



Symantec™ DeepSight™ Threat Management System

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

CONTENU

- > Les risques croissants des entreprises
- > Symantec DeepSight Threat Management System : un système global d'alertes en temps réel
- > Avantages de la sécurité proactive

Sommaire

Introduction	1
Les risques croissants des entreprises	1
La sécurité proactive : informations, expertise et configuration	2
Symantec DeepSight Threat Management System : un système global d'alertes en temps réel	3
Fonctionnement de Symantec DeepSight Threat Management System	6
Symantec DeepSight Threat Management System en action	7
Avantages de la sécurité proactive	9
Conclusion	9
Glossaire	10

> Introduction

Symantec DeepSight Threat Management System est un système d'alertes en temps réel personnalisable et complet qui fournit des notifications en cas d'attaques globales et des contre-mesures pour bloquer les attaques avant qu'elles n'atteignent l'entreprise.

Au cours de ces dernières années, les systèmes informatiques ont enregistré une augmentation considérable des intrusions, des attaques par déni de service, des vers, des menaces complexes et d'autres attaques. En réponse à cette situation, les entreprises ont été contraintes d'adopter une approche plus stratégique vis-à-vis de la sécurité du réseau qui consiste à collecter, analyser et réagir systématiquement en fonction d'informations détaillées sur les risques et les vulnérabilités. Les systèmes de détection d'intrusion (IDS) représentent une arme stratégique dans la lutte contre les attaques réseau. Toutefois, jusqu'à présent, leur utilisation a été largement réactive. Les experts en sécurité réseau sont souvent tellement occupés à tenter d'analyser leur réseau avant le déclenchement d'une attaque et à résoudre les problèmes qu'ils ont rarement le temps ou les ressources nécessaires pour anticiper l'attaque suivante. Les pare-feu permettent également de renforcer la protection contre les attaques. Toutefois, ils sont beaucoup plus efficaces lorsqu'ils sont correctement configurés pour bloquer le trafic malveillant. Pour les administrateurs, le défi consiste à savoir à quoi ressemblent les nouvelles attaques afin de pouvoir prendre les mesures appropriées pour sécuriser leur système et ce, tout en continuant à poursuivre leurs activités.

Ce document décrit comment Symantec DeepSight Threat Management System fournit des informations pertinentes, personnalisées et proactives, provenant des experts en sécurité de Symantec qui suivent l'évolution des attaques ciblées sur les entreprises dans le monde entier. Grâce à Symantec DeepSight Threat Management System, les entreprises peuvent affiner leurs stratégies de sécurité, réduire le temps passé à rechercher et à dépister les événements de sécurité, analyser les éléments clés des incidents et les statistiques des attaques pour permettre aux experts en sécurité de prendre des décisions avisées avant le déclenchement d'une attaque.

> Les risques croissants des entreprises

Le développement phénoménal d'Internet a entraîné une explosion du nombre de menaces de sécurité. Comme l'illustre la Figure 1, le CERT (Computer Emergency Response Team)/CC, l'un des plus importants centres de rapports chargés du suivi des problèmes de sécurité Internet, a enregistré une croissance rapide de chaque catégorie d'incident, notamment :

- Les tentatives d'accès non autorisé à un système ou à ses données
- Les interruptions indésirables ou le déni de service
- L'utilisation non autorisée d'un système pour le traitement ou le stockage des données
- Les modifications des caractéristiques du matériel, des microprogrammes ou des logiciels, à l'insu ou sans le consentement du propriétaire¹

Mais le problème ne se situe pas uniquement au niveau du nombre croissant de ces menaces. Alors que les entreprises du monde entier, quel que soit leur secteur économique, s'appuient de plus en plus souvent sur Internet pour gérer et développer leurs activités, chaque attaque, avec ses éventuels effets perturbateurs et impacts économiques négatifs, est susceptible d'être plus virulente. En 2002, la perte moyenne par incident externe a atteint 226 000 dollars.²

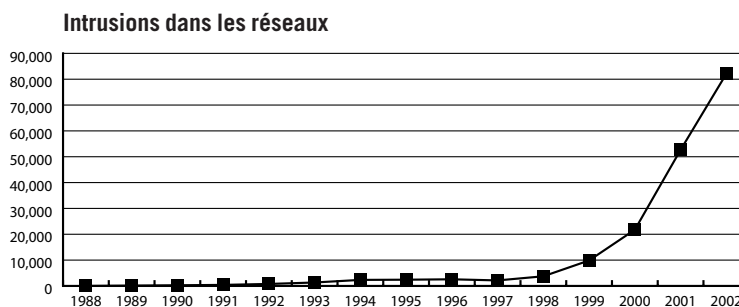


Figure 1. Le nombre d'incidents de sécurité dans les réseaux a augmenté parallèlement au développement phénoménal d'Internet (source : CERT/CC).

