Tivoli software

IBM Tivoli Security Operations Manager

Points forts

- Centralise les opérations de sécurité sur l'ensemble du réseau de l'entreprise
- Aligne les opérations de sécurité sur les opérations informatiques et les priorités d'entreprise pour optimiser la continuité de service
- Aide à traiter les exigences de conformité et les règles de gestion du risque d'entreprise
- Aide à minimiser le temps nécessaire pour reconnaître et résoudre les incidents de sécurité

La disponibilité du réseau et des ressources est absolument essentielle pour l'entreprise et la garantie du service. Mais les entreprises, les organismes gouvernementaux et les fournisseurs de services peuvent perdre chaque année des millions d'euros suite à des vers ou d'autres types de programmes malveillants qui affectent les ressources d'entreprise et les services aux clients. C'est pourquoi la sécurité des informations est l'une des principales missions de tout responsable informatique dans une entreprise.

Afin d'optimiser la disponibilité des ressources et du service et protéger les informations des clients, les responsables de la sécurité des systèmes d'information (RSSI) doivent aujourd'hui pouvoir :

- reconnaître et traiter rapidement les incidents de sécurité ;
- mettre en œuvre des règles de sécurité ;
- soutenir des initiatives d'audit et de conformité.

Le problème est que chacune de ces activités implique que les données de sécurité résident dans toute l'entreprise. Les entreprises et les fournisseurs de services doivent pouvoir consulter et analyser ces données dispersées, rapidement et efficacement. Dans les environnements multi-fournisseurs complexes d'aujourd'hui, cela nécessite de s'appuyer sur une solution intégrée et automatisée.

Pour répondre à ces défis, adoptez IBM Tivoli Security Operations Manager — une plateforme d'informations de sécurité et de gestion des événements (SIEM) conçue pour améliorer l'efficacité, la rentabilité et la visibilité des opérations de sécurité et de la gestion du risque d'information. Tivoli Security Operations Manager centralise et stocke les données de sécurité dans toute l'infrastructure technologique ; vous pouvez ainsi :

- Automatiser le regroupement, la corrélation et l'analyse de logs.
- Reconnaître, rechercher et résoudre automatiquement les incidents.
- Rationaliser le suivi et le traitement des incidents.
- Permettre la surveillance et l'application de règles.
- Fournir des rapports détaillés pour les efforts de conformité.

Tivoli Security Operations Manager automatise de nombreuses activités répétitives et longues, nécessaires pour des opérations de sécurité performantes. Le résultat est une approche efficace et rentable en matière d'opérations de sécurité.

Centraliser le regroupement de logs dans des environnements multi-fournisseurs

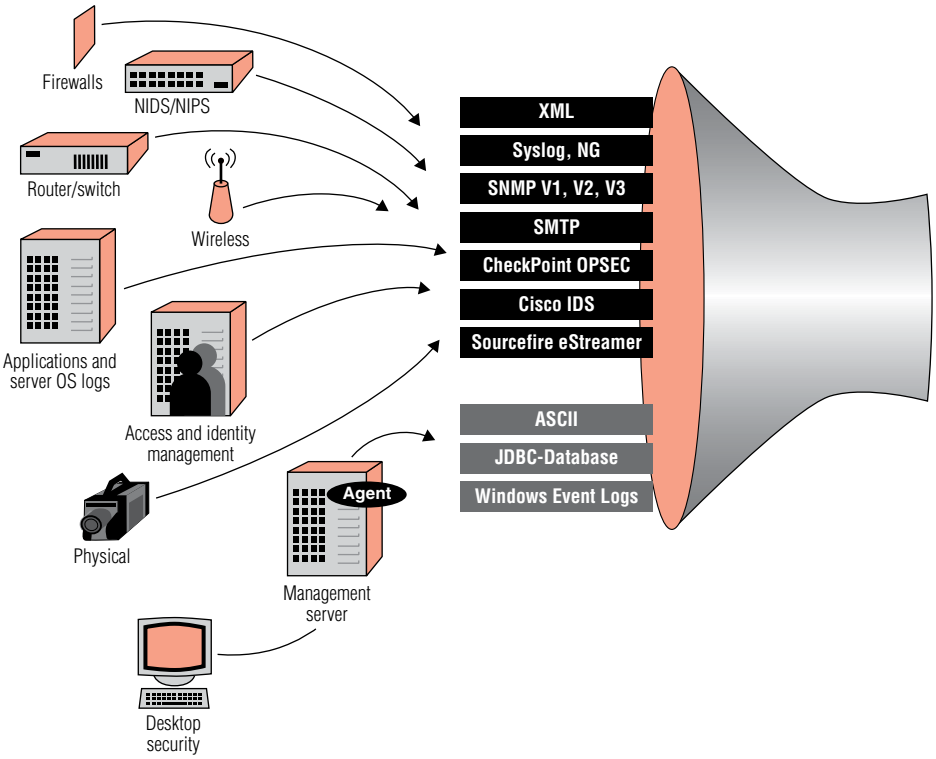
Afin de détecter les attaques, les programmes malveillants, les erreurs de configuration potentiellement dangereuses et les abus internes, une équipe de sécurité doit analyser des ensembles de données d'événement dans toute l'infrastructure de sécurité :

