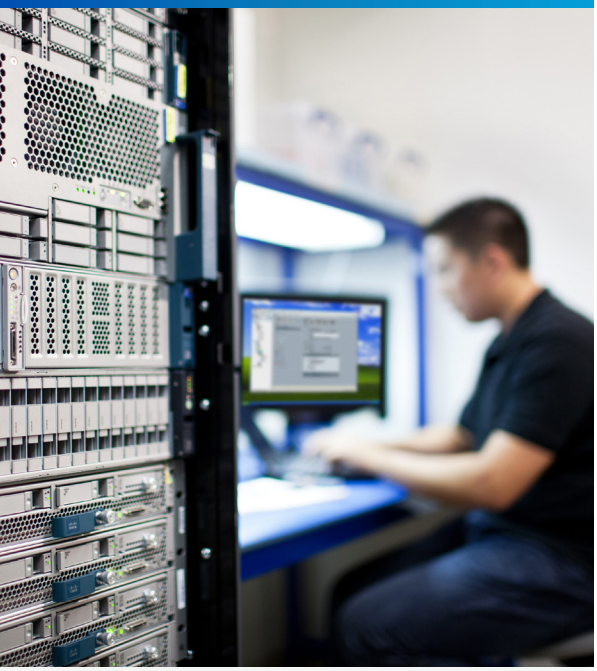
Gestion des menaces



Des Avantages :

- **Renforcement de la position de sécurité** par l'intermédiaire d'une démarche exhaustive traitant à la fois la préparation et la réaction
- **Confiance accrue dans les protections continues** grâce à une méthodologie établie, un savoir unique et une équipe chevronnée
- **Meilleure visibilité** et compréhension plus approfondie de vos opérations et de votre infrastructure grâce à l'utilisation de technologies innovantes et d'analyses complètes effectuées en continu par des experts

Service d'intervention pour les incidents liés à la sécurité de Cisco

Aperçu des menaces dynamiques actuelles

Les entreprises sont soumises à des attaques de différentes provenances. En 2014, les atteintes à la sécurité ont coûté près de 500 G$, selon IDC. Pendant ce temps, il y a une pénurie mondiale de professionnels de la sécurité, alors qu'un million de nouveaux postes demeurent vacants, selon le Rapport annuel sur la sécurité de Cisco de 2015. Cette pénurie de talents, combinée à une augmentation des incidents, a entraîné une position de sécurité généralement faible dans la plupart des entreprises. Des attaques réussies provoquent d'énormes pertes financières, la perte de propriété intellectuelle, la mise en danger des renseignements et de la confiance des clients, et une diminution de la valeur de l'entreprise.

Le Service d'intervention pour les incidents liés à la sécurité de Cisco[MD] renforce considérablement vos défenses de réseau et de sécurité des renseignements. Tirant profit des plus récentes connaissances et des pratiques exemplaires, il fait fonctionner toutes les couches de défense et fournit une gamme complète de moyens pour aider les structures à se préparer aux incidents, à les gérer, à y réagir et à s'en remettre plus rapidement et de façon plus efficace.

Seuls 50 % des responsables de la sécurité des systèmes d'information s'accordent à dire qu'« il est facile de déterminer l'étendue d'un danger, de le contenir et d'y remédier »

(Rapport annuel 2015 sur la sécurité de Cisco)

Position de sécurité renforcée grâce à la préparation et la réponse

Le service de réponse aux incidents liés à la sécurité de Cisco est une solution intégrée aux services de sécurité et de consultation de Cisco qui fournit l'expertise pour évaluer et concevoir une démarche de sécurité capable de stimuler la croissance de l'entreprise, de réduire les coûts et d'atténuer les risques. En synthétisant les meilleures pratiques et en utilisant des cadres de sécurité efficaces développés par le secteur, l'équipe responsable de traiter les incidents de Cisco offre une gamme complète de fonctionnalités qui permettent de venir en aide aux entreprises. Notre équipe responsable de traiter les incidents se compose d'experts en sécurité des données provenant de différents milieux, comme la police, la sécurité d'entreprise et la sécurité technologique. Notre équipe travaille directement avec le groupe de Renseignements collectifs sur la sécurité (CSI) pour préciser les menaces connues ou non, mesurer les risques et les classer par ordre de priorité et réduire les risques futurs.