1. Source : CERT Coordination Center Incident Reporting Guidelines. Copyright © 1998, 1999, 2000, 2001, 2002 Carnegie Mellon University.
2. Source : Computer Security Institute/Federal Bureau of Investigation 2002 Computer Crime and Security Survey

En raison du nombre croissant d'attaques réseau et de leur coût potentiel élevé, les entreprises se rendent compte qu'elles doivent rassembler toutes leurs ressources pour se protéger contre les intrus. Pour de nombreuses entreprises, la première ligne de défense consiste à renforcer la protection autour de leurs ressources informatiques, en installant différents mécanismes de sécurité physiques et logiques. Les outils et techniques des éventuels intrus étant de plus en plus sophistiqués, les produits de sécurité doivent également l'être. Désormais, les entreprises réalisent qu'il est essentiel de se doter d'un système d'alertes en temps réel qui puisse gérer de manière proactive les menaces et les vulnérabilités pour optimiser leur stratégie de sécurité. Les meilleures équipes de sécurité de l'information en entreprise ont besoin d'informations pertinentes, complètes, précises et spécifiques aux configurations, sur les risques, les vulnérabilités et la pathologie des attaques. Les responsables informatiques doivent bénéficier d'un système de gestion de menaces afin d'être en mesure de prendre des décisions rapides, précises et censées pour protéger leurs systèmes.

> **La sécurité proactive : informations, expertise et configuration**

Pour développer une stratégie de gestion des menaces efficace, les experts en sécurité doivent collecter et analyser un grand nombre d'informations générales sur la sécurité, issues de plusieurs sources, notamment les alertes de virus et de vulnérabilités, les carnets d'adresses, les articles de presse et les fournisseurs de services d'infogérance sécurité. De nombreux systèmes et services ont été créés pour aider les spécialistes informatiques à détecter, gérer et réagir en fonction de ces informations. Les systèmes de détection d'intrusion (IDS) font partie des armes de l'arsenal de sécurité. Ces produits contrôlent en permanence les réseaux et conservent des journaux détaillés de toutes les intrusions ou attaques. De même, les pare-feu permettent aux utilisateurs de filtrer l'activité du réseau et de conserver des journaux détaillés de cette activité.

Toutefois, à eux seuls, les systèmes de détection d'intrusion sont limités. Ils permettent aux responsables informatiques de suivre et d'intervenir en fonction des événements dans leur propre réseau. L'analyse des journaux du pare-feu d'une entreprise le permet également. Ces systèmes proposent un aperçu complet des menaces courantes auxquelles fait face l'entreprise. Cependant, ils peuvent refléter une vue subjective des risques et des vulnérabilités. Sans disposer d'un contexte plus large, les experts en sécurité peuvent prendre des décisions et formuler des réponses qui n'optimisent pas leur stratégie de sécurité. Par exemple :

- Les journaux des systèmes IDS et des pare-feu ne peuvent pas déterminer si l'activité vise spécifiquement une seule entreprise ou si elle fait partie d'une attaque plus vaste concernant plusieurs entreprises.
- Les produits IDS peuvent identifier les attaques courantes, mais ils ne permettent pas aux entreprises d'évaluer ni de réduire le risque de futures attaques, faisant de cette solution un modèle de sécurité réactif.
- L'avantage des systèmes de pare-feu réside uniquement dans leur configuration. Les administrateurs peuvent optimiser leur pare-feu pour protéger leurs ressources seulement après avoir reçu des informations sur les menaces globales.