- Systèmes de détection des intrusions
- Pare-feux
- Réseaux privés virtuels
- Applications antivirus

De plus, des informations importantes doivent être obtenues auprès des serveurs ou hôtes d'infrastructure informatiques ou opérationnelles classiques.

Malheureusement, le volume de données et le nombre de machines réparties sur un réseau classique peuvent rendre impossible l'analyse manuelle des données de sécurité.

Par conséquent, il est important d'automatiser le processus de regroupement d'événements à partir d'unités et de systèmes dispersés au sein d'un unique emplacement central, où les données seront corrélées afin de faciliter les réponses et les rapports sur les incidents.



Tivoli Security Operations Manager offre une plateforme que votre entreprise peut utiliser pour regrouper automatiquement les logs hôte, les événements de sécurité, les données d'équipements et les données de vulnérabilité à des fins d'analyse et de corrélation.

La centralisation et le regroupement automatique des données sont également essentiels pour les efforts de conformité. Les entreprises stockent souvent leurs données de journal pendant de longues périodes, pour permettre l'analyse historique des données, si nécessaire.

Tivoli Security Operations Manager est une plateforme sur laquelle votre entreprise peut automatiquement regrouper les logs hôte, les événements de sécurité, les données d'équipements et les données de vulnérabilité. Sélectionnez la quantité et la source des données que vous souhaitez intégrer dans le logiciel et Tivoli Security Operations Manager collecte ces données à l'aide de protocoles standard et natifs, comme Extensible Markup Language (XML), syslog, Simple Network Management Protocol (SNMP), Simple Mail Transfer

Protocol (SMTP), CheckPoint OPSEC, Sourcefire eStreamer et bien d'autres encore. Il peut également utiliser son propre agent universel à faible impact pour collecter les informations. Tivoli Security Operations Manager collecte les données d'événements et de logs à partir de centaines d'unités différentes «prêtes à utiliser» dès à présent. En outre, il prend également en charge vos unités personnalisées et vos applications internes.

Améliorer la détection des incidents par une corrélation entre unités

A partir des informations collectées sur l'infrastructure, Tivoli Security Operations Manager peut vous aider à détecter les attaques, les abus et toute activité anormale. Le logiciel analyse et hiérarchise les données d'événements en utilisant quatre techniques de corrélation complémentaires :

- Corrélation basée sur des règles : détecte les attaques et violations de règles connues.
- Corrélation de vulnérabilité : mappe les attaques connues et les vulnérabilités système connues.
- Corrélation statistique : identifie les anomalies en effectuant une analyse avancée des événements et des hôtes.
- Corrélation de susceptibilité : aide à déterminer la probabilité d'exposition pour tout système donné.

En outre, Tivoli Security Operations Manager peut utiliser vos priorités d'entreprise pour pondérer l'importance des équipements pendant le processus de corrélation afin de hiérarchiser les activités de sécurité. Lorsque les analystes de sécurité utilisent la console, ils ne voient pas une liste infinie d'événements de sécurité, mais des informations significatives qui ont été hiérarchisées conformément à vos objectifs et vos règles.

