



Symantec™ ManHunt™

Réduction des risques

Internet expose les ressources de l'entreprise à des risques considérables : une seule et unique attaque peut coûter des millions de dollars. Les préjudices subis peuvent également se traduire par une perte de confiance des clients et la perte des droits de propriété intellectuelle, sans compter la perte de temps et d'argent pour l'entreprise qui tente de se remettre sur pied après une attaque de ce type. Les produits de sécurité tels que les firewalls et les systèmes de détection d'intrusion (IDS) traditionnels offrent certes un certain niveau de protection. Cependant, la protection réelle des ressources réseau requiert un investissement important en termes de temps et de ressources afin de rassembler les informations de sécurité nécessaires. SYMANTEC MANHUNT fournit les informations pertinentes dont les entreprises ont besoin pour pouvoir intervenir efficacement à chaque attaque.

> Sécurité performante des réseaux d'entreprise

Symantec ManHunt détecte d'une manière beaucoup plus complète que les IDS traditionnels les intrusions, analyse les menaces et y répond en temps réel pour protéger les réseaux d'entreprise. De plus, ManHunt offre une gestion cohérente de la sécurité en identifiant les menaces et en regroupant les informations afin d'optimiser les réponses face aux menaces émergentes. Grâce à l'utilisation de ManHunt en mode cluster (sondes réparties géographiquement sur le réseau), à la détection des anomalies de protocoles, au moteur d'analyse et de corrélation en temps réel, ManHunt supprime les données erronées (« faux positifs ») pour ne présenter que des informations appropriées à votre problématique de sécurité.

> Technologie de détection exhaustive

Alors que les attaques deviennent plus sophistiquées et plus sournoises, les IDS traditionnels ne sont plus en mesure de discerner les attaques furtives. L'architecture de détection hybride de ManHunt permet de personnaliser les fonctions de détection des sondes selon l'environnement réseau. A l'aide d'un ensemble de technologies de détection visant à améliorer l'identification des attaques, ManHunt décèle les activités malveillantes grâce à une détection des anomalies de protocoles, à la surveillance de la bande passante, au contrôle des états de protocoles et au réassemblage des paquets IP.

> Détection des nouvelles attaques

Face aux menaces permanentes que représentent les diverses attaques polymorphes, il est essentiel qu'elles soient immédiatement identifiées, gérées et contrées. Symantec ManHunt identifie les attaques connues et inconnues en analysant les flux réseau à l'aide de la détection des anomalies de protocoles. Ce type de détection ne requiert aucune signature préalable nécessaire pour détecter la plupart des types d'attaques, et permet à Symantec ManHunt de détecter et d'identifier les attaques dès leur apparition, avant même la publication des signatures. Cette fonction de nouvelles attaques permet déliminer la période de temps pendant laquelle l'attaque est connue sans avoir de signatures disponibles. De plus, les experts en sécurité peuvent personnaliser les sondes ManHunt en écrivant des règles au format Snort afin de leur permettre d'adapter leurs IDS à leur problématique d'entreprise.

PRINCIPALES FONCTIONNALITES

- > Fournit une gestion cohérente et efficace de la sécurité réseau, permettant ainsi une protection contre les intrusions et les attaques onéreuses.
- > Protège les infrastructures IT d'entreprise grâce à une détection gigabit et évolutive (jusqu'à 2 gigabits par seconde), à une analyse des menaces et des réponses en temps réel à l'aide de politiques de sécurité.
- > Rassemble les données de toute l'entreprise et fournit des informations pertinentes au moyen de sondes réparties géographiquement sur le réseau et d'une analyse et corrélation d'événements en temps réel.
- > Identifie et réagit face aux attaques connues ou inconnues, grâce à une détection exhaustive et à une corrélation d'informations.
- > Pris en charge par Symantec™ Security Response – l'équipe mondiale de support et de recherche en matière de sécurité Internet

Architecture de détection ManHunt



Grâce à un ensemble de méthodologies de détection visant à améliorer l'identification des attaques, ManHunt peut suivre les nouvelles menaces en constante évolution.

> Détection gigabit pour les environnements haut débit

Symantec ManHunt protège vos systèmes d'informations grâce à une surveillance du trafic gigabit pouvant être mis en œuvre à n'importe quel niveau de l'entreprise, y compris sur des backbones gigabits. En combinant des techniques d'analyse protocolaire et de signatures d'attaques, ManHunt est la meilleure solution de détection d'intrusion capable de gérer un réseau gigabit, prouvé par des tests effectués par un laboratoire tiers indépendant.