Les entreprises doivent pouvoir exploiter les compétences et l'expérience des experts en sécurité réseau du monde entier pour anticiper et bloquer les attaques avant leur déclenchement. Toutefois, la plupart des tentatives de mise en place d'une approche plus proactive vis-à-vis de la gestion des menaces a échoué en raison de facteurs tels que :

- L'absence d'un système global de sondes pour contrôler l'activité de l'attaque
- Le volume de données nécessaires pour créer un ensemble d'échantillons statistiquement valables
- L'absence de technologie pour analyser ces données

Par ailleurs, le nombre croissant, la complexité et le taux de réussite des attaques ne permettent pas aux experts en sécurité d'évaluer leur vulnérabilité uniquement en analysant les intrusions dans leur périmètre. Pour les aider à visualiser les modèles et les tendances, ils doivent bénéficier d'informations détaillées sur les différentes attaques qui sévissent sur le marché et dans le pays ainsi que d'informations sur leur date de parution. Malheureusement, la plupart des entreprises n'ont pas la possibilité d'obtenir ce genre d'informations car les données d'intrusion sont extrêmement sensibles. Même si ces données étaient disponibles, les comprendre relèverait du défi et ce, pour deux raisons :

1. Chaque produit IDS et de pare-feu signale les incidents en utilisant sa propre technologie unique, réduisant de ce fait toute chance d'obtenir une image complète des attaques en fonction des différents systèmes et entreprises.
2. Les experts en sécurité ne peuvent pas partager les données de leurs systèmes IDS et de pare-feu en temps réel.

Symantec est capable de relever ces défis et reconnaît le besoin urgent d'adopter une approche plus proactive vis-à-vis de la gestion des menaces. Symantec DeepSight Threat Management System permet aux entreprises de mieux anticiper et de bloquer toute attaque réseau. Symantec DeepSight Threat Management System comble le fossé entre la prise de conscience et l'action, permettant ainsi aux experts en sécurité de déployer les contre-mesures nécessaires avant qu'un intrus n'attaque leur système ou n'endommage leurs opérations.

> **Symantec DeepSight Threat Management System : un système global d'alertes en temps réel**

Symantec DeepSight Threat Management System est une solution de gestion des menaces personnalisable et exhaustive qui fournit des alertes en temps réel en cas d'attaques et des contre-mesures pour empêcher toute attaque d'atteindre l'entreprise. Symantec DeepSight Threat Management System fournit des informations sur l'exposition potentielle d'une entreprise en évaluant les événements IDS et des pare-feu des entreprises dans le monde entier pour identifier les tendances, les anomalies et les modèles d'attaques. Les administrateurs peuvent ainsi répondre aux importantes questions telles que :

- Les entreprises présentant des caractéristiques particulières (telles que le secteur, la taille ou l'emplacement) sont-elles sujettes aux attaques ?
- Quels produits et quelles plates-formes informatiques sont visés ou sont particulièrement vulnérables ?
- Quelles vulnérabilités présentent les risques les plus élevés ?
- Quels systèmes doivent recevoir des correctifs et dans quel ordre ?
- Les attaques proviennent-elles d'adresses IP ou de pays spécifiques ?
- Quels types d'attaques sont les plus fréquents ?
- Le risque d'attaque est-il plus élevé certains jours de la semaine ou à certaines heures de la journée ?
- Quels sont les correctifs, les solutions ou les informations supplémentaires disponibles pour bloquer des menaces spécifiques ?

Tout comme un système de prévisions météorologiques à long terme, Symantec DeepSight Threat Management System permet aux entreprises de prendre des mesures préventives avant qu'une catastrophe n'arrive. Ce service est constitué d'un réseau de données rassemblant plus de 19 000 partenaires enregistrés présents dans plus de 180 pays. Les experts en menaces de Symantec contrôlent en permanence ces données, analysent l'activité globale, contrôlent le trafic suspect et identifient l'origine des attaques.

Symantec DeepSight Threat Management System effectue un suivi des attaques par type, source, heure, emplacement et profil de victime, puis permet aux informaticiens d'utiliser ces données pour évaluer les risques et les vulnérabilités grâce à un moteur de corrélation révolutionnaire et à de puissants outils analytiques. Ce système fournit un cliché de l'activité Internet en cours, ainsi qu'une analyse personnalisée et en temps réel des menaces pour chaque client. Les alertes de menaces personnalisées, de codes malveillants et de seuil d'activité d'incident sont envoyées via une console Web sécurisée ou par courrier électronique, par fax, par message vocal ou par message SMS. Par ailleurs, les clients reçoivent des rapports quotidiens, hebdomadaires et mensuels succincts. Symantec DeepSight Threat Management System permet également aux utilisateurs d'effectuer des recherches dans la base de données des événements de Symantec grâce à un outil de notification personnalisé.

