techniques
- Bibliothèque de formation Platinum

2.4.2a. Bibliothèque de connaissances techniques

Le service de bibliothèque de connaissances techniques (TKL) est un service par abonnement qui permet d'accéder aux meilleures pratiques et aux connaissances techniques des services de Cisco élaborées par les spécialistes en ingénierie des services de Cisco. La bibliothèque permet aux utilisateurs finaux d'accéder à des ressources d'apprentissage et à des renseignements techniques comme les livres blancs, les guides de conception et de mise en œuvre, les études de cas, les livres publiés par Cisco Press, les webinaires en direct et les vidéos à la demande. La bibliothèque est rendue accessible par Cisco par l'intermédiaire d'un portail Web sécurisé.

La bibliothèque de connaissances techniques n'est disponible que dans certaines zones géographiques qui seront spécifiées dans le devis.

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- 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

Solutions prises en charge

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

Responsabilités de Cisco

- Rendre le contenu accessible au nombre de personnes autorisées spécifié dans le devis du client, y compris les clips multimédias sous la forme de contenu vidéo ou audio à la demande, ainsi que le contenu en encadré comme les livres blancs, les études de cas, les guides de conception, les guides de configuration, les guides de dépannage, les documents de formation, les guides de déploiement, les manuels en ligne et les intercalaires.
- Fournir la liste des formations en ligne accessibles aux personnes autorisées par l'intermédiaire du portail.

Remarque : Cisco peut réviser, mettre à jour ou supprimer des clips multimédias ou du contenu en encadré précédemment publiés (le contenu mis à jour). Cisco mettra à disposition du client tout le contenu mis à jour dans le cadre des services. Le contenu mis à jour exclura les versions de clips multimédias ou de contenu en encadré (s'il y a lieu) précédemment publiées que le contenu mis à jour est censé remplacer.

Livrables

- Accès à la TKL, une bibliothèque en ligne de ressources d'apprentissage et renseignements techniques

2.4.2b. Bibliothèque de formation Platinum Cisco

La bibliothèque de formation Cisco Platinum (CPLL) est un ensemble de ressources techniques à la demande, de cours en ligne et d'ateliers pratiques interactifs. Un conseiller en formation Cisco assiste le client avec des recommandations de cursus et l'exploitation du contenu de cours CPLL.

Solutions prises en charge

- Cisco Expert Care

Responsabilités de Cisco

- Accès à un conseiller en formation Cisco, qui offre de l'aide dans le contexte des recommandations de cursus et le recours aux cours CPLL.
- Donner accès à des ressources techniques à la demande de CPLL, à des cours en ligne et à des exercices pratiques interactifs.

Livrables

- Accès à la bibliothèque de formation Cisco Platinum

Remarque : Le nombre de places donnant accès au CPLL est indiqué dans le devis.

2.4.3. Formation Cisco

- La formation Cisco permet d'accéder à un catalogue de plus de 250 cours différents sur la certification et la formation sur les produits disponibles en inscription libre ou en accès restreint (groupe privé). Un conseiller pédagogique Cisco aide le client pour la sélection et la planification des cours.

2.4.3a. Formation Cisco en accès libre

La formation Cisco en accès libre permet d'accéder à un catalogue de formations dirigées par un instructeur et des formations sur les produits, disponibles en inscription ouverte au public. Les formations sont fournies dans des salles de formation Cisco ou chez des partenaires de formation autorisés de Cisco (Cisco Authorized Learning Partners). Un conseiller pédagogique Cisco aide le client pour la sélection et la planification des cours.

Solutions prises en charge

- Cisco Expert Care

Responsabilités de Cisco

- Les places pour les cours proposés publiquement proviennent d'un catalogue de formations dirigées par des instructeurs et de formations sur les produits. Les classes sont fournies en direct ou virtuellement.

