Services de gestion et de surveillance à distance pour la sécurité par Cisco

Présentation du produit

Les services de gestion à distance de la sécurité proposés par Cisco® (Cisco® Remote Management Services for Security : Cisco RMS for Security) permettent de gérer, de surveiller et de prévenir les attaques complexes, les programmes malveillants et les vulnérabilités des réseaux modernes, 24 h sur 24. Grâce à eux, vous n'aurez plus à vous soucier des tâches de gestion quotidiennes et votre personnel informatique pourra se concentrer sur les initiatives commerciales stratégiques.

Les services Cisco RMS for Security incluent la mise à disposition d'une équipe dédiée, composée d'informaticiens particulièrement compétents, qui fonctionne comme une extension de votre service informatique. À l'aide d'une méthodologie éprouvée et d'un processus basé sur l'ITIL®, l'équipe Cisco met en œuvre des solutions fiables pour assurer la continuité de votre activité. Nos clients gardent en permanence le contrôle sur leur propre réseau et ils disposent d'une parfaite visibilité sur la santé de leur réseau et sur l'avancement de notre travail grâce au portail Internet innovant Cisco RMS for Security.

Vue d’ensemble du service

Il est fondamental de prévenir et de corriger les problèmes de sécurité relatifs à votre réseau tout en conservant un niveau élevé de performance, de disponibilité et de fiabilité pour les ressources de votre entreprise. Bien entendu, il est également primordial de protéger la confidentialité et l'intégrité de vos données commerciales. Afin d'éviter la formation de brèches de sécurité pouvant occasionner des accès non autorisés à votre réseau (ou par lesquelles des membres de votre équipe pourraient, volontairement ou non, compromettre des ressources de votre entreprise), vous devez assurer une surveillance globale et continue, mais également gérer les incidents survenant sur l'ensemble de votre réseau. Cependant, il vous incombe d'affecter avec prudence vos ressources en termes de réseau et de sécurité. À l'heure où les organisations essaient d'anticiper chaque menace éventuelle, l'augmentation des coûts liés à la surveillance et à la gestion de leur sécurité peut empiéter sur les investissements nécessaires dans d'autres secteurs commerciaux. Heureusement, votre entreprise n'a pas à se soucier du développement ou de la maintenance d'un

système de gestion de la sécurité pour suivre l'évolution constante des menaces actuelles. En effet, vous pouvez déléguer les opérations quotidiennes de surveillance et de gestion de la sécurité à une équipe d'experts en sécurité certifiés selon les standards de l'industrie.

Cisco propose les meilleures pratiques de l'industrie en matière de correction des problèmes de sécurité. Ces pratiques sont issues de l'expérience que nous avons accumulée grâce à l'exploitation et à l'installation de nos solutions de sécurité, particulièrement dans les domaines de l'analyse et de la résolution de millions d'incidents de sécurité.

Les services de gestion à distance de la sécurité proposés par Cisco comprennent la gestion des incidents de sécurité, des problèmes, des modifications, de la configuration, des conflits de version et de la création de rapports pour les technologies de sécurité Cisco, et ce 24 h sur 24 et 7 jours sur 7. Les experts en sécurité Cisco surveillent en permanence l'environnement de votre réseau, de façon à maximiser le temps de fonctionnement et la valeur de votre infrastructure réseau et à rentabiliser votre investissement en matière de sécurité. Ils assurent également de façon plus efficace les processus de modification des commandes, de configuration et de gestion des versions. Ils améliorent la visibilité de votre stratégie de sécurité actuelle et permettent de dédier davantage de vos ressources informatiques à vos projets commerciaux stratégiques.

