Services Cisco du système de prévention des intrusions

Protégez vos périphériques Cisco® IPS (Intrusion Prevention System, système de prévention des intrusions) contre les menaces de sécurité actuelles avec un service complet qui inclut une assistance technique permanente, le remplacement du matériel, les mises à jour logicielles et des fichiers de signature, et des informations dynamiques sur les menaces globales.

Protégez votre réseau contre les menaces et les attaques malveillantes ou néfastes.

Cisco Services for IPS permet d'améliorer la continuité de l'activité en vous aidant à :

- protéger les informations confidentielles ;
- maximiser la disponibilité et la fiabilité du réseau ;
- contrôler les dépenses via une plus grande stabilité des opérations réseau ;
- minimiser les incidences économiques potentielles des interruptions d'activité ;
- limiter les risques via une veille sécuritaire.

Vue d'ensemble du service

Les attaques de sécurité peuvent être isolées et locales, organisées et globales. Le mode d'attaque peut sembler familier, comme pour les dénis de service, mais il pourrait aussi s'agir d'une menace hybride, plus sophistiquée et faisant appel à des techniques d'ingénierie sociale, ou même d'une menace invisible, telle que l'infection de sites Web légitimes. Les conséquences de brèches non détectées et non contenues dans la sécurité sont bien connues, et incluent des frais importants de réparation et de restauration, des pertes de chiffre d'affaires, la mise en danger et la perte de données vitales, l'interruption de l'activité et des préjudices portés à la réputation de votre entreprise.

Une stratégie de sécurité proactive permettra à votre réseau de se protéger et se défendre automatiquement contre les nouvelles menaces, quel que soit leur type ou leur origine. Cisco Services for IPS, associé à votre système Cisco IPS (Intrusion Prevention System, système de prévention des intrusions), joue l'un des rôles les plus importants au niveau de la réaction coordonnée du réseau en protégeant votre entreprise contre les nouvelles menaces situées à la périphérie du réseau et au-delà.

Cisco Services for IPS offre des mises à jour de protection et une veille globale permanentes pour les dernières menaces de sécurité, des mises à jour du logiciel système, l'assistance d'experts en réseau et sécurité, et des options avancées de remplacement du matériel. Avec Cisco Services for IPS, vous n'avez plus à vous demander si votre système de prévention des intrusions dispose des informations les plus récentes pour vous défendre contre les attaques provenant de menaces locales et globales. Cisco Services for IPS vous aide non seulement à réduire l'exposition au risque, mais aussi à renforcer la productivité du personnel interne chargé de la maintenance des systèmes de sécurité.

© 1992–2009 Cisco Systems, Inc. Tous droits réservés. Ce document de Cisco contient des informations publiques.

Une approche exhaustive des services de prévention des intrusions

Cisco Services for IPS inclut les éléments suivants :

- protection dynamique et accès aux informations de gestion des menaces :
  - mises à jour des signatures ;
  - mises à jour de corrélation globale et de réputation Cisco* ;
  - Cisco IntelliShield Search Access ;
  - Cisco IPS Threat Defense Bulletin ;
- mises à jour du système d'exploitation et du moteur IPS ;
- assistance technique 24 heures sur 24 ;
- outils et applications d'assistance Cisco.com ;
- remplacement matériel avancé avec options de temps de réponse plus rapide et sur site.

*Disponible sur des produits IPS spécifiques.

Services de protection dynamiques contre les menaces organisées

Cisco Security Intelligence Operations (SIO) permet l'identification, l'analyse et la correction des menaces pour offrir le plus haut niveau de sécurité aux clients Cisco. Le centre opérationnel de suivi des menaces de SIO emploie plus de 500 analystes en sécurité répartis sur cinq sites à travers le monde et qui se consacrent 24 heures sur 24, 7 jours sur 7 et 365 jours par an à l'identification des menaces. Ces ingénieurs analysent les modèles de trafic de Cisco SensorBase, le plus grand réseau de surveillance de trafic en temps réel au monde, génèrent pratiquement en temps réel des règles pour des services tels que la corrélation globale Cisco et publient des mises à jour de sécurité opportunes. Certains des moyens utilisés par Cisco Services for IPS pour fournir les informations et ressources opportunes dont vous avez besoin pour vous défendre de façon proactive contre les menaces vous sont présentés ci-après.