Réduire le temps de résolution en intégrant la recherche et la réponse aux incidents

Pour vous aider à réduire fortement le temps nécessaire pour traiter des attaques, des erreurs de configuration ou des abus, Tivoli Security Operations Manager intègre des outils de recherche et de réponse. Le logiciel facilite également le processus de signalisation progressive et de suivi. Les fonctionnalités de recherche comprennent les éléments suivants :

- Outils de recherche en un clic intégrés.
- Réponses automatisées pour bloquer les menaces et fermer la boucle.
- Suivi géographique des activités douteuses.
- Système d'établissement de tickets orienté sécurité.

Améliorer l'efficacité par une intégration opérationnelle

Tivoli Security Operations Manager traite les inefficiences opérationnelles subies par les sociétés informatiques non organisées en réseau, en facilitant le flux des données de gestion d'incidents entre les équipes de sécurité, de réseau et d'opérations de gestion des systèmes. Par exemple, Tivoli Security Operations Manager s'intègre étroitement dans le réseau et les produits de gestion système de l'entreprise (y compris les gestionnaires et tableaux de bord d'événements, ainsi que IBM Tivoli Enterprise Console) et dans les systèmes d'établissement de tickets des centres d'assistance informatique, comme Remedy. Vous pouvez vous appuyez sur ces intégrations pour :

- Prendre en charge les exigences d'assurance d'entreprise et de service.
- Corréler des aperçus de sécurité avec des informations d'environnement opérationnel plus large.
- Faciliter davantage la résolution des incidents.

Tivoli Security Operations Manager est également intégré dans IBM Tivoli Identity Manager et IBM Tivoli Access Manager for e-business afin de fournir une surveillance des règles d'accès et d'identité des clients, en appliquant des règles et en détectant et traitant rapidement les tentatives d'abus potentielles.

Renforcer la compréhension par des rapports détaillés

Les outils d'exploration de données à la volée, de rapports historiques,

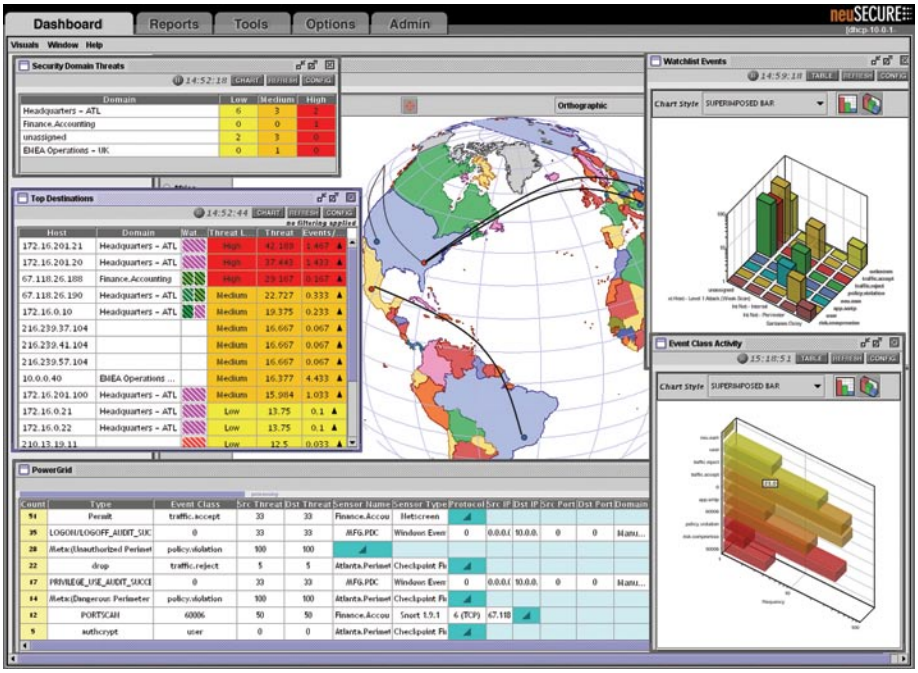


Tableau de bord de recherche principal de Tivoli Security Operations Manager

d'audit automatique et de suivi de Tivoli Security Operations Manager comprennent des composants essentiels pour comprendre les tendances de sécurité. De plus, ces rapports aident le service informatique à communiquer des informations de sécurité pertinentes aux autres publics, comme les équipes de gestion et d'audit.

