

Symantec™ DeepSight™ Threat Management System

Protection des réseaux contre les menaces grâce au système de sécurité d'alertes en temps réel

La technologie de sécurité des environnements en réseau actuels n'est pas suffisante pour protéger les ressources de l'entreprise contre les vulnérabilités et les menaces émergentes. Les utilisateurs, les processus, les informations et la technologie doivent fonctionner en parfaite symbiose pour garantir une sécurité performante. Faisant partie d'un programme de sécurité d'entreprise efficace, SYMANTEC DEEPSIGHT THREAT MANAGEMENT SYSTEM renforce la sécurité en déclenchant des alertes en temps réel en cas d'attaques, de menaces éventuelles et de nouvelles vulnérabilités, permettant ainsi aux administrateurs de prévoir et d'évaluer les risques avec plus de précision. Grâce aux alertes personnalisées et à une analyse détaillée des menaces, des évaluations pertinentes et une aide à la prise de décision, cette solution représente l'un des systèmes d'alertes en temps réel leader du marché pour détecter les attaques au niveau mondial.

> De la sensibilisation à l'action

Symantec DeepSight Threat Management System rassemble et corrèle en permanence des données sur les attaques provenant des systèmes de sécurité de plus de 19 000 partenaires, ainsi que d'autres sources confidentielles et publiques regroupées dans plus de 180 pays dans le monde entier. Les spécialistes de Symantec mettent à profit leurs différentes relations dans le monde de l'industrie pour conserver une trace des dernières techniques d'attaques. Les experts de Symantec analysent les informations sur les menaces pour identifier les attaques actives et fournir des analyses complètes basées sur la configuration du réseau d'un environnement d'entreprise spécifique.

> Prévention des attaques grâce à des informations à jour

Grâce aux alertes avancées fournies avant que toute attaque n'atteigne l'entreprise, le système permet aux administrateurs de prendre des mesures proactives pour protéger leur infrastructure et éviter les périodes d'indisponibilité du réseau, la perte de productivité ou de nuire à la réputation de l'entreprise. Grâce aux alertes automatisées et hiérarchisées et au Web, le système fournit des informations détaillées et statistiquement fiables sur les attaques qui permettent d'effectuer un suivi par heure, pays, entreprise, etc. Les correctifs, les contre-mesures, les solutions de contournement et d'autres sources de référence sont également proposées, permettant ainsi de réagir immédiatement.

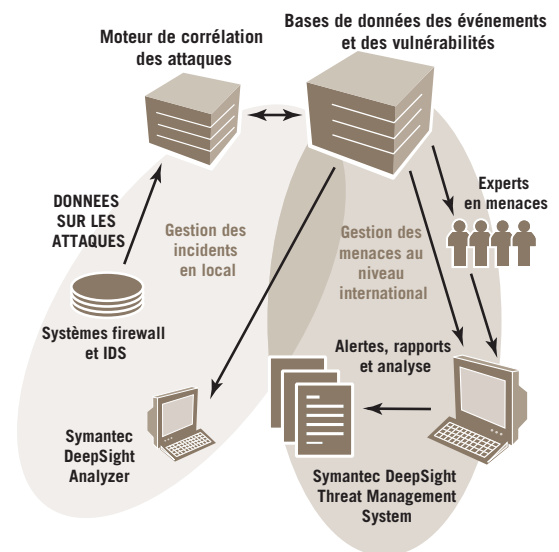
> Optimisation des ressources de sécurité grâce à la protection des alertes en temps réel

Grâce à DeepSight Threat Management System, les départements informatiques peuvent concentrer leurs ressources sur la prévention des attaques. En exploitant la réactivité et les informations proactives, les entreprises peuvent déployer des contre-mesures spécifiques pour empêcher les menaces de frapper leur propre réseau. En vous évitant de passer des heures à glaner des informations sur des centaines de sites Web et dans les courriers électroniques pour rassembler des renseignements, ce système optimise les ressources informatiques tout en garantissant le bon fonctionnement de vos activités.

Symantec DeepSight Threat Management System est un service d'alertes Web qui fournit des alertes en temps réel en cas d'attaques réseau. Symantec Event Database, l'application principale, rassemble et corrèle les données des firewalls et des solutions IDS des partenaires. Les données des firewalls étendent les fonctions d'alertes en temps réel en collectant des données sur les menaces connues et inconnues ; tandis que les données des solutions IDS fournissent des informations détaillées sur les attaques. Symantec utilise ces données collectées pour fournir un aperçu global des informations sur les attaques dans tout le système. Grâce à la console Web sécurisée, le système fournit des analyses personnalisées sur les menaces, incluant des alertes, des rapports et des déclencheurs. Les alertes sont envoyées directement à l'administrateur responsable des technologies spécifiques par courrier électronique, par fax, par message SMS ou par message vocal.

PRINCIPALES FONCTIONNALITES

- > Les alertes détaillées fournissent des informations en temps réel sur les incidents de sécurité collectés auprès de milliers de sources exclusives et de sondes d'attaques dans le monde entier
- > Les informations optimisent la structuration, l'affectation et le déploiement des ressources et du personnel de sécurité
- > La personnalisation complète permet aux administrateurs de configurer les alertes et les rapports automatisés pour répondre aux besoins de leur infrastructure informatique unique
- > Les fonctions puissantes de rapport et de suivi permettent de quantifier le retour sur investissement en matière de sécurité pour la répartition des ressources et la justification des dépenses
- > Supporté par Symantec™ Security Response, l'équipe mondiale d'intervention et de recherche en matière de sécurité, disposant des compétences nécessaires pour répondre aux besoins de votre entreprise



Architecture de Symantec DeepSight Threat Management System

➤ Une solution complète basée sur des statistiques pertinentes

Les experts de Symantec utilisent des techniques sophistiquées et l'exploration des données pour détecter les modèles de données indiquant le déclenchement d'une attaque. En fonction du profil des vulnérabilités et des attaques, ils génèrent des alertes et des rapports détaillés et pertinents.