Mise à jour des signatures

La vue complète qu'a Cisco du paysage des menaces Internet permet de créer les nouveaux fichiers de signature indispensables pour protéger votre réseau contre les dernières menaces et vulnérabilités. Nos analystes et experts en menaces identifient les vulnérabilités et développent de nouveaux fichiers de signature ainsi que des mises à jour des fichiers existants pour les périphériques IPS. Cisco teste les protections existantes ainsi que les nouvelles par rapport à une bibliothèque sans cesse enrichie d'exploits validés. Les fichiers de signature sont testés de manière approfondie, à la fois en interne et en externe par nos partenaires en signatures, pour s'assurer de leur qualité.

Avec Cisco Services for IPS, votre périphérique IPS peut recevoir automatiquement des mises à jour des signatures pour contrôler les menaces et vulnérabilités émergentes et fournir une protection avant qu'elles n'affectent votre infrastructure. Les mises à jour des signatures sont généralement publiées une fois par semaine. Selon l'urgence de la vulnérabilité, le niveau de gravité des dommages potentiels et la crédibilité de la source, Cisco peut publier de nouvelles signatures dans les heures suivant la découverte de la menace. Les mises à jour peuvent être transmises de façon proactive à votre périphérique Cisco IPS ou gérées par votre équipe de sécurité.

Mises à jour de corrélation globale et de réputation

Cisco Services for IPS vous offre un accès à des fonctionnalités de protection dynamiques telles que les mises à jour de corrélation globale et de réputation, uniquement disponibles auprès de Cisco. Avec la corrélation globale, votre périphérique Cisco IPS reçoit tout au long de la journée des mises à jour globales des menaces de Cisco SIO, toutes les cinq minutes si nécessaire, permettant ainsi à votre périphérique Cisco IPS de bloquer deux fois plus d'activités malveillantes que les périphériques IPS reposant uniquement sur l'inspection et l'évaluation locales.

La corrélation globale consulte les informations globales se rapportant aux menaces dans le réseau Cisco SensorBase, qui reçoit en permanence des notifications de menaces en provenance de centaines de milliers de déploiements de sécurité Cisco IPS, de pare-feu, Web et de messagerie électronique du monde entier, associées à des centaines de flux d'informations de partenaires. Les algorithmes de corrélation globale complexes de Cisco, associés à des centaines d'analystes en sécurité, transforment ces données contextuelles en mises à jour de corrélation globale.

Les mises à jour de réputation sont utilisées conjointement avec la corrélation globale pour surveiller l'activité des expéditeurs et donner à ces derniers une note de réputation qui peut bloquer immédiatement les attaquants les plus redoutables.

Le Tableau 1 présente les fonctionnalités et les avantages de Cisco Services for IPS.

© 1992–2009 Cisco Systems, Inc. Tous droits réservés. Ce document de Cisco contient des informations publiques.