Cisco propose les meilleures pratiques de l'industrie en matière de correction des problèmes de sécurité. Ces pratiques sont issues de l'expérience que nous avons accumulée grâce à l'exploitation et à l'installation de nos solutions de sécurité, particulièrement dans les domaines de l'analyse et de la résolution de millions d'incidents de sécurité. Les ingénieurs en sécurité qui travaillent pour Cisco ont une excellente connaissance des produits et technologies de sécurité Cisco, notamment dans le domaine des technologies les plus récentes et les plus avancées telles que celles du produit Cisco Security Monitoring, Analysis and Response System (MARS). De plus, nos ingénieurs bénéficient d'une grande expérience en ce qui concerne l'exploitation avancée des pare-feux Cisco PIX®, des systèmes de détection des intrusions Cisco (Intrusion Detection System : IDS), des systèmes de prévention contre les intrusions Cisco (Intrusion Prevention Systems : IPS) , des solutions Cisco Adaptive Security Appliance (ASA), des routeurs à services intégrés Cisco (Integrated Services Routers : ISR), de Cisco Security Agent (CSA) et des outils de sécurité essentiels disponibles dans le logiciel Cisco IOS®. En outre, les ingénieurs en sécurité Cisco ont une parfaite maîtrise de la Bibliothèque pour l'infrastructure des technologies de l'information (Information Technology Infrastructure Library :ITIL®), ainsi que de tous les autres standards encadrant notre activité. Grâce à ces solides connaissances et expériences, l'équipe des services de gestion à distance de la sécurité Cisco constitue un précieux complément de votre personnel informatique. Elle assure une assistance opérationnelle de premier ordre 24 heures sur 24 et 7 jours sur 7, pour l'ensemble de vos technologies de sécurité Cisco.

Les services de gestion à distance de la sécurité Cisco comprennent :

- Les services de gestion des incidents, des problèmes et des modifications relatifs aux équipements de sécurité Cisco
- La surveillance en continu des incidents relatifs aux équipements de toutes marques.
- Des rapports complets

Le tableau n° 1 répertorie les exemples de services de surveillance et de gestion, ainsi que les éléments livrables. Les éléments livrables sont répertoriés en détail dans la description des services de gestion à distance de la sécurité Cisco.

Table 1. Services de surveillance et de gestion, et éléments livrables.

Services et éléments livrables	Description
Évaluation de la capacité de gestion	L'évaluation de la capacité de gestion est effectuée par les analystes de Cisco RMS Security afin de déterminer si l'ensemble des composants gérés fonctionne correctement avant de mettre en place la gestion de la transition. Tous les composants gérés doivent être configurés et déployés. Ils doivent fonctionner correctement avant la mise en œuvre des services de surveillance à distance pour la sécurité assurés par Cisco.
Gestion des incidents	La gestion des incidents est un processus ITIL® utilisé par Cisco RMS SOC pour identifier et hiérarchiser les incidents relatifs à la sécurité. Cisco RMS SOC surveillera activement les principaux événements et les seuils relatifs à la sécurité des composants gérés dans l'infrastructure réseau du client. Grâce à la détection et à la corrélation automatique, dès qu'un incident de sécurité a lieu, un ticket d'incident est créé et le client reçoit une notification par courrier électronique. Cette communication peut comporter des procédures de correction, lesquelles dépendent des services de sécurité nécessaires.