Livrables

- Places pour la formation Cisco en inscription libre

Responsabilités du client

- Au moins quarante-cinq (45) jours avant la séance de formation, fournir une liste des participants, leur rôle et leur fonction par rapport à l'objet de la séance.
- Coordonner et programmer une formation Cisco à l'aide d'un conseiller pédagogique Cisco.

2.4.3b. Formation privée pour groupes à accès restreint

La formation privée Cisco pour groupes à accès restreint permet d'accéder à un catalogue de formations dirigées par un instructeur et des formations sur les produits, offertes à des groupes privés de douze (12) personnes. La formation est fournie à l'emplacement du client et est adaptée à son réseau. Un conseiller pédagogique Cisco aide le client pour la sélection et la planification des cours.

Solutions prises en charge

- Cisco Expert Care

Responsabilités de Cisco

- Les places pour les cours privés proviennent d'un catalogue de formations dirigées par des instructeurs et de formations sur les produits. Les classes sont fournies en direct ou virtuellement.

Livrables

- Places pour les formations privées pour groupes à accès restreint

Responsabilités du client

- Au moins quarante-cinq (45) jours avant la séance de formation, fournir une liste des participants, leur rôle et leur fonction par rapport à l'objet de la séance.
- Coordonner et programmer une formation Cisco à l'aide d'un conseiller pédagogique Cisco.

2.5. Réseau classifié(États-Unis seulement)

La formation sur les réseaux classifiés propose des séances de formation qui aident le client à fournir des services permettant de prendre en charge un réseau classifié.

2.5.1. Assistance pour réseau classifié

Le service d'assistance pour réseau classifié Cisco (ARC) aide le Client à résoudre rapidement les problèmes signalés à Cisco. Les clients profitent d'une assistance réactive et directe en tout temps par les spécialistes en ingénierie d'assistance habilités qui connaissent bien la conception et les opérations du réseau du client. Le service ARC utilise des techniques avancées de dépannage grâce à une équipe d'experts certifiés sur une grande variété de technologies et solutions de Cisco.

Le service ARC est composé des services suivants :

- Gestion des opérations High-Touch ARC
- Soutien technique High-Touch ARC

2.5.1a. Gestion des opérations High-Touch ARC (États-Unis seulement)

Remarque : Les livrables du service de gestion des opérations High-Touch ARC sont achetés avec un seul UGS CON-AS-RS-OPT des Services opérationnels essentiels Cisco et permettent d'aider le Client à résoudre les problèmes signalés pour l'une ou l'autre des technologies énumérées ci-dessous.

Technologies prises en charge

- Routage et commutation
- Réseau sans fil
- Gestion et orchestration de réseau
- Infrastructure centrée sur les applications
- Orchestration et automatisation de centre de données
- Communications unifiées

- Systèmes informatiques
- Réseau de stockage
- Commutation de centres de données
- Collaboration vidéo
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- WAN défini par logiciel
  - Gestion et orchestration de réseau
  - Routage et commutation