> Analyse et corrélation des événements en temps réel

Un moteur performant d'analyse et de corrélation filtre les données erronées pour conserver uniquement les informations pertinentes. Ainsi, les administrateurs ne se perdent pas dans la quantité de données remontées. La corrélation des événements en temps réel permet à ManHunt de détecter et de reconnaître rapidement les attaques à l'aide de l'analyse « Cross Node ». Cette procédure réduit considérablement les efforts d'identification des menaces fournis par les responsables de la sécurité, leur permettant ainsi de se consacrer à la gestion des politiques et à l'analyse des intrusions sophistiquées, plutôt qu'à l'examen des historiques d'événements non liés.

> Capture et analyse de tous les paquets, sans exception.

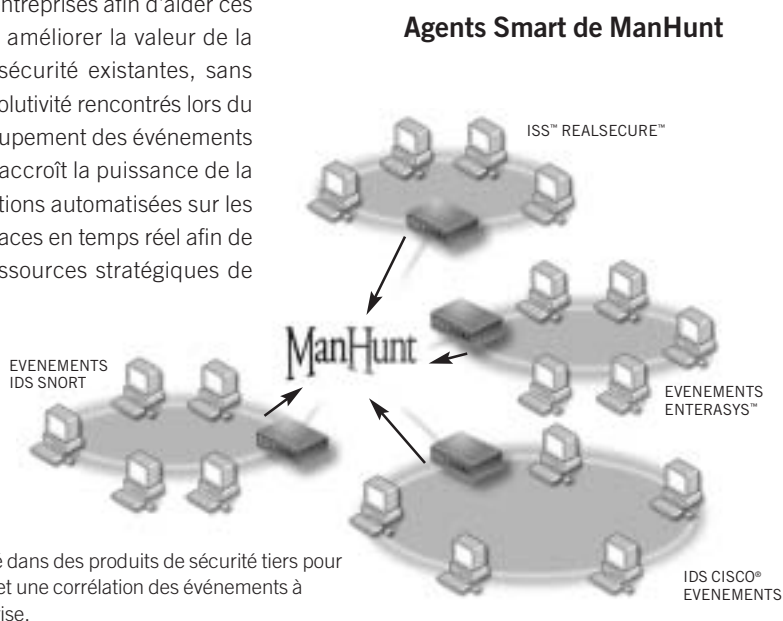
Pour une analyse efficace d'une attaque et de ses caractéristiques, ManHunt peut être configuré pour enregistrer tous les paquets composant une attaque (quelque soit la technologie de détection utilisée). Les administrateurs peuvent rapidement déterminer si le paquet capturé est un événement bénin pouvant être facilement filtré ou s'il doit être différencié pour une analyse plus complète. Les paramètres de trafic incluant les adresses IP, les ports source et de destination, le type de protocole, le moment et l'importance de la capture peuvent être utilisés comme filtres, ce qui permet ainsi aux experts en sécurité d'analyser tout le flux de données ou seulement quelques paquets de la même connexion.

> Déploiement de la protection de la sécurité d'entreprise

La technologie Smart Agent de Symantec ManHunt permet une collecte des événements de différentes sources à l'échelle des entreprises afin d'aider ces dernières à optimiser leur niveau de protection et améliorer la valeur de la détection des menaces de leurs ressources de sécurité existantes, sans entraîner pour autant de problèmes de coûts et d'évolutivité rencontrés lors du déploiement de produits IDS traditionnels. Le regroupement des événements de sécurité tiers dans un emplacement centralisé accroît la puissance de la structure d'analyse de ManHunt. Puis, les interventions automatisées sur les incidents permettent l'identification rapide des menaces en temps réel afin de réduire le risque de dommages éventuels des ressources stratégiques de l'entreprise.

ANALYSE EN TEMPS REEL

- > Hiérarchisation des multiples déploiements de ManHunt grâce à l'analyse Cross Node
- > Gestion holistique de la sécurité via une analyse et une corrélation des événements tiers en temps réel comprenant Snort, ISS™ RealSecure™, Enterasys™ Dragon™, Cisco® IDS, Checkpoint™, NetScreen® et Tripwire®
- > Référentiel de données sur la sécurité (conforme FIPS 140) signé numériquement et autorisé



➤ Réponse proactive basée sur des politiques de sécurité

Pour défendre activement le réseau, ManHunt ne se contente pas d'une identification et d'une alerte passive des incidents. Grâce aux réponses définies selon des politiques, ManHunt peut gérer et contrôler les attaques en temps réel, puis engager d'autres actions requises pour intervenir face aux incidents. Des politiques personnalisées fournissent une intervention immédiate face aux intrusions ou aux attaques de déni de service en fonction du type d'incident et de l'emplacement de l'événement sur le réseau. La suspension de session, FlowChaser™, les filtres de qualité de service (QoS), l'enregistrement du trafic, et les réponses « Handoff » peuvent être combinés pour protéger les ressources stratégiques de l'entreprise. Si les réponses face aux incidents requièrent une analyse plus approfondie, ManHunt intègre des fonctions d'analyse et de journalisation pour examiner les paquets capturés et obtenir des informations spécifiques détaillées.