Le tableau 1 répertorie les rapports spécifiques fournis par Symantec DeepSight Threat Management System. Grâce à ces rapports, les données brutes des journaux d'IDS et de pare-feu fournissent des indications pour mieux bloquer les menaces de façon proactive.

Tableau 1. Rapports fournis par Symantec DeepSight Threat Management System

Titre	Description
Résumé des événements	Résumé de l'activité des événements observée par les sondes de DeepSight. Il permet de déterminer les événements les plus marquants et de définir leur historique.
Résumé des ports	Résumé de l'activité des ports observée par les sondes de DeepSight. Il permet de déterminer les ports visés et de définir la tendance de cette activité.
Résumé des catégories	Résumé de l'activité des événements par catégorie ou classe d'événements observée par les sondes de DeepSight.
Résumé des produits cible	Résumé des produits et des applications visés dans le monde entier.
Résumé de l'origine	Résumé de l'origine des événements globaux. Il permet de déterminer qui vise les sondes de DeepSight et de définir la tendance de l'activité de l'attaque à partir de chaque source.
Résumé de la destination	Résumé de la zone démographique affectée par les événements signalés au DeepSight Threat Management System.
Analyse de l'adresse IP	Fournit des indications sur l'activité d'une seule adresse IP observée par les sondes de DeepSight. Ce rapport est constitué d'un nombre de composants qui reflètent l'activité, les habitudes et les applications visées par l'adresse IP. En mettant en corrélation ces différentes données, il fournit l'origine de l'assaillant, ainsi que les vulnérabilités et les services visés par celui-ci.
Analyse des événements	Fournit une analyse détaillée de l'activité entourant un événement spécifique. Ce rapport fournit un historique de l'activité de l'événement. Il explique qui est à l'origine de l'activité et qui est visé.

Analyse des ports	Fournit une analyse détaillée de l'activité entourant un port spécifique. Ce rapport fournit un historique de l'activité visant le port sélectionné. Il explique qui est à l'origine de l'activité et qui est visé.
Fournisseurs de services Internet à l'origine des attaques	Affiche les dix principaux fournisseurs de services Internet responsables du plus grand nombre d'attaques, ainsi que la fréquence des attaques pour chaque fournisseur.
Taux d'infection des adresses IP source	Fournit une description du nombre d'adresses IP source pour un critère choisi. Ce rapport permet d'évaluer le taux de propagation d'une menace spécifique. Dans le cas d'un événement spécifique relatif à un ver, il permet également d'évaluer le nombre de systèmes infectés.
Adresses IP source	Fournit un résumé des principales adresses IP source responsables de l'activité du réseau choisie. Ce rapport contient un graphique des tendances décrivant l'activité décrite à partir des principales adresses.
Ports associés	Affiche les ports source associés les plus courants utilisés dans une attaque d'un port de destination fourni par l'utilisateur. Le graphique à barres représente les dix ports source les plus répandus utilisés avec un port de destination fourni par l'utilisateur, ainsi que la fréquence des attaques correspondantes pour chaque port source. Ce rapport indique tous les modèles de chevaux de Troie ou de failles.
Pays d'origine	Affiche les dix pays les plus dangereux à l'origine du plus grand nombre d'attaques.
Heure des événements	Fournit une description de la période pendant laquelle les événements de sécurité se produisent le plus souvent sur votre réseau. Cette information permet de suivre l'historique et l'allocation des ressources pour les planifications ultérieures.
Pays cible	Affiche les dix pays les plus visés, auxquels est destiné le plus grand nombre d'attaques.
Marchés cible	Affiche la fréquence des attaques ciblées par rapport à certains types de marchés.
Attaques en fonction de la taille des entreprises	Affiche la fréquence des attaques ciblées par rapport à la taille des entreprises.
Attaques en fonction du chiffre d'affaires des entreprises	Affiche la fréquence des attaques ciblées par rapport au chiffre d'affaires des entreprises.
Ancienneté de l'attaque	Décrit les événements en fonction de l'ancienneté des vulnérabilités associées à ceux-ci et de l'ancienneté des événements.