Responsabilités de Cisco

- Désigner une personne du service d'assistance pour réseau classifié Cisco (responsable des opérations ARC) pour servir de point de contact non technique principal qui fournira les livrables et les activités.
- Fournir les éléments suivants :
  - Gestion de l'escalade des demandes de dossiers : le responsable des opérations facilitera la résolution des problèmes de manière réactive en ce qui a trait aux problèmes techniques que le client aura signalés à Cisco et l'aidera à déterminer si les ressources appropriées sont assignées aux problèmes techniques signalés. Ceci comprend la nécessité d'informer le centre d'assistance technique de Cisco (TAC) et le spécialiste en ingénierie de Cisco qui connaît le réseau du client de tout événement planifié en ouvrant le dossier et d'aviser le TAC des renseignements pertinents relatifs à l'événement planifié.
  - Ensemble de rapports de base : le responsable des opérations fournira des rapports hebdomadaires, mensuels et trimestriels au client.
  - Analyse trimestrielle des données d'opérations : le responsable des opérations aura une rencontre trimestrielle avec le client pour discuter des livrables et des activités afin d'examiner l'alignement sur les objectifs opérationnels du client. Ceci peut comprendre l'utilisation du contrat d'assistance réactive, les statistiques de dossiers, les problèmes de qualité, une analyse globale des cas (comme par priorité de cas ou de type de produit), l'analyse du réseau et les tendances d'autorisations de retour de matériel (ARM).
  - Analyse opérationnelle élaborée des problèmes critiques : Cisco procédera à une analyse des données opérationnelles axée sur les problèmes critiques en relevant les lacunes de connaissances du client, de même que les anomalies ou lacunes opérationnelles. Cisco fournira des recommandations et indiquera les solutions possibles que le client pourra choisir de mettre en œuvre pour permettre de combler ces lacunes de connaissances et de qualité du système.
- Assurer un accès à l'équipe d'assistance pour réseau classifié par un numéro de téléphone fourni par Cisco pour les services suivants :
  - Fournir un suivi de dossiers et du dépannage, s'il y a lieu, jusqu'à vingt-quatre (24) heures par jour et sept (7) jours par semaine comme suit :
    - Appels de gravité 1 et 2 : objectif de réponse dans un délai de quinze (15) minutes.
    - Appels de gravité 3 et 4 : objectif de réponse dans un délai de soixante (60) minutes pendant les heures ouvrables normales, de 8 h à 17 h (HNE).
- Fournir un portail client pour les billets d'incident :
  - Classifier chaque billet d'incident selon une version modifiée des catégories d'incidents du CERT américain : http://www.us-cert.gov/governmentusers/reporting-requirements.
  - Selon les informations connues par Cisco au moment de la création de l'incident, accorder une priorité élevée, moyenne ou faible à tous les incidents en fonction d'un ou de plusieurs critères comme le type d'infection, la confirmation de l'incident ou le nombre de ressources touchées par l'incident. Les niveaux de priorités sont définis de la façon suivante :
    - Élevé : impact commercial critique ou perte de données pour le client.
    - Moyen : effet négatif pour le client, perte potentielle de données, perte potentielle de service.
    - Faible : effet négatif minime pour le client Pas de perte financière. Pas de perte de données.
- Aviser par voie électronique les interlocuteurs désignés par le client au sujet des nouveaux incidents.
- Transmettre des recommandations de mesures d'atténuation, s'il y a lieu, pour l'incident concerné.
- Noter toute mesure corrective nécessitant l'intervention du client, y compris les lacunes dans les renseignements fournis.

Autres responsabilités

* Ne s'applique que si le Client a acheté ces livrables conjointement aux services gérés à distance Cisco.

- Désigner un responsable des opérations ARC qui agira comme interlocuteur principal pour les procédures de gestion du changement.
- Définir le champ d'application global des travaux nécessaires pour adapter le réseau existant du Client et le préparer à la gestion des composants gérés par Cisco, notamment l'évaluation des changements nécessaires à la plateforme, au réseau et aux procédures du Client afin de lancer les services.
- Fournir et aider à gérer un plan de transition qui définit le champ d'application général de la transition des services, déterminer les étapes de référence qui serviront à mesurer la progression du projet, définir les exigences pour assurer la connectivité et l'accès du service, et fixer une date de lancement (ou un ensemble de dates) à laquelle Cisco commencera à gérer ou à surveiller les composants gérés.
- Définir les renseignements sur les stocks et les exigences relatives à la topologie nécessaires pour activer ou intégrer les composants gérés.

Livrables

- Gestion de l'escalade des demandes de dossiers
- Ensemble de rapports de base
- Analyse trimestrielle des données d'opérations
- Analyse opérationnelle élaborée des problèmes critiques
- Suivi de dossiers et dépannage
- Plan de transition (ces livrables ne s'appliquent que si le Client a souscrit aux services gérés à distance Cisco)

Offre groupée de livrables facultatifs

L'offre groupée de livrables facultatifs peut être ajoutée aux livrables indiqués ci-dessus. Les livrables et activités décrits ci-dessous sont offerts individuellement, en groupe de deux livrables facultatifs ou intégralement. Le client ne peut pas choisir plus de deux livrables facultatifs à moins que l'ensemble des livrables facultatifs ne soit sélectionné.