Laissez nos experts travailler avec vous afin de développer un nouveau programme, réévaluer les programmes existants ou fournir une assistance rapide lorsqu'une attaque survient.

© Cisco ou ses filiales, 2015. Tous droits réservés.

Composants du service de réponse aux incidents liés à la sécurité de Cisco

Préparation : services proactifs

- **Évaluation de l'état de préparation dans le cas d'une intrusion dans l'infrastructure :** En évaluant la conception réseau, les contrôles de sécurité, les systèmes d'exploitation, la configuration de la sécurité du personnel, les systèmes de correctifs, les pare-feux, la journalisation et les autres systèmes liés, Cisco parvient à comprendre de façon plus approfondie l'environnement du client et est capable de prédire les vecteurs d'attaques potentielles et de recommander les contrôles de sécurité nécessaires.
- **Évaluation des opérations de préparation en matière de sécurité :** Par le biais d'une évaluation de la préparation de votre équipe de sécurité, en fonction des incidents antérieurs et des rôles et responsabilités actuels, Cisco vérifie que votre organisation possède les ressources, les connaissances et les outils nécessaires pour différents types d'enquêtes et formule des recommandations.
- **Évaluation des opérations de préparation :** Les recommandations faites en prévision de futurs événements sont présentées par le biais d'une évaluation de votre modèle d'exploitation et de vos activités.
- **Évaluation des intrusions dans les communications :** Cisco fournit de l'assistance en construisant un cadre de communication qui comprend une structure de conformité appropriée pour une prise de conscience et une réaction coordonnées de la direction, de l'ensemble de la chaîne d'approvisionnement de l'organisation et de façon externe avec les clients.
- **Opérations de sécurité et formation d'intervention d'urgence :** Une formation est assurée en ce qui a trait aux dernières compétences à acquérir afin de guider, coordonner et traiter un incident. En outre, une formation technique est offerte au personnel du service de sécurité pour l'analyse des programmes malveillants et des différents outils de sécurité.

Réponse : services réactifs

- **Évaluation et enquête :** Détermine la méthode d'attaque et décompose le code malveillant, notamment sa trajectoire, sa destination et son objectif final, par l'intermédiaire d'une analyse technique du ou des systèmes infectés.
- **Développement de contre-mesures :** Développe des contre-mesures afin d'aider à détecter, mettre en quarantaine, suivre et empêcher toute action supplémentaire de la personne malveillante. Ces mesures peuvent fournir des indicateurs du niveau de compromission, de fuite de renseignements et d'exploitation de vulnérabilités.
- **Déploiement de contre-mesures :** Déploie toutes les contre-mesures qui ont été développées pour aider à détecter les incidents et à y mettre un terme, créées dans le respect de la sécurité des renseignements et des meilleures pratiques des fournisseurs.
- **Validation des contre-mesures :** Valide l'efficacité des contre-mesures nouvellement déployées et effectue une analyse de performance de toute amélioration de la conception nécessaire. Les résultats, comprenant de la documentation destinée à la direction, aux organismes de régulation et aux autorités, détaillent les faits de l'attaque, son atténuation, et les pertes ensuivies, le cas échéant.

L'intervention d'urgence de Cisco peut inclure une ou plusieurs des options suivantes afin d'isoler et de corriger une attaque :

- évaluation des sources de journaux;
- analyse et exploitation de données;
- analyse d'images d'expertise;
- surveillance dynamique des systèmes infectés;
- rétroingénierie des logiciels malveillants;
- analyse d'exploitation et nouvelle implémentation.

Prochaines étapes

Rendez-vous sur www.cisco.com/go/securityservices pour communiquer avec nos conseillers et protéger votre entreprise dès aujourd'hui.

© Cisco ou ses filiales, 2015. Tous droits réservés. Cisco et le logo Cisco sont des marques de commerce ou marques de commerce déposées de Cisco ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques de commerce de Cisco, rendez-vous à l'adresse : www.cisco.com/go/trademarks. Les autres marques de commerce mentionnées appartiennent à leur détenteur respectif. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et une autre entreprise. (1110R)

DEC14CS4667 08/15