> Fonctionnement de Symantec DeepSight Threat Management System

Grâce à Symantec DeepSight Threat Management System, les entreprises peuvent se consacrer à leurs ressources de sécurité en déployant des contre-mesures stratégiques pour atténuer de manière proactive l'impact des attaques, plutôt qu'en recherchant sur les sites Web ou dans les courriers électroniques des informations sur une attaque ou sur la façon de s'en protéger. Symantec rassemble les données de ses partenaires, les met en corrélation et les analyse pour identifier des attaques éventuelles et fournir aux clients des informations pertinentes et en temps réel sur les correctifs et les menaces en vue de se protéger. Par ailleurs, une équipe de Symantec composée d'experts en menaces examine les données globales, identifie les attaques potentielles et fournit des analyses et des alertes détaillées. Pour bénéficier d'une meilleure hiérarchisation des ressources et des dépenses en matière de sécurité, il est indispensable de fournir rapidement des informations pertinentes, exhaustives et spécifiques aux experts en sécurité afin d'augmenter le retour sur investissement.

La Figure 2 décrit les composants clés de l'architecture de Symantec DeepSight Threat Management System.

- SYMANTEC DEEPSIGHT EXTRACTOR est un programme qui normalise et transmet les événements des journaux IDS et de pare-feu à la base de données des événements de Symantec. Une entreprise peut automatiquement transférer ses données d'événements vers la base de données d'événements de Symantec pour être interprétées et analysées. Symantec DeepSight Extractor garantit la confidentialité des clients grâce aux protocoles de gestion de réseau standard sécurisé et à la suppression des adresses IP facultatives.
- SYMANTEC DEEPSIGHT ANALYZER permet aux informaticiens de suivre et de gérer les incidents et les attaques sur leur propre réseau. Cette solution permet également de corréler les attaques provenant de différents produits de pare-feu et IDS, offrant ainsi aux informaticiens un aperçu complet de leurs environnements. Symantec DeepSight Analyzer compare les incidents avec la plus grande base de données de vulnérabilités (gérée par Symantec), effectue le suivi des attaques et fournit des informations sur la façon de se protéger contre celles-ci, génère des rapports de statistiques sur les incidents et gère les menaces. Les utilisateurs de Symantec DeepSight Analyzer soumettent anonymement le trafic réseau et les tentatives d'intrusion suspects à la base de données des événements de Symantec via Symantec DeepSight Extractor. Symantec utilise ces informations pour identifier les modèles dans les attaques. Celles-ci servent ensuite de système d'évaluation des menaces pour Symantec DeepSight Threat Management System. En retour, les participants reçoivent un accès à une console Web personnalisée et sécurisée sur les incidents. Le système est constitué de plusieurs utilitaires rentables qui offrent un suivi local des incidents, des rapports personnalisés sur les incidents et qui génèrent des messages de notification sur les assaillants. *REMARQUE : L'envoi de données à la base de données des événements de Symantec est facultatif pour les utilisateurs de Symantec DeepSight Threat Management System.*
- SYMANTEC DEEPSIGHT THREAT MANAGEMENT SYSTEM analyse automatiquement les journaux entrants d'IDS et de pare-feu pour détecter les modèles susceptibles de déclencher une attaque. Une fois identifiés, des alertes peuvent être envoyées automatiquement aux utilisateurs en fonction des critères définis. En outre, l'équipe des experts en menaces de Symantec contrôle et analyse de nouveau les modèles. Cette équipe fournit une analyse détaillée de la menace et des actions que les utilisateurs peuvent mener pour sécuriser leur environnement.