- Coordination et élaboration de rapports EFA : coordonner les retours de matériel nécessitant une analyse de défaillance et la communication avec le Client au sujet de la situation; une assistance régulière sur le plan des rapports, des statuts et de la présentation des enjeux aux niveaux supérieurs sera offerte.
- Rapport sur les niveaux de prestation de services : fournir des rapports sur le niveau des services fournis.
- Rapports personnalisés : fournir des rapports personnalisés soit pour respecter les exigences de rapports de l'accord de niveau de service, soit selon les spécifications du client.
- Responsable des opérations ARC sur le site : mettre à disposition une personne qui se consacrera aux tâches liées à la gestion des opérations sur le site spécifié du client pendant la durée indiquée sur le devis des services.

Offre groupée de livrables facultatifs

- Coordination et élaboration de rapports EFA
- Rapport sur les niveaux de prestation de services
- Rapports personnalisés
- Responsable des opérations ARC sur le site

Restrictions

- Pour la gestion de l'escalade des demandes de dossiers, la préouverture de dossiers pour les événements planifiés ne doit pas dépasser deux (2) événements par mois.

Responsabilités du client

- Coordonner les visites sur le site fournies par Cisco et aviser Cisco au moins trente (30) jours avant la visite prévue; si la date de visite prévue est modifiée, des frais supplémentaires pourraient s'ajouter.
- Signaler directement les problèmes de niveau de gravité 1 et 2 à l'aide du numéro de téléphone fourni par Cisco; les temps de réponse ne concernant pas les problèmes signalés à l'aide de Cisco.com ou de tout autre moyen de communication électronique.

2.5.1b. Soutien technique High-Touch ARC (États-Unis seulement)

Le service d'assistance technique High-Touch ARC (HTTS ARC) permet d'avoir accès à une équipe de spécialistes du réseau qui peuvent évaluer et accélérer la résolution de problèmes, définir une solution qui vise à limiter les interruptions de réseau et aider le personnel d'opérations du réseau à mettre en œuvre la solution appropriée pour améliorer la disponibilité de l'infrastructure opérationnelle essentielle du Client.

Tous les services du HTTS ARC seront fournis par des citoyens des États-Unis, à partir d'emplacements sécurisés aux États-Unis appliquant des contrôles stricts d'accès aux données. Toutes les données du client sont stockées sur un réseau doté de contrôles stricts d'accès aux données.

Segment de clientèle cible

- Agences du gouvernement américain, ou petites et moyennes entreprises qui utilisent des réseaux classifiés.
- Entités gouvernementales américaines non fédérales, ou petites et moyennes entreprises ayant des exigences de sécurité strictes.

Dépendances

- Afin de pouvoir souscrire à l'assistance technique High-Touch ARC, la gestion des opérations High-Touch ARC est requise pour l'ensemble du réseau du client.
- Selon le niveau d'autorisation nécessaire, le service peut commencer au plus tard trente (30) jours après l'acceptation du bon de commande.
- Pour les clients sur des réseaux classifiés ou non classifiés, le service HTTS ARC sera fourni à distance à partir du centre de données sécurisé ARC situé dans le Research Triangle Park en Caroline du Nord.

Technologies prises en charge

- Routage et commutation
- 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
- Collaboration vidéo
- Sécurité de réseau
- Politique de sécurité et accès

Solutions prises en charge

- Orchestration du service réseautique
  - Gestion et orchestration de réseau
  - Orchestration et automatisation de centre de données
- WAN défini par logiciel
  - Gestion et orchestration de réseau
  - Routage et commutation