Tableau 1. Fonctionnalités et avantages de Cisco Services for IPS

Caractéristiques	Produits livrables	Avantages
· Mise à jour des signatures	· Accès à de nouveaux fichiers de signatures réseau et algorithmes de protection de couche réseau basés sur des fichiers pour une protection contre les attaques réseau. · Cisco fournit des mises à jour de signatures pour de nombreuses formes d'attaques dans les heures suivant l'identification de nouvelles menaces ou vulnérabilités. · Les nouvelles mises à jour de signatures sont généralement publiées au moins une fois par semaine, et les signatures critiques peuvent être publiées dans les heures suivant l'identification d'une vulnérabilité.	· Prend en charge le confinement immédiat des menaces et contribue à prévenir les risques de panne réseau ou de dégradation des performances. · Cisco Services for IPS est disponible pour les éléments suivants : – appliances Cisco IPS ; – lames pour les commutateurs Cisco Catalyst® 6500 et les routeurs à services intégrés ; – appliances de sécurité adaptables ; – routeurs à services intégrés avec IPS intégré dans le logiciel Cisco IOS.
· Mises à jour de corrélation globale et de réputation Cisco*	· Mises à jour en temps réel sur l'environnement de menaces global au-delà du périmètre. · Les informations de corrélation globale et de réputation sont mises à jour depuis le réseau Cisco SensorBase, toutes les cinq minutes si nécessaire.	· Détecte un nombre plus important de menaces, et ce de manière plus précoce et avec une plus grande précision, de façon à protéger les ressources critiques contre les attaques malveillantes. · Offre une visibilité par rapport aux attaques multipoint incluant les attaques en série, les robots récolteurs d'adresses, les attaques par programmes malveillants et les « darknets ». · Les mises à jour de corrélation globale et de réputation bloquent les attaquants connus avant qu'ils aient la possibilité de rechercher et d'attaquer les ressources critiques.
· Cisco IntelliShield Search Access	· Accès à la base de données Cisco IntelliShield Alert Manager pour une recherche détaillée des dernières menaces et vulnérabilités.	· Facilite vos efforts de gestion d'une infrastructure réseau sécurisée.
· Cisco IPS Threat Defense Bulletin	· Bulletin envoyé par e-mail et comportant des informations exhaustives sur les dernières menaces et vulnérabilités, ainsi que sur les protections Cisco IPS, et des informations opportunes sur les mises à jour et avis de produits, et un accès à une bibliothèque de recherches en matière de sécurité.	· Contribue à réduire les risques grâce à des notifications proactives et à des informations détaillées sur les menaces émergentes.
· Versions du système d'exploitation et du moteur IPS	· Fournit de nouvelles améliorations en matière de performances et une nouvelle fonctionnalité IPS au sein de l'ensemble de fonctionnalités sous licence, avec accès aux types suivants de versions du système d'exploitation de prévention des intrusions : – mises à jour de maintenance, correctifs d'ingénierie et service packs (par exemple 6.0 à 6.0.2) ; – mises à jour mineures (par exemple 6.0 à 6.1) ; – mises à jour majeures (par exemple 6.0 à 7.0).	· Contribue à la protection des investissements en rendant les nouvelles fonctions et fonctionnalités IPS disponibles pour améliorer la prévention des menaces réseau. · Améliore la sécurité globale du réseau ainsi que des ressources connectées au réseau, et l'intégrité des informations sensibles de l'entreprise, des employés et des clients.
· Assistance technique	· Fournit à votre personnel un accès distant aux ingénieurs de sécurité du centre d'assistance technique Cisco.	· Contribue à l'amélioration de la productivité et de l'efficacité opérationnelle du personnel.
· Outils et applications d'assistance Cisco.com	· Accès enregistré aux outils et applications de l'assistance technique sur Cisco.com.	· Assure une assistance 24 heures sur 24, 7 jours sur 7, dans le monde entier. · Aide à résoudre rapidement les problèmes connus et fournit des outils pour instituer et gérer votre relation avec Cisco.

© 1992–2009 Cisco Systems, Inc. Tous droits réservés. Ce document de Cisco contient des informations publiques.

Caractéristiques	Produits livrables	Avantages
· Remplacement matériel avancé	· Offre les options de remplacement avancé suivantes : – le jour ouvrable suivant ; – le même jour ouvrable, sous 4 heures, 5 jours par semaine ; – le même jour ouvrable, sous 2 ou 4 heures, 7 jours par semaine. · Des options de remplacement sur site, par un ingénieur, sont également disponibles pour les temps de réponse ci-dessus.	· Fournit des options flexibles pour le remplacement matériel avancé. · Contribue à maximiser la disponibilité pour garantir une protection continue contre les menaces.