Services et éléments livrables	Description
Surveillance des incidents	La surveillance des incidents fait partie intégrante du service de gestion des incidents, lequel implique que le système de surveillance de sécurité Cisco indique les défauts, les dépassements de seuil de performance, ainsi que tout événement déclenchant un incident de sécurité. Activités : • Surveillance (24 h sur 24, tous les jours de l'année) des éléments gérables sur l'infrastructure de sécurité appliquée au réseau du client • Surveillance continue des défauts et incidents de performance (re: alerte) sur les composants gérés dans l'infrastructure de sécurité appliquée au réseau du client • Surveillance continue des défauts et incidents de performance (re: alerte) sur les composants gérés dans l'infrastructure de sécurité appliquée au réseau du client • Détection des incidents • Corrélation des incidents, le cas échéant • Corrélation des incidents avec IntelliShield, le cas échéant Élément(s) livrable(s) : • Incidents confirmés répertoriés dans la base de données de gestion de la configuration (Configuration Management Database : CMDB) de Cisco RMS
Enregistrement des incidents	L'enregistrement des incidents fait partie intégrante du service de gestion des incidents, lequel implique que le système de création de tickets Cisco collecte les données d'alarme / d'événement / de corrélation, leur associe des informations pertinentes sur la configuration de l'élément, puis créé un ticket d'incident. Activités : • Associer aux informations d'alarme les informations de configuration de l'élément à partir de Cisco ROS CMDB • Associer aux informations d'alarme les informations IntelliShield pertinentes à partir de Cisco IntelliShield Élément(s) livrable(s) : • Création d'un ticket d'incident • Publication du ticket d'incident en ligne via le portail afin que le client puisse consulter les opérations de traitement des tickets et leurs principales étapes
Notification des incidents	La notification des incidents fait partie intégrante du service de gestion des incidents, lequel implique que Cisco envoie par courrier électronique aux contacts définis par le client une notification pour les nouveaux incidents et les nouvelles étapes du processus de gestion des incidents. Les notifications électroniques sont envoyées à une adresse e-mail ou à un équipement permettant de recevoir des e-mails afin de communiquer le numéro du ticket d'incident. Le client (ou son fournisseur favori) peut à tout moment consulter le statut d'un incident, ainsi que des informations détaillées via le portail Internet Cisco RMS. Activités : • Notification électronique automatisée pour le ou les contacts spécifiques indiqués par le client lors du processus d'activation des services. • Application du profil de notification du client pour les étapes de création du ticket d'incident Élément(s) livrable(s) : • Envoi d'une notification électronique de ticket d'incident selon le profil de notification du client • Apparition des enregistrements de notification sur le ticket d'incident
Hiérarchie et classification des incidents	La hiérarchie et la classification des incidents fait partie intégrante du service de gestion des incidents, lequel implique que les incidents Cisco soient gérés selon le niveau de sévérité, comme il est décrit par le standard IT Infrastructure Library (ITIL®). Le niveau de sévérité dépend de nombreux facteurs, notamment des attributs de création de tickets prédéfinis tels que l'impact sur l'activité, le degré d'urgence et la valeur de la ressource (le cas échéant et s'ils ont été entrés dans la base de données de gestion de la configuration Cisco pendant la phase d'activation du service). Activités : • Classification automatique des incidents selon les catégories défaut, performance ou sécurité Élément(s) livrable(s) : • Hiérarchisation des incidents selon les attributs de la création de ticket

Services et éléments livrables	Description
Clôture de l'incident	La clôture de l'incident fait partie intégrante du service de gestion des incidents, lequel implique que l'incident soit clôturé selon les conditions de clôture d'incident établies lors du processus d'activation du service. Si l'incident se reproduit, un nouveau ticket d'incident sera créé pour refléter précisément la nature récurrente de l'incident et favoriser l'identification des problèmes. Selon leur fréquence, les incidents récurrents peuvent déclencher une requête de modification (Request For Change :RFC) recommandée par Cisco pour résoudre l'incident récurrent. Cet incident doit être résolu par le client . Activités : • L'incident a été clôturé automatiquement, conformément au processus d'activation du service. • Élément(s) livrable(s) : • Clôture automatiquement le ticket d'incident • Notification électronique pour cette étape d'événement de ticket d'incident, si le client l'a demandé.
Corrélation avancée d'événement de sécurité	Identifie les schémas suspects à partir de données corrélées multidimensionnelles améliorant la visibilité de votre sécurité en liant plusieurs activités de sécurité sur le réseau. Fonction de corrélation tout-en-un pour respecter les règles de plusieurs pays, corrélation de vulnérabilité, algorithmes statistiques avec corrélation historique permettant d'identifier les schémas d'attaque récurrents, les attaques lentes automatisées, les schémas d'événements anormaux et les menaces potentielles pour les ressources de grande valeur. Applique une logique conditionnelle pour identifier les scénarios d'attaques probables avec la possibilité de prendre en compte les événements passés pour améliorer la détection en temps réel des attaques actuelles et imminentes.
Portail accessible depuis Internet	Cisco fournit un portail en ligne afin que le client puisse consulter les tickets, les mesures de ticket et les rapports pour tous les composants gérés par les services de gestion à distance de la sécurité assurés par Cisco. Élément(s) livrable(s) : • Un identifiant de connexion au portail pour chaque employé autorisé par le client • Informations d'inventaire sur le portail (disponibilité selon le composant géré), notamment : • Description du système • Fournisseur maintenance • Type d'opération de maintenance et numéro de contrat • Numéro de série • Adresse IP • Informations sur le ticket d'incident et de requête de service sur le portail (selon disponibilité), notamment : • Numéro d'identification du ticket d'incident et de requête de service : le numéro de suivi attribué par Cisco SOC à chaque ticket • Date et heure d'ouverture du ticket d'incident et de requête de service : la date à laquelle le ticket a été ouvert • Description du ticket d'incident et de requête de service : une brève description du(es) incident(s) ou de la(es) requête(s) de service détaillé(e)(s) dans le ticket • Statut du ticket d'incident et de requête de service : le statut actuel du ticket tel qu'il est déterminé par la note la plus récente ajoutée au ticket • Site(s) affecté(s) : dans le ticket, l'emplacement des sites où les composants gérés sont affectés