Renseignements supplémentaires à recueillir

- Structure organisationnelle, objectifs de solutions, exigences commerciales, techniques et opérationnelles.
- Politique de sécurité, processus de gestion des incidents de sécurité et procédures de gestion des incidents.
- Documents de classification et de hiérarchisation des ressources.
- Renseignements et politiques sur le trafic normal et permissible du réseau.
- Documentation sur l'identification, la classification et la hiérarchisation des systèmes et des données essentiels.
- Rapports trimestriels d'analyses de vulnérabilité, qui comprennent des détails comme les ports d'écoute, la version des services et les bases de référence ponctuelles des vulnérabilités associées aux ressources essentielles, comme les serveurs et les applications logicielles.
- Situations ou emplacements du réseau où la saisie des paquets en entier n'est peut-être pas autorisée.
- Renseignements sur les stocks et exigences relatives à la topologie, noms des hôtes, adresses IP, chaînes SNMP, mots de passe et tout autre renseignement nécessaire pour activer ou intégrer les composants gérés.

Responsabilités de Cisco

Gestion de projets :

- Outre les responsabilités du chef de projet Cisco décrites dans les conditions générales des services opérationnels essentiels Cisco, le chef de projet devra effectuer ce qui suit :
    - Définir le flux de communication avec le commanditaire de projet et les principales parties prenantes.
    - Vérifier l'état des dépendances, les risques et les problèmes associés à une prestation réussie du service.
    - Agir comme interlocuteur principal pour les procédures de gestion du changement.

Première séance **:**

- Organiser la première séance dans les quarante-cinq (45) jours suivant la réception du bon de commande afin d'examiner le processus d'activation et les activités avec le client et de créer un plan de projet d'activation du service.
- Surveiller la transition et gérer les incidents des composants gérés :

Remarque : La collecte d'observations et la première séance doivent être achevées avant la prise en charge des responsabilités de la transition :

- Responsable du suivi des dossiers et du dépannage de la transition pour les technologies prises en charge, comme spécifiées dans le devis.
- Exécuter le plan de transition afin d'effectuer la transition du réseau existant du client vers la gestion des composants gérés par Cisco, ce qui inclut les responsabilités suivantes :
- Définir un champ d'application global et les étapes
- Définir les exigences de l'état de préparation, afin d'établir la connexion et l'accès aux composants gérés par Cisco.
- Définir les renseignements sur les stocks et les exigences relatives à la topologie nécessaires pour activer ou intégrer les composants gérés.
- Fixer la date de lancement à partir de laquelle Cisco commencera à gérer et surveiller les composants gérés et à laquelle le client pourra accéder au service.
- Mener une séance d'information de fin de transition à la fin des activités de la transition susmentionnée qui comprendra les éléments suivants :
    - Révision du processus d'escalade des incidents.
    - Recommandations en fonction des renseignements analysés auxquelles donner suite, s'il y a lieu.
    - La date de lancement du service de surveillance et de gestion des incidents par le HTTS ARC.

Surveillance et gestion des incidents des composants gérés **:**

- Le HTTS ARC est fourni à distance (pas sur site) et donne notamment au client un accès direct à l'équipe fédérale spéciale d'assistance sécurisée par un numéro de téléphone fourni par Cisco. Les objectifs de temps de réponse au client du HTTS ARC sont les suivants :
    - Appels de gravité 1 et 2 : objectif de réponse dans un délai de quinze (15) minutes.
    - Appels de gravité 3 et 4 : objectif de réponse dans un délai de soixante (60) minutes.

Remarque : Les temps de réponse ne visent pas les problèmes signalés à l'aide de Cisco.com ou de tout autre moyen de communication électronique.

- Fournir des services de suivi de dossiers et de dépannage, s'il y a lieu, vingt-quatre (24) heures sur vingt-quatre, sept (7) jours par semaine.
- Fournir un accès en tout temps à des spécialistes en ingénierie qui connaissent le réseau du client pour une résolution plus rapide des problèmes.
- Fournir un service d'assistance au niveau du réseau qui évalue les demandes de services au-delà du niveau des périphériques afin de déterminer et de prendre en charge les symptômes au niveau du réseau.
- Fournir un numéro sans frais dédié. Seuls le numéro de contrat de service et les renseignements de base du profil CCO du client lui seront demandés.
- Surveiller les composants gérés recensés dans le plan de transition.
- Traiter les incidents comme suit :
    - Créer des billets d'incident sur le portail client.