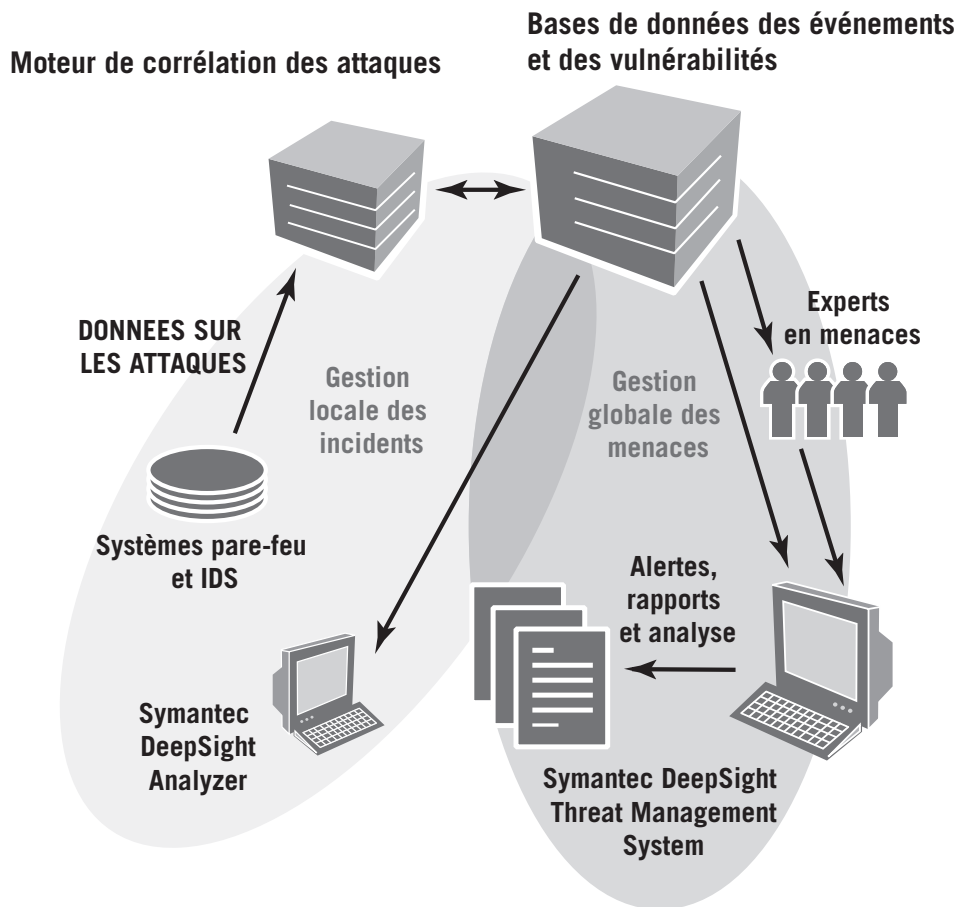


Figure 2. Composants clés de l'architecture de Symantec DeepSight Threat Management System.

> Symantec DeepSight Threat Management System en action

VER SQLEXP (VER HAMMER)

Le 25 janvier 2003, Symantec DeepSight Threat Management System a enregistré une augmentation importante et soudaine du trafic UDP sur le port 1434. Ce port est habituellement associé au processus Microsoft SQL Server Monitor. Cette augmentation soudaine de l'activité des attaques a été confirmée ultérieurement comme étant le résultat d'un ver résident sur la mémoire appelé W32.SQLEXP.Worm.

Le ver W32.SQLEXP.Worm exploite une vulnérabilité de dépassement de la capacité des piles dans le processus Microsoft SQL Server Monitor afin de s'autopropager. Le processus de propagation de SQLEXP et l'augmentation du trafic réseau ont entraîné une dégradation des performances du réseau sur Internet au cours de la propagation.

Ce ver ne contenait pas de données malveillantes. Son principal objectif consistait à se propager le plus rapidement possible. Ce ver aurait pu être beaucoup plus dangereux et contenir un code permettant d'endommager les systèmes infectés. L'objectif principal de ce ver était la consommation de la bande passante du réseau, ce qui a dans certains cas entraîné la perte de tous les paquets sur des réseaux. Pour cette raison, ce ver a d'abord été désigné par erreur comme une attaque par déni de service.