➤ Analyse automatisée des attaques dans et au-delà de l'entreprise

Grâce à la technologie sophistiquée FlowChaser, ManHunt détecte le flux et la régulation du trafic malveillant, en dépistant les attaques jusqu'à leur origine pour identifier rapidement le point d'entrée des attaques réseau. Lorsque les limites ont été atteintes, ManHunt envoie et reçoit des informations de dépistage à l'aide d'un protocole propriétaire pour communiquer avec les routeurs en amont en dehors de son domaine afin de poursuivre le suivi d'une attaque. Si le flux des attaques provient d'un autre fournisseur Internet, l'incident est transmis au pair en amont afin d'en continuer le suivi.

➤ Protection évolutive de l'entreprise

La protection de l'entreprise ne s'arrête pas à un segment unique. Une solution évolutive capable de résister au pirate le plus déterminé est en effet requise. ManHunt va au-delà des exigences en matière de déploiements IDS des grandes entreprises en fournissant la première collaboration intelligente entre des sondes ManHunt dispersés géographiquement sur le réseau. Les sondes peuvent changer dynamiquement de segments de réseau à surveiller en fonction de vos priorités, facilitant ainsi le contrôle des VLANs et des ports et permettant de réduire les coûts de déploiement sans compromettre la couverture de détection.

➤ Haute disponibilité

Pour renforcer davantage ses protections réseau, divers nœuds ManHunt peuvent être déployés dans une configuration haute disponibilité afin de garantir une détection des événements continue et un temps de fonctionnement optimal. Si un nœud primaire du groupe à haute disponibilité échoue, le nœud secondaire continue la détection des événements actuels et futurs en toute transparence, et ce sans perte de données ou de trafic. Chaque dispositif ManHunt fournit également une répartition de charge interne en distribuant intelligemment les flux de trafic entre les unités centrales de traitement.

➤ Déploiement efficace et évolutif

Un système ManHunt ou un groupe haute disponibilité peut être configuré pour contrôler plusieurs segments, switchs ou VLANs basés sur leur utilisation combinée de la bande passante et non sur le nombre de segments réseau. Au fur et à mesure de l'agrandissement de l'architecture réseau des cartes réseau peuvent être ajoutées à ManHunt avec le nombre de sondes nécessaires afin de répondre aux exigences de bande passante, sans avoir besoin d'un système supplémentaire.

De plus, ManHunt peut également se déployer en clusters de sondes (128 sondes maximum) dotés d'une console d'administration unique. L'ensemble des communications entre les nœuds ManHunt et la console de gestion est cryptée AES-256 afin de garantir l'intégrité du déploiement. Contrairement aux produits IDS traditionnels, le déploiement clusterisé et le contrôle rapide de ManHunt est adapté aux plus grandes entreprises.

REponses Proactives

- Réponses proactives basées sur des politiques de sécurité (ensemble de paramétrage qui permet de répondre automatiquement aux attaques)
- Analyse des adresses IP usurpées jusqu'à leur origine grâce aux technologies FlowChaser et TrackBack
- Prise en charge de réseau étendu avec des interventions « Handoff » et une communication de routeurs sécurisée
- Recommandations de filtres QoS pour une protection de déni de service
- Enregistrement ciblé du trafic déclenché par des réponses automatisées face aux événements
- Prise en charge de réponses personnalisées

DEPLOIEMENT EFFICACE

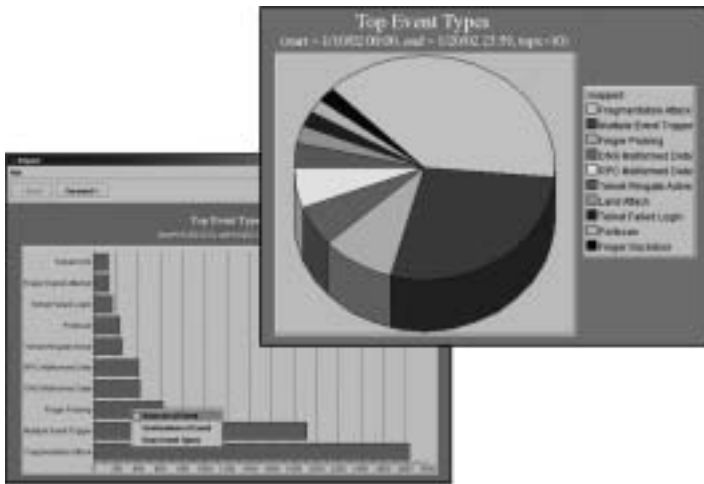
- Contrôle de quatre interfaces Gigabit Ethernet ou 12 interfaces Fast Ethernet maximum sur un hôte ManHunt unique
- Tolérance aux pannes à haute disponibilité
- Intégration transparente aux infrastructures de switches et de routeurs
- Polyvalence de configuration via des ports multiples 10/100 et des ports gigabits capable de détecter des hubs, une ou plusieurs copies/ports VLAN, et/ou sur plusieurs switches
- Console de gestion centrale pour surveiller les événements à partir de divers produits de sécurité (dispositifs INFOSEC, IDS systèmes, IDS réseau et IDS basés sur des leurres)
- Fonction d'exportation de données d'audit sur un Syslog centralisé
- Communications entre hôtes et GUI conformes FIPS 197 (AES-256)