- Classifier chaque billet d'incident selon une version modifiée des catégories d'incidents du CERT américain trouvées ici :
- https://www.us-cert.gov/government-users/reporting-requirements
- Selon les informations connues par Cisco au moment de la création de l'incident, accorder une priorité élevée, moyenne ou faible à tous les incidents en fonction de plusieurs critères comme le type d'infection, la confirmation de l'incident ou le nombre de ressources touchées par l'incident. Les niveaux de priorités sont définis de la façon suivante :
  - Élevé : impact commercial critique ou perte de données pour le client.
  - Moyen : effet négatif pour le client, perte potentielle de données, perte potentielle de service.
  - Faible : effet négatif minime pour le client Pas de perte financière. Pas de perte de données.
- Aviser par voie électronique les interlocuteurs désignés par le client au sujet des nouveaux incidents.
- Fournir des recommandations d'atténuation selon leur disponibilité pour l'incident de sécurité associé.
- Si Cisco prend connaissance d'un incident, Cisco s'efforcera d'informer le point de contact désigné du client pour le service.

Livrables

- Plan de transition
- Séance d'information de fin de transition

Responsabilités du Client

- Collaborer avec le spécialiste en ingénierie de configuration de réseau de Cisco afin de créer les éléments suivants s'ils n'existent pas afin d'aider à la résolution de problèmes et à la mise en œuvre de solutions appropriées :
  - Carte topologique avec réseaux IP
  - Modèles de conception et de configuration
- Exécuter les tâches définies dans le plan de transition en soutien à l'activation du service.
- Fournir un accès électronique raisonnable au réseau du client pour que Cisco puisse fournir le service.
- Signaler directement les problèmes de niveau de gravité 1 et 2 à l'aide du numéro de téléphone fourni par Cisco.
- Examiner les billets d'incidents sur le portail client et fournir dans un délai raisonnable des renseignements pour la résolution et la clôture des billets.
- Mettre en œuvre des solutions d'atténuation recommandées par Cisco dans les meilleurs délais afin d'accélérer la résolution des incidents et d'améliorer la disponibilité de l'infrastructure opérationnelle essentielle du Client.

Définition des termes utilisés

- **Portail client** : application Web fournie au client par Cisco pour donner la meilleure des visibilités au service HTTS ARC, y compris les rapports et billets d'incidents.
- **Billets d'incident** : rapport énuméré contenant les détails d'un incident détecté par le HTTS ARC et nécessitant l'attention du client.
- **ISO** : Organisation internationale de normalisation
- **Incident de sécurité** ou **Incident** : série unique d'événements indésirables ou inattendus en matière de sécurité de l'information, présentant une probabilité importante de compromettre les opérations commerciales et de menacer la sécurité informatique (ISO 27035).

3. ATTÉNUATION DES MENACES

Le service d'atténuation des menaces fournit une aide en matière de préparation et de gestion des incidents.

NAV. SECT.

La section **Atténuation des menaces** comprend les capacités et les livrables de services suivants, qui sont tous marqués d'un signet pour faciliter la navigation :

3.1. Gestion des incidents de sécurité

Le service de gestion des incidents de sécurité est axé sur la préparation et la gestion des incidents à l'aide d'activités ciblées qui évaluent le processus de préparation et de gestion.

3.1.1. Service Conservation de la réponse aux incidents

Le service de conservation de gestion des incidents (IR) examine et évalue le programme de préparation aux incidents du client.

Architecture prise en charge

- Sécurité

Renseignements supplémentaires à recueillir

- Les renseignements sur la stratégie de gestion des incidents, y compris les processus et les flux de travail.