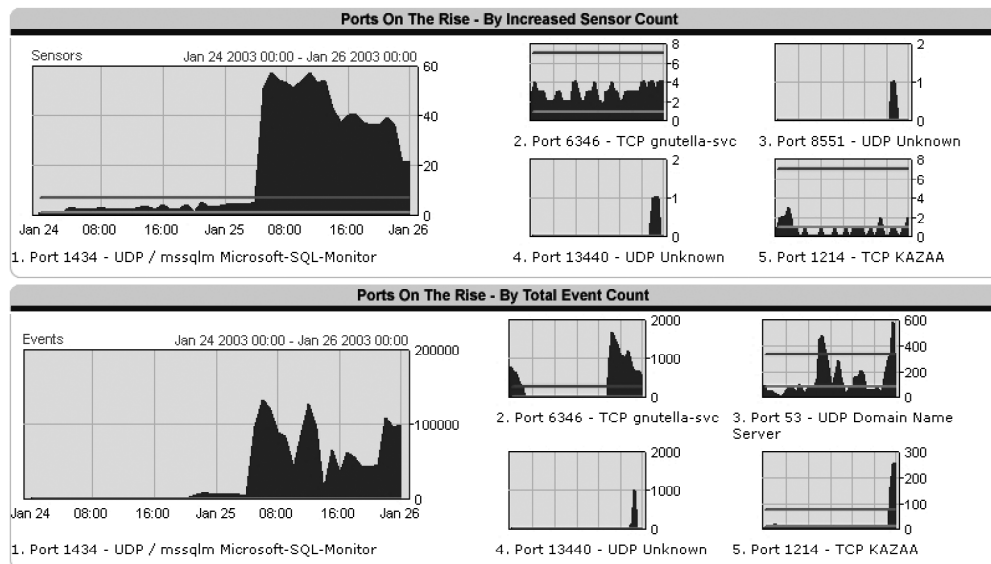


Figure 3. SQLExp – Ports sollicités signalés par Symantec DeepSight Threat Management System

Symantec DeepSight Threat Management System a automatiquement envoyé une alerte de port à 06:00 GMT le 25 janvier, au moment où une activité intense du port 1434 a été observée par le moteur d'analyse. Même si l'alerte de port n'a pas pu déterminer la cause de l'augmentation de trafic, les informations fournies par cette alerte ont permis d'avertir l'utilisateur en temps réel de l'avènement d'un incident global. Ces clients ont pu immédiatement bloquer le trafic sur le port 1434, évitant ainsi toute infection et réduisant ainsi l'impact de cette menace. Deux heures plus tard, Symantec DeepSight Threat Management System a publié une alerte d'incident qui a identifié cette menace comme un ver. Grâce à la quantité d'informations disponible, l'alerte d'incident a été mise à jour avec des détails supplémentaires sur le ver, la vulnérabilité visée par celui-ci et des liens directs vers les correctifs requis pour éliminer cette vulnérabilité.

Les clients de Symantec DeepSight Threat Management System ont reçu une alerte en temps réel sur le ver SQL.Exp ainsi qu'une analyse détaillée de la menace, permettant ainsi aux administrateurs d'intervenir rapidement et efficacement pour protéger leurs ressources.

> Avantages de la sécurité proactive

En aidant les entreprises à anticiper et à prévenir les attaques avant leur déclenchement, Symantec DeepSight Threat Management System permet au personnel informatique des entreprises d'adopter une approche proactive de la gestion des menaces grâce :

- **AUX ALERTES ANTICIPÉES DES ATTAQUES.** Les alertes de code malveillant et d'incident localisent les sources, les causes et les vulnérabilités des attaques, souvent dans les minutes qui suivent leur propagation. Les experts en sécurité peuvent ensuite prendre immédiatement des mesures préventives.
- **AUX ALERTES SPÉCIFIQUES AUX CONFIGURATIONS.** Les alertes peuvent être personnalisées et basées sur une infrastructure réseau spécifique, plus besoin de consulter des alertes concernant des technologies externes à l'entreprise.
- **A UNE ALLOCATION PLUS EFFICACE DES RESSOURCES DE SÉCURITÉ.** Symantec DeepSight Threat Management System permet aux experts en sécurité d'adapter leur stratégie de sécurité en fonction des incidents probables et des attaques risquant d'endommager leur configuration informatique unique. Par conséquent, ils peuvent utiliser plus intelligemment leur infrastructure de sécurité existante en identifiant les modifications stratégiques à implémenter et en définissant les autres investissements à effectuer.
- **AU REMPLACEMENT DES HYPOTHÈSES PAR DES DONNÉES BRUTES ET DES CONSEILS D'EXPERT.** Symantec DeepSight Threat Management System fournit des faits objectifs et des fonctions d'analyse puissantes qui permettent d'évaluer les risques et de prendre des décisions avisées telles que le moment adéquat pour isoler des opérations de réseau ou bloquer des groupes d'utilisateurs. Grâce à la disponibilité immédiate des données à partir de la console Web ou par courrier électronique, par fax, par message vocal ou par message SMS, Symantec DeepSight Threat Management System réduit considérablement le temps et les efforts fournis par les experts en sécurité pour rechercher et dépister les événements de sécurité. Ces derniers ont constamment accès aux alertes et aux analyses, n'importe où dans le monde.
- **A UN APERÇU GLOBAL DES TENDANCES EMERGENTES EN MATIÈRE DE SÉCURITÉ.** En comparant les données des journaux des entreprises avec les informations de la base de données des événements de Symantec, Symantec DeepSight Threat Management System place les données de pare-feu et d'IDS dans un contexte et une perspective appropriés. La base de données des événements de Symantec transforme les rapports et les descriptions uniques sur les incidents de chaque produit pare-feu ou IDS principal dans un format cohérent, afin que les administrateurs bénéficient d'un panorama complet et précis des tendances stratégiques en matière de sécurité dans le monde entier.