Services de gestion

La plateforme Cisco RMS for Security offre une large gamme de services de gestion de la sécurité, comprenant une couverture complète des équipements de sécurité Cisco. Grâce à cette couverture complète, nos ingénieurs et analystes Cisco RMS for Security peuvent travailler en collaboration pour gérer davantage de déploiements de produits et solutions de sécurité Cisco, et donc favoriser l'efficacité, la continuité et la productivité de nos clients. Le tableau n° 2 répertorie les services de gestion des technologies de sécurité Cisco :

Table 2. Gestion des technologies de sécurité Cisco

Équipements Cisco pris en charge	
Systèmes Cisco de prévention contre les intrusions	* Capteurs Cisco IPS 42xx * Cisco AIP-SSM pour ASA 5500 Series Adaptive Security Appliances * Module de service de détection des intrusions (IDSM-2) Cisco Catalyst® 6500 * Cisco IOS IPS pour Routeurs à Services Intégrés * Module d'intégration avancée Cisco IPS pour Routeurs à Services Intégrés
Appliances de sécurité Cisco PIX 500	* Appliance Cisco PIX 5xx
Cisco ASA (Adaptive Security Appliance) 5500	* Cisco ASA 55xx
Routeurs à Services Intégrés prenant en charge le pare-feu Cisco IOS et le système de prévention contre les intrusions Cisco IOS (Intrusion Prevention System : IPS)	Gamme Cisco ISR : * 8xx * 18xx * 28xx * 38xx * 72xx * 73xx
Cisco VPN	* Cisco VPN 3xxx, ASA 55xx, PIX 5xx, gamme Cisco ISR
Cisco MARS	* Gamme Cisco MARS
Système de contrôle d'accès sécurisé Cisco (ACS)	* Cisco Secure ACS 4.0 et 5.0
Web Application Firewall	* Appliance Cisco ACE Web Application Firewall
Cisco Security Manager	* Cisco Security Manager
Moteur de configuration Cisco	* Moteur de configuration Cisco

La plateforme Cisco RMS for Security est conçue pour collecter et corréler des sources de données importantes comprenant les protocoles réseau, tels que Syslog et NetFlow, afin de proposer un aperçu plus complet du réseau du client.

La plateforme Cisco RMS for Security est conçue de façon à proposer des fonctions de surveillance et de gestion particulièrement robustes, ce qui permet à Cisco ROS de déployer une solution de sécurité gérée de façon plus holistique afin de protéger au mieux les réseaux de nos clients contre les attaques et les menaces émergentes.

Services de surveillance

Les réseaux évoluent en permanence. C'est pourquoi les choix technologiques sont fondés sur différents critères. De plus, la plupart des réseaux représentent un environnement hétérogène constitué de produits de sécurité issus de différents fournisseurs. La plateforme Cisco RMS for Security offre à nos clients une couverture plus diversifiée du dispositif de sécurité de leur réseau grâce à la surveillance des produits de sécurité issus des principaux fournisseurs. Le tableau 3 indique quelques-uns des produits pris en charge.