Responsabilités de Cisco

- Fournir un ou plusieurs des livrables de réponse aux incidents de sécurité suivants dans le cadre de la rétention :
- Évaluation de la préparation face aux incidents, stratégie de gestion des incidents et planification (par exemple, plans de gestion des incidents, manifestes), exercices sur table, chasse proactive aux menaces, évaluation de la compromission
- Les incidents d'urgence qui peuvent inclure le triage, la coordination, l'investigation (analyse et investigation, par exemple), le confinement et la correction.
- Fournir un accès d'urgence aux services de gestion des incidents pendant la période d'abonnement.
- Faire preuve d'efforts conformes aux usages du commerce pour a) affecter une ressource à distance par téléphone dans un délai de quatre (4) heures et b) commencer le déploiement de personnel sur le site du Client dans un délai de vingt-quatre (24) heures.
- Effectuer une mise à jour mensuelle de l'état de préparation du Client face aux incidents.

Livrables

Les livrables du service peuvent inclure une partie ou l'ensemble des éléments suivants :

- Rapport d'évaluation de l'état de préparation à la gestion des incidents
- Stratégie, plan et guide de gestion des incidents
- Rapport sur les exercices sur table
- Rapport sur la recherche proactive de menaces
- Rapport d'évaluation des compromissions
- Rapport d'intervention d'urgence en cas d'incident

Restrictions

Remarque : Les conditions générales des Services opérationnels essentiels Cisco – Responsabilités générales – Limitations spécifiques au service de rétention des réponses aux incidents de sécurité.

3.1.2. Amélioration de la conservation de la réponse aux incidents

Le service Amélioration de la conservation de la réponse aux incidents de sécurité (IR) est axé sur la préparation et la gestion des incidents à l'aide d'activités ciblées qui évaluent les capacités de prévention, de détection et de réponse aux incidents.

Architecture prise en charge

- Sécurité

Renseignements supplémentaires à recueillir

- Les renseignements sur la stratégie de gestion des incidents, y compris les processus et les flux de travail.

Responsabilités de Cisco

- Fournir un ou plusieurs des livrables de réponse aux incidents de sécurité suivants dans le cadre de l'amélioration de la rétention :
    - Évaluation de la préparation des incidents, stratégie de gestion des incidents et planification (par exemple, plans de gestion des incidents, manifestes), exercices de plateau, chasse aux menaces proactives, évaluation de la compromission,
    - Les incidents d'urgence qui peuvent inclure le triage, la coordination, l'investigation (notamment l'analyse et l'investigation), le confinement et la correction,
    - Évaluer les capacités de prévention et de détection des attaques par le client grâce à une évaluation de l'équipe Purple Team d'un appareil et d'un segment de réseau.
- Fournir un accès d'urgence aux services de gestion des incidents pendant la période d'abonnement.
- Faire preuve d'efforts conformes aux usages du commerce pour a) affecter une ressource à distance par téléphone dans un délai de quatre (4) heures et b) commencer le déploiement de personnel sur le site du Client dans un délai de vingt-quatre (24) heures.
- Effectuer une mise à jour mensuelle de l'état de préparation du Client face aux incidents.

Livrables

Les livrables du service peuvent inclure une partie ou l'ensemble des éléments suivants :

- Rapport d'évaluation de l'état de préparation à la gestion des incidents
- Stratégie, plan et guide de gestion des incidents
- Rapport sur les exercices sur table
- Rapport sur la recherche proactive de menaces
- Rapport d'évaluation des compromissions
- Rapport d'évaluation de l'équipe Purple Team
- Rapport d'intervention d'urgence en cas d'incident

Restrictions

Remarque : Les conditions générales des Services opérationnels essentiels Cisco – Responsabilités générales – Limitations spécifiques au service d'amélioration de rétention des réponses aux incidents de sécurité.

4. EXPERT EN OPÉRATIONS SUR PLACE

L'expert en opérations sur place fournit aux clients une assistance opérationnelle sur site en matière de gestion des incidents, et de gestion des problèmes, ainsi que de la consultation sur site pour les initiatives opérationnelles en matière de fiabilité, de sécurité, de performance et d'exploitation de l'infrastructure et des applications Cisco.