➤ Alertes configurables

Les alertes de code malveillant et de menaces sont envoyées dans l'heure suivant la découverte d'une activité anormale ou d'un comportement hostile. Ces alertes contiennent des explications techniques détaillées, ainsi que des solutions de contournement ou des correctifs. Elles peuvent être rapidement personnalisées pour s'adapter aux configurations spécifiques des réseaux, des systèmes et des logiciels dans un environnement d'entreprise. Par ailleurs, vous pouvez définir des déclencheurs pour réagir en cas d'activités intenses sur une technologie, un port, une entreprise ou un type d'attaque. Ceux-ci génèrent ensuite des alertes et des rapports en cas de développement d'attaques.

➤ Rapports complets et personnalisables

Les rapports sur les analyses des menaces fournissent des explications détaillées sur les attaques, leur origine, la propagation, les facteurs d'atténuation et la prévention. Destinés aux spécialistes de la sécurité et aux dirigeants, les résumés quotidiens, hebdomadaires et mensuels décrivent les attaques, les vulnérabilités et les tendances au cours de la période d'évaluation. Les administrateurs peuvent facilement mener leur propre analyse pour examiner les catégories d'attaques ou visualiser les paramètres détaillés. Plus de vingt rapports différents couvrant une multitude de paramètres et des modèles peuvent être utilisés pour une programmation automatique.

➤ Internet en un clin d'œil

Pour obtenir un résumé en ligne sur l'état d'Internet, Symantec DeepSight Threat Management System génère en permanence une page récapitulative sur les événements de firewall et IDS. Sur une seule page, les administrateurs peuvent visualiser des informations détaillées sur différents types d'attaques actifs, y compris les activités intenses, les pays, les fournisseurs d'accès à Internet, les adresses IP, les ports, les produits, etc. En outre, la page Symantec Analyse Watch vous ouvre une fenêtre sur le monde des spécialistes de Symantec, soulignant rapidement les points sensibles éventuels que nos experts identifient comme les plus dangereux.

➤ Supporté par Symantec Security Response

Pour bénéficier d'une protection intelligente, appropriée et permanente, Symantec DeepSight Threat Management System est supporté par Symantec Security Response, l'équipe mondiale d'intervention et de recherche sur la sécurité. Elle apporte des réponses globales et rapides lors de l'apparition de nouveaux virus et mène des recherches proactives sur les menaces à venir.

Solutions d'alertes en temps réel de Symantec – une approche proactive de la sécurité

- Les solutions d'alertes en temps réel de Symantec avertissent les entreprises en temps réel pour leur permettre de mieux protéger leurs ressources stratégiques. En les avertissant de nouvelles menaces potentielles dès leur identification, par le biais d'informations pertinentes et détaillées, Symantec DeepSight Alert Services aide les administrateurs à remédier aux vulnérabilités avant qu'elles ne puissent être exploitées, et permet de protéger les systèmes contre les codes malveillants avant qu'ils ne frappent. Pour prévenir les entreprises en temps réel d'une menace potentielle, Symantec DeepSight Threat Management System suit les événements de sécurité dans le monde entier, envoyant ainsi une alerte dès qu'une menace active se développe. Symantec DeepSight Threat Management System permet aux administrateurs de mieux évaluer les menaces et de réagir en fonction des informations reçues grâce à une meilleure compréhension des risques de l'entreprise. Pour plus d'informations, visitez le site <http://www.symantec.fr>.

LES SOLUTIONS D'ALERTE EN TEMPS REEL CONSTITUENT DES COMPOSANTS CLES DE SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY ASSOCIE DES TECHNOLOGIES DE NIVEAU MONDIAL, DES SERVICES COMPLETS ET DES EQUIPES D'INTERVENTION D'URGENCE DANS LE MONDE ENTIER POUR AIDER LES ENTREPRISES A FONCTIONNER DE MANIERE FIABLE ET SECURISEE.

CONFIGURATION REQUISE

- Navigateurs :
 - Microsoft Internet Explorer versions 5.5+
 - Netscape Navigator versions 6.x+
- Les fonctions suivantes du navigateur doivent être activées :
 - Cookies
 - JavaScript
 - SSL

- Adobe Acrobat Reader 4.0 ou supérieur pour visualiser les alertes et les rapports
- Une adresse électronique pour recevoir les rapports et les alertes

SIEGE INTERNATIONAL
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
Tél. : +1.408.253.9600
Fax : +1.800.441.7234

BUREAU FRANCAIS
Symantec France
Immeuble River Seine
25 Quai Gallieni
92150 Suresnes
France
Tél. : +33 (0) 1 41 38 57 00
Service Clientèle Entreprise
Tél. : +33 (0) 1 70 20 00 00
www.symantec.fr

BUREAU SUISSE
Symantec Switzerland AG
Grindelstrasse 6
8303 Bassersdorf
Switzerland
Tel. +41-1-838 49 00
www.symantec.com

Pour plus d'infos sur le Service Clientèle et le Support technique, visitez le site www.symantec.com/eusupport/