Table 3. Produits tiers

Équipements tiers pris en charge	
TippingPoint	* TippingPoint IPS 210E, 600E, 1200E, 2400E, 5000E, SMS
IBM/ISS	* Gamme IBM/ISS GX
CheckPoint	* Checkpoint UTM, VSX, IAS, SM
Juniper	* Juniper IDP, ISG, SRX, SSG, NSM

La possibilité de surveiller les produits issus de différents fournisseurs en plus des produits Cisco offre à nos clients un service plus complet robuste, qui permet de surveiller une plus grande partie du réseau et de stopper les activités malveillantes avant qu'elles n'affectent la continuité de votre

activité. Grâce à cette surveillance complète des technologies de sécurité issues de différents fournisseurs, nos clients bénéficient des avantages et de l'expertise d'une société unique offrant ses propres solutions de surveillance et de sécurité. De plus, la capacité de notre plateforme à surveiller en temps réel les produits des fournisseurs mentionnés ci-dessus donne à Cisco la flexibilité nécessaire pour étendre cette liste en fonction des besoins de nos clients.

Corrélation multiple et exploitation d'informations à la demande

Pour relever les défis auxquels les services informatiques modernes font face en matière de sécurité, Cisco RMS for Security permet d'exploiter des informations à la demande grâce aux données accumulées et corrélées. Sans un aperçu global et spécialisé des risques et des attaques, la capacité à réduire ces risques et à protéger le réseau, les données et la continuité de l'activité est largement diminuée. C'est pourquoi Cisco RMS for Security et ses experts SOC font partie d'un écosystème cohérent composé d'équipes, de produits et de technologie associés de façon à proposer des solutions concrètes adaptées aux dispositifs de sécurité de chacun de nos clients. Cette vision multi-dynamique de la sécurité est rendue possible par les sources collaboratives suivantes :

Cisco Security Intelligence Operations

Le service Cisco Security Intelligence Operations centralise les opérations de sécurité. Il est constitué d'un ensemble de données et de plusieurs équipes associées pour fournir des informations prêtes à l'emploi et des solutions concrètes pour prévenir les risques sur une échelle globale. Ces informations sont collectées et exploitées par un ensemble de moyens technologiques et humains. Le tableau n° 4 répertorie ces flux d'informations liées à la sécurité.

Table 4. Flux d'informations de sécurité

Équipe	Élément livrable
Équipe Cisco STAT	Test de vulnérabilité des équipements Cisco
Équipe Cisco Applied Intelligence (Exploitation des informations)	Rédaction de guides et de règles visant à limiter la vulnérabilité de la technologie Cisco IPS
Équipe Cisco IPS Signature Development (Développement des signatures IPS)	L'équipe d'ingénieurs qui développe et teste les signatures pour la technologie de prévention contre les intrusions de Cisco
Chercheurs Cisco	Une équipe de recherche qui analyse les activités hostiles sur le réseau telles qu'elles apparaissent globalement, et qui propose à nos clients des solutions pour limiter ces attaques malveillantes. Cette équipe est continuellement impliquée dans la recherche sur les botnets, l'identification des exploits (programmes malveillants visant à exploiter une faille de sécurité) de navigateur Internet, la découverte d'exploits de serveur de type « zero day » (disponible avant la protection adéquate), l'analyse de données SensorBase, l'analyse continue des programmes malveillants et l'analyse des vecteurs d'attaque sur proxy ouvert.
IntelliShield	Une équipe d'ingénieurs qui conçoit et publie des informations sur les menaces pour les équipements proposés par tous les fournisseurs afin de limiter le risque d'attaques malveillantes
SenderBase et SensorBase	Une technologie leader sur le marché, intégrée aux équipements de sécurisation du courrier électronique Cisco IronPort, ainsi qu'aux équipements de sécurité Cisco IPS, qui détecte et signale les menaces globales en temps réel, puis établit des rapports qui sont envoyés automatiquement au service Security Intelligence Operations de Cisco, assurant ainsi une protection globale contre les menaces rencontrées au niveau local.
Équipe Product Security Incident Response (PSIRT) de Cisco	Une équipe dédiée au niveau global qui est chargée de gérer la réception et le traitement des informations relatives aux vulnérabilités en termes de sécurité des produits et réseaux Cisco, ainsi que leur publication dans des rapports.
ROS Security Operations Center	L'équipe d'ingénieurs et d'analystes spécialisés dans la sécurité qui assure les services de sécurité Cisco RMS for Security services. Cette équipe d'experts en sécurité est chargée du déroulement de l'ensemble des services Cisco Security Intelligence Operations.