> Gestion des incidents

Les opérateurs IDS travaillent souvent par équipe ou se relaient sur la console, entraînant ainsi un problème de communication entre les intervenants sur le statut des attaques, l'attribution des responsabilités et le suivi des événements de l'incident. Avec ManHunt, les incidents peuvent être facilement suivis grâce à l'ajout d'annotations concernant le traitement de l'attaque. Les autres intervenants de l'entreprise peuvent ainsi connaître les détails de l'incident, la façon dont l'opérateur l'a traité et accéder à une base de données récapitulant l'historique des activités.

> Fonctions de rapport avancées

ManHunt multiplie les niveaux de rapport en proposant des rapports allant d'un format synthétique au format beaucoup plus détaillé des attaques. Grâce à ses fonctions de rapport, les entreprises peuvent mesurer l'efficacité globale de l'infrastructure sécurité, le niveau de sécurité atteint et visualiser des informations spécifiques sur la sécurité.



Les options de notification comprennent des graphiques et des tableaux détaillés contenant des informations sur les événements qui montrent clairement les tendances des attaques et l'état global de la sécurité du réseau de l'entreprise.

Pour plus d'informations sur Symantec ManHunt, visitez le site <http://www.symantec.fr/region/fr/product/smh.html>

LA DETECTION D'INTRUSION CONSTITUE UN COMPOSANT CLE 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 SYMANTEC MANHUNT 2.2

CONFIGURATION DU SYSTEME MANHUNT

- Sun® Solaris™ 8 64 bits ou Solaris 8 Intel® Edition avec distribution complète et prise en charge OEM (Consultez la documentation produit pour le niveau de correctif.)
- SPARC™ dédié ou matériel Intel® (Consultez la documentation produit pour des instructions concernant la plate-forme.)
- 1 interface réseau pour chaque dispositif contrôlé. Jusqu'à 12 Fast Ethernet ou 4 Gigabit Ethernet (Consultez la documentation produit pour la liste des cartes d'interface réseau gérées.)
- 1 interface réseau pour l'administration/la gestion
- Mémoire RAM 1Gb/s pour les configurations Fast Ethernet, mémoire RAM 2Gb/s pour des configurations Gigabit uniques, mémoire RAM 4Gb/s pour les configurations multi-gigabit
- Environnement Java™ 2 Runtime, édition standard 1.2.2

CONFIGURATION DE LA CONSOLE D'ADMINISTRATION

- Microsoft® Windows® 98/NT® 4.0/2000, Solaris 2.6/7/8
- Processeur Intel Pentium II ou supérieur, ou Ultra SPARC II ou supérieur
- 256 Mo de RAM
- Java™ 2 Runtime Environment, édition standard 1.3 ou 1.4

GESTION ET USAGES

- > Console de gestion facile à utiliser, personnalisation simplifiée, gestion des politiques, filtrage et génération des interventions
- > Gestion en un point unique à l'aide d'une console pour différents déploiements ManHunt
- > Fonction d'exportation d'événements et d'incidents vers des bases de données SQL
- > Réduction des faux positifs grâce à un filtrage incident/événement
- > Analyse performante détaillée avec interception de l'intégralité des paquets, y compris les entêtes et les données utiles
- > Description détaillée des événements comprenant les failles et les données de vulnérabilité, des liens aux ressources supplémentaires, des références croisées avec CVE et des ID d'événements tiers
- > Fonction de notification améliorée comprenant des graphiques et des tableaux personnalisables et pré-définis
- > Annotations d'événements et notation des incidents

"L'opinion des testeurs est unanime : le système de détection ManHunt de Symantec satisfait entièrement les exigences et les attentes de l'utilisateur final pour lequel ce système a été conçu et a par conséquent reçu le prix "NetWORKS As Advertised"."



SIEGE INTERNATIONAL
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
Tel. : +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/