NAV. SECT.

La section **Expert en opérations sur place** comprend les capacités et les livrables de services suivants, qui sont tous marqués d'un signet pour faciliter la navigation :

4.1. Conseiller avisé

Le conseiller de confiance fournit du leadership pour permettre aux clients de bénéficier des Services opérationnels essentiels Cisco 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.

4.1.1. Service de consultation relative aux opérations sur place

Les services de consultation sur site sont fournis dans le lieu désigné par le client jusqu'à cinq (5) jours par semaine (en attente de 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
- Réseau de stockage
- Commutation de centres de données
- Infrastructure centrée sur les applications
- Orchestration et automatisation de centre de données
- Tetration
- Communications unifiées
- Collaboration vidéo
- Solution de collaboration hébergée
- Service à la clientèle
- Réunions et messagerie infonuagiques
- Sécurité de réseau
- Politique de sécurité et accès
- Sécurité du nuage
- Menace avancée
- Réseau central de transmission par paquets
- Politique de mobilité et accès
- 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
  - Systèmes informatiques
- WAN défini par logiciel
  - Routage et commutation
  - Gestion et orchestration de réseau
- Réseau central virtuel de transmission par paquets
  - 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

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 en appui à la planification, au séquencement et à 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 l'expert-conseil Cisco spécialiste en réseautique devront être régies selon le service et les livrables commandés par le client et elles sont soumises à l'approbation de Cisco, qui ne doit pas s'y opposer sans raison valable.

Produits livrables

Les livrables pris en charge par le service de consultation sur site se fondent sur les livrables des Services opérationnels essentiels Cisco pour les opérations qui sont précisés dans le devis des services commandés par le Client, qui peuvent comprendre les composants suivants :

Observations sur la plateforme	• Meilleures pratiques en matière de configuration • Étapes du cycle de vie du matériel • Analyse diagnostique • Avis de problème constaté • Vérification
Gestion du cycle de vie du logiciel	• Élaboration de procédures et de processus de gestion logicielle • Normes de version et d'analyse de logiciels • Conformité pour le suivi des logiciels • Étapes importantes du cycle de vie du logiciel • Évaluation de l'impact client pour les avis de sécurité du produit
Évaluation des technologies	• Évaluation de la résilience • Évaluation de la sécurité de la solution de collaboration • Évaluation de vérification des radiofréquences • Évaluation des radiofréquences de réseau local sans fil
Gestion des opérations	• Soutien technique en cas d'escalade
Gestion des connaissances	• Séance de transfert de connaissances pour les opérations
Gestion des instruments	• Examen des instruments de gestion • Évaluation de la planification et de la préparation du déploiement des outils de gestion

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.

4.1.2. Soutien aux opérations sur site

Le service d'assistance sur site est fourni dans un emplacement désigné par le client jusqu'à cinq (5) jours par semaine (selon les restrictions de travail locales).

Le service d'assistance sur site n'est offert que pour certains lieux géographiques et sera détaillé dans le devis des services.

Solutions prises en charge

- Cisco Expert Care

Responsabilités de Cisco

- Les responsabilités assumées par le service d'assistance sur site sont définies dans les livrables décrits ci-dessus.

Gestion des opérations	• Gestion des incidents • Gestion des problèmes – Ingénierie High-Touch

Remarque : Cisco peut juger nécessaire d'offrir les livrables dans une combinaison de services de soutien sur site et de soutien à distance.

Livrables

- Gestion des incidents liés au service d'assistance sur site
- Gestion des problèmes du service d'assistance sur site de l'ingénierie High-Touch

Remarque : Le devis spécifie les livrables achetés pour le service d'assistance sur site pour les opérations.

Responsabilités du client

- Donner à Cisco des directives au sujet des activités de soutien et des priorités pour lesquelles le client a besoin du service d'assistance de Cisco.