Fonctionnalités de corrélation multiple

Grâce à toutes les informations collectées par les services Cisco Security Intelligence Operations, la plateforme Cisco RMS for Security est capable d'assurer des fonctionnalités puissantes de

corrélation tout-en-un qui permettent d'identifier et de limiter avec plus de précision les menaces et les attaques. La corrélation est basée sur un moteur multidimensionnel dans lequel des règles sont créées, modifiées et affinées selon les évolutions des menaces et des attaques, mais également selon les informations globales mentionnées ci-dessus. Le tableau n° 5 répertorie ces moteurs de corrélation.

Table 5. Moteurs de corrélation

Moteur	Fonction
Corrélation basée sur une règle	Des règles constituées d'une ou plusieurs affirmations basées sur une série de conditions, de périodes et de règles permettant de réduire le nombre d'alarmes non pertinentes et d'améliorer le temps de réponse aux véritables attaques
Corrélation de vulnérabilité	Utilisée pour intégrer les données de vulnérabilité de façon à réduire le nombre d'alarmes non pertinentes
Corrélation statistique	Donne la possibilité d'analyser le comportement du réseau et d'identifier les menaces selon la sévérité et les schémas d'événements anormaux
Corrélation historique	Donne la possibilité d'identifier les schémas d'attaque répétitive et d'attaque lente automatisée pouvant être dissimulés parmi des millions d'événements de sécurité non traités

Plateforme d'applications de gestion de la sécurité Cisco

Pour finir, nous nous sommes assurés que dans la plateforme Cisco RMS for Security, les données sont collectées avant la corrélation et l'analyse à partir de toutes les sources gérées. C'est pourquoi, selon la conception et les schémas de trafic du réseau protégé par l'architecture de sécurité du client, nos services de surveillance et de gestion permettent à certains clients de bénéficier d'au moins une appliance ROS Management Application Platform (MAP) 3050. Les appliances MAP 3050 constituent une extension de Cisco ROS Data Communication Network (DCN) déployée sur le site du client pour collecter, corréler, compresser et transmettre à Cisco ROS DCN les données relatives aux événements de sécurité. De plus, un routeur de terminaison Cisco ROS VPN sera déployé sur le site du client afin de faciliter la gestion et la surveillance de la connectivité du réseau.

Avantages

Les services de gestion à distance de la sécurité Cisco comprennent des fonctionnalités de détection, d'analyse et de correction des événements de sécurité critiques. Ils vous aident ainsi à gérer la sécurité de votre réseau à moindre coût. Ces services sont inspirés des meilleures pratiques de l'industrie développées sur la base de l'exploitation de millions d'environnements de sécurité concrets, mais également à partir d'une collaboration étroite entre les différentes équipes Cisco responsables de la conception et du développement des produits de sécurité Cisco. Les services de gestion à distance de la sécurité Cisco aident votre organisation à :

Les services de gestion à distance de la sécurité Cisco comprennent des fonctionnalités de détection, d'analyse et de correction des événements de sécurité critiques. Ils vous aident ainsi à gérer la sécurité de votre réseau à moindre coût.