> Conclusion

Les progrès en matière de technologie de sécurité sont souvent dépassés par les nouveaux outils et les nouvelles techniques développés par les éventuels intrus. Alors que les rendements des autres mécanismes de sécurité logiques et physiques commencent à décroître, de nombreuses entreprises se rendent compte que la pièce la plus efficace et la plus importante du puzzle est une solution d'alertes en temps réel proactive.

Grâce à Symantec DeepSight Threat Management System, les entreprises peuvent exploiter l'expérience et les compétences des experts en sécurité réseau du monde entier pour mieux anticiper et contrer les attaques. En évaluant le profil du réseau et les données des journaux des pare-feu et des IDS d'une entreprise et en les comparant aux informations semblables provenant de milliers d'autres entreprises, Symantec DeepSight Threat Management System fournit des informations pertinentes, complètes et précises aux experts en sécurité, permettant ainsi une hiérarchisation plus efficace des ressources et des dépenses en matière de sécurité.

> Glossaire

Si vous n'êtes pas familier avec l'un des termes utilisés dans ce rapport, vous trouverez des informations supplémentaires et un glossaire à l'adresse suivante : <http://www.symantec.fr>.

CRÉÉE EN 1982, À CUPERTINO, AU CŒUR DE LA SILICON VALLEY, SYMANTEC, LEADER MONDIAL DES TECHNOLOGIES ET DES SERVICES DE SÉCURITÉ INTERNET, PROPOSE UNE LARGE GAMME DE BOITIERS ET DE LOGICIELS DE SÉCURITÉ DE RÉSEAU ET DE CONTENU AUX PARTICULIERS, AUX ENTREPRISES ET AUX FOURNISSEURS D'ACCÈS INTERNET. SYMANTEC ASSURE LA PROTECTION POUR LES POSTES DE TRAVAIL, LES SERVEURS ET LES PASSERELLES. CES SOLUTIONS COUVRENT LES BESOINS EN DÉTECTION DE VIRUS, PARE-FEU ET RÉSEAU PRIVÉ VIRTUEL, GESTION DES VULNÉRABILITÉS, DÉTECTION D'INTRUSION, FILTRAGE DE CONTENU INTERNET ET DE MESSAGERIE ÉLECTRONIQUE, DE TÉLÉINTERVENTION, DÉPLOIEMENT, ASSISTANCE, MAINTENANCE ET DE SERVICES PROFESSIONNELS DE SÉCURITÉ POUR LES ENTREPRISES ET LES FOURNISSEURS D'ACCÈS INTERNET, DANS LE MONDE ENTIER. LA MARQUE NORTON DE SYMANTEC, SPÉCIALISÉE DANS LES PRODUITS DE SÉCURITÉ GRAND PUBLIC, DOMINE LE MARCHÉ INTERNATIONAL DE LA VENTE AU DÉTAIL. BASÉE À CUPERTINO (CALIFORNIE), SYMANTEC EST PRÉSENTE DANS 38 PAYS. POUR PLUS D'INFORMATIONS, VISITEZ LE SITE WWW.SYMANTEC.FR

WORLD HEADQUARTERS
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

L'entreprise Symantec est présente dans plus de 40 pays à travers le monde. Pour plus d'informations concernant les bureaux locaux, consultez le site : www.symantec.fr

POUR PLUS D'INFOS SUR LE SERVICE CLIENTÈLE ET LE SUPPORT TECHNIQUE, VISITEZ LE SITE www.symantec.com/eusupport