* Les mises à jour de corrélation globale et de réputation Cisco sont disponibles sur les appliances Cisco IPS42xx, ASA 55xx avec modules IPS, modules IPS (IDSM-2) pour les commutateurs Cisco Catalyst, et modules AIM-IPS et NME-IPS pour les routeurs à services intégrés. La corrélation globale Cisco n'est actuellement pas disponible pour les périphériques basés sur le logiciel Cisco IOS (IPS sur logiciel Cisco IOS) ou ASA-5505-AIPS.

Disponibilité

Cisco Services for IPS est disponible dans le monde entier et peut être commandé auprès de votre représentant Cisco local ou d'un partenaire certifié Cisco. Pour rechercher un partenaire certifié Cisco dans votre région, utilisez l'outil Partner Locator, disponible à l'adresse www.cisco.com/go/partnerlocator. Pour obtenir une liste complète des services techniques disponibles pour vos produits et applications Cisco, utilisez notre outil de recherche de service, disponible à l'adresse www.cisco-servicefinder.com.

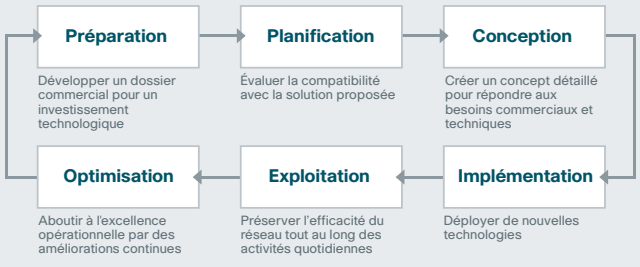
Pourquoi choisir les services Cisco ?

Cisco Services développe des réseaux et des applications permettant une collaboration plus efficace entre les personnes qui les utilisent. Cisco propose un ensemble complet de produits et services de sécurité afin de vous aider à éviter les interruptions d'activité. Cisco Services for IPS aide votre réseau à se défendre contre de nombreuses menaces et vous permet de réagir rapidement et efficacement en cas d'attaque. Que vous utilisiez la technologie IPS dans des routeurs ou commutateurs, ou que vous comptiez sur la protection transparente fournie par nos appliances de sécurité, Cisco fournit un grand nombre de périphériques de défense contre les menaces qui permettent d'identifier et d'éradiquer rapidement les menaces réseau.

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 son réseau de partenaires expérimentés et de ses clients, nous pouvons atteindre d'excellents résultats.

Approche Cisco par cycle de vie de services



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 son réseau de partenaires expérimentés et de ses clients, nous pouvons atteindre d'excellents résultats.

© 1992–2009 Cisco Systems, Inc. Tous droits réservés. Ce document de Cisco contient des informations publiques.

Informations complémentaires

Pour plus d'informations sur Cisco Services for IPS, visitez le site www.cisco.com/go/services/ips ou contactez votre représentant local.

Pour plus d'informations sur les services techniques Cisco, visitez le site www.cisco.com/go/ts.

Services Cisco

Making Networks Work.
Better Together.

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

Siège social en Asie
Cisco Systems (USA) Pte. Ltd.
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 et les numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco à l'adresse **www.cisco.com/go/offices.**

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, le logo Cisco, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra et Welcome to the Human Network sont des marques commerciales ; Changing the Way We Work, Live, Play, and Learn, Cisco Store et Flip Gift Care sont des marques de service ; Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, le logo IronPort, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx et le logo WebEx sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques commerciales mentionnées dans ce document ou sur le site Web sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (0907R)

C78-554808-00 08/09

© 1992–2009 Cisco Systems, Inc. Tous droits réservés. Ce document de Cisco contient des informations publiques.