- Optimiser la valeur de vos investissements en matière de sécurité en garantissant le fonctionnement, la disponibilité et la mise à jour des principales configurations de sécurité modernes
- Concentrez vos ressources sur vos activités stratégiques en déléguant les opérations quotidiennes de surveillance et de gestion de la sécurité relatives à votre infrastructure informatique
- Réduisez vos investissements en capitaux et vos dépenses d'exploitation en réalisant des économies d'échelle sur vos processus de gestion des modifications, de la configuration et des versions logicielles avec l'aide d'une équipe disponible 24 h sur 24

Portail Internet Cisco RMS

Le portail Internet Cisco RMS for Security nous permet d'offrir à nos clients un service très pratique : un accès permanent à leurs services de sécurité gérés et la surveillance de leur réseau par les ingénieurs Cisco SOC. En effet, le portail Internet Cisco RMS for Security donne à nos clients la possibilité de contrôler « par-dessus notre épaule » les événements et les alarmes générés par leurs services gérés, ainsi que les rapports et les mesures prises par les ingénieurs et les analystes Cisco RMS for Security. Faisant partie intégrante du portail Internet Cisco RMS for Security, toute une série de rapports sont à votre disposition. Ils peuvent être utilisés par un responsable ou un ingénieur spécialisé dans la sécurité afin de compléter les informations dont nous avons besoin pour observer les tendances des incidents de sécurité et prendre des mesures rapides pour contrer une menace. Ces nouveaux rapports offrent un affichage en temps réel des risques de sécurité actuels ainsi qu'une indication des équipements à partir desquels ils ont été générés. Ces rapports sont les suivants :

- Rapports sur les attaques bloquées grâce à la prévention contre les intrusions
  Principales attaques bloquées par les signatures
  Principales attaques bloquées par les capteurs
  Principales attaques bloquées à la source
  Principales attaques bloquées à destination
  Catégories de signatures IPS
- Rapports de synthèse sur la prévention contre les intrusions
  Principales signatures renvoyées/sévérité relative aux signatures
  Principales sources d'attaques
  Principales destinations attaquées
  Synthèse de la sévérité des signatures par capteur
  Sévérité pour les principales signatures renvoyées
- Rapport de synthèse sur le pare-feu
  Nombre total de paquets refusés
  Principales adresses sources refusées
  Principales adresses de destination refusées
  Principaux protocoles refusés
  Principaux refus en raison du règlement de contrôle d'accès
- Rapports d'échec de l'authentification
  Principales tentatives échouées en raison de l'adresse source
  Principales tentatives d'authentification échouées en raison de l'adresse de destination
  Principaux échecs d'authentification en raison de l'équipement
  Principales tentatives échouées en raison du nom d'utilisateur
- Rapports de synthèse sur la bande passante
  Principales applications
  Principale Source/Destination

En communiquant cette liste exhaustive des rapports disponibles, Cisco RMS for Security permet aux clients de disposer de toutes les informations pertinentes afin de prendre les décisions qui s'imposent pour satisfaire en permanence les besoins en sécurité de son organisation.

Pourquoi choisir les services Cisco ?

Les services Cisco permettent de développer des réseaux et des applications assurant une collaboration plus efficace entre les personnes qui les utilisent. Dans un monde exigeant une meilleure intégration des individus, des informations et des idées, le réseau devient une plate-forme stratégique. Le réseau fonctionne mieux lorsque les services, associés aux produits, créent des solutions adaptées aux besoins et aux opportunités des entreprises.

L'approche exclusive de Cisco prenant en compte le cycle de vie des services (Cisco Lifecycle Services) définit les activités requises à chaque phase du cycle de vie du réseau pour offrir un service d'une qualité irréprochable. Grâce à une méthodologie fondée sur la collaboration et alliant les forces de Cisco, de notre réseau de partenaires expérimentés et de nos clients, nous pouvons atteindre d'excellents résultats.

Les services de gestion à distance de la sécurité Cisco prennent en charge le réseau Cisco Self-Defending Network, une solution architecturale conçue pour les environnements de sécurité en évolution constante. La sécurité est intégrée à tous les niveaux et, grâce à une approche par cycle de vie pour les services, les entreprises peuvent concevoir, mettre en œuvre, exploiter et optimiser des plates-formes réseau qui défendent les processus métier essentiels contre les attaques et les interruptions, protègent la confidentialité et permettent de contrôler la conformité aux réglementations et aux stratégies.

Disponibilité, commandes et autres informations

Informations sur les commandes de service de gestion

Le tableau n° 6 répertorie les informations sur les commandes de service de gestion.

Table 6. Informations sur les commandes de service de gestion

Description du produit	Référence du service
Gamme de services de gestion des incidents Cisco ASA	CON-ROSF-ASAMG
Gamme de services de gestion des incidents Cisco ASA Contournement de panne	CON-ROSF-ASAFO
Gamme de services de gestion des incidents Cisco ASA Contextes additionnels	CON-ROSF-ASACON
Gamme de services de gestion des incidents Cisco PIX	CON-ROSF-PIXMG
Gamme de services de gestion des incidents Cisco PIX Contournement de panne	CON-ROSF-PIXFO
Gamme de services de gestion des incidents Cisco PIX Contextes additionnels	CON-ROSF-PIXCON
Gamme de services de gestion des incidents Cisco ISR	CON-ROSF-ISRSECMG
Gamme de services de gestion des incidents Cisco IPS	CON-ROSF-IPSMG
Gamme de services de gestion des incidents Cisco IPS Contournement de panne	CON-ROSF-IPSFO
Gamme de services de gestion des incidents Cisco IPS Capteur virtuel supplémentaire	CON-ROSF-IPSVS
Service de gestion Cisco VPN	CON-ROSF-VPNMG
Service de gestion du système de contrôle d'accès sécurisé Cisco	CON-ROSF-ACSMG
Gamme de services de gestion Cisco MARS	CON-ROSF-MARSMG

Le tableau n° 7 répertorie les informations sur les commandes de service de surveillance.

Table 7. Informations sur les commandes de service de surveillance

Description du produit	Référence du service
Gamme de services de surveillance des incidents Cisco ASA	CON-ROSF-ASAMN
Gamme de services de surveillance des incidents Cisco PIX	CON-ROSF-PIXMN
Gamme de services de surveillance des incidents de sécurité Cisco ISR	CON-ROSF-ISRSECMN
Gamme de services de surveillance des incidents Cisco IPS	CON-ROSF-IPSMN
Service de surveillance du système de contrôle d'accès sécurisé Cisco	CON-ROSF-ACSMN
Gamme de services de surveillance Cisco MARS	CON-ROSF-MARSMN
Gamme de services de surveillance du pare-feu Juniper	CON-ROSF-JNPFWMN
Gamme de services de surveillance de Juniper IDP	CON-ROSF-JNPIDPMN
Service de surveillance de Juniper SSL VPN	CON-ROSF-JNPSSLMN
Service de surveillance de CheckPoint Firewall 1	CON-ROSF-CHPFWMN
Service de surveillance de CheckPoint VPN 1	CON-ROSF-CHPVPNMN
Service de surveillance de TippingPoint IPS	CON-ROSF-TIPMN
Service de surveillance de IBM ISS IPS	CON-ROSF-IBMISSMN

Plateformes d'applications gérées par Cisco Security

Le tableau 8 répertorie les plateformes d'applications gérées par Cisco Security.

Table 8. Plateformes d'applications gérées par Cisco Security

Description du produit	Référence du service
Security MAP 3050	CON-ROSF-SECMAP
Security MAP 3050 Capacity Rate	CON-ROSF-SECMAPCR
Service Security MAP 3050 yr2+	CON-ROSF-SECMAP2Y
Routeur filtrant de contrôle d'accès sécurisé – par équipement	ROS-RMS-IRScreen

Pour plus d'informations à propos des services de gestion à distance de la sécurité Cisco, visitez la page http://cisco.com/go/ros ou contactez votre responsable de compte Services Cisco. Pour plus d'informations sur le service Cisco Security Intelligence Operations, visitez la page http://cisco.com/security.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose Californie

Siège social en Asie
Cisco Systems (USA) Pte.
Singapour

Siège social en Europe
Cisco Systems International BV
Amsterdam. Pays-Bas

Cisco dispose de plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco à l'adresse **www.cisco.com/go/offices.**