Ces fonctionnalités comprennent :

- Des modèles de rapports standard et personnalisables.
- Un ordonnanceur de rapport automatisé.
- L'exportation HTML, PDF et XML de tous les graphiques et tableaux.
- Un audit automatique et un suivi de toutes les activités de sécurité.

Tivoli Security Operations Manager s'appuie sur les informations stockées dans une base de données d'événements de sécurité pour fournir des rapports et des tendances historiques à la demande.

Sélectionner l'option de déploiement qui correspond à votre environnement

Tivoli Security Operations Manager comprend une architecture modulaire capable de s'adapter et d'évoluer avec l'infrastructure de sécurité de votre entreprise. Chacun des composants, le module de regroupement d'événements qui collecte et normalise les données, le serveur de gestion central qui effectue une analyse et une corrélation avancées et la base de données qui stocke les informations historiques, peut être réparti sur des équipements distincts ; les composants peuvent sinon être déployés ensemble.

Une entreprise peut déployer plusieurs modules de regroupement d'événements au sein de son organisation pour prendre en charge de plus gros volumes d'informations d'événements ou pour faciliter la répartition géographique des ressources système. Un client utilise, par exemple, 12 modules de regroupement d'événements pour ses sites dispersés géographiquement : la société peut alors répartir la collecte et le traitement des données.

De la même façon, les modules de regroupement d'événements peuvent tous envoyer des données vers un serveur de gestion central unique, ou bien une entreprise peut utiliser plusieurs serveurs pour optimiser la disponibilité ; si un serveur est indisponible pour un module de regroupement d'événements, il redirigera l'événement vers un serveur de gestion central secondaire.

Fournir une plateforme pour offrir des services de sécurité gérés

En plus de servir de plateforme de sécurité informatique essentielle aux entreprises et transporteurs de moyenne et grande taille, Tivoli Security Operations Manager peut également

faire office de socle puissant et éprouvé pour une entreprise de services de sécurité gérés rentable. Les mêmes options de déploiement qui assurent l'extensibilité et la stabilité du logiciel pour toute entreprise permettent également à Tivoli Security Operations Manager de répondre aux besoins d'un environnement de services largement répartis.

Pour les fournisseurs de services de sécurité gérés, Tivoli Security Operations Manager permet de :

- Réduire les coûts opérationnels en offrant un haut niveau d'automatisation opérationnelle.
- Optimiser le temps de réalisation, grâce à une mise en œuvre rapide et des fonctionnalités «prêtes à utiliser» immédiates.
- Présenter des niveaux de service et une valeur ajoutée aux clients par des fonctionnalités de rapport complètes.

Tivoli Security Operations Manager en un clin d'œil

Configurations système recommandées pour le serveur de gestion central :

- Plateforme Red Hat Enterprise Linux ES 3.0 avec :
  - Dual Intel Pentium IV, 3,0 GHz ou unité centrale supérieure
  - RAM 4 Go ou plus
  - Disque dur 120 Go ou plus (notez que les exigences de stockage dépendent surtout du taux global d'événements système et des objectifs d'archivage et de rapports)
- Plateforme Sun Solaris 9 avec :
  - SunFire V440 Dual 1,5 GHz ou UltraSparc supérieur
  - RAM 4 Go ou plus
  - Disque dur 146 Go ou plus

Configurations système recommandées pour le module de regroupement d'événements :

- Plateforme Red Hat Enterprise Linux ES 3.0 avec :
  - Pentium IV, 3,0 GHz ou unité centrale supérieure
  - RAM 2 Go ou plus
  - Disque dur 36 Go ou plus
- Plateforme Sun Solaris 9 avec :
  - SunFire V240 Dual 1,5 GHz ou UltraSparc supérieur
  - RAM 2 Go ou plus
  - Disque dur 73 Go ou plus

Navigateurs pris en charge pour le client :

- Microsoft Internet Explorer 6.x ou plus
- Mozilla Firefox 1.7 ou plus
- Sun Java™ 1.4.2_08 ou plus

Bases de données prises en charge :

- MySQL 4.1
- Oracle Enterprise Edition 9*i*

Conclusion

Les brèches de sécurité peuvent entraîner de sérieuses conséquences mesurables : perte de revenus, temps d'arrêt, impact sur l'image, endommagement des équipements informatiques, perte d'informations clients ou propriétaires, coûts de nettoyage et de restauration et frais de litiges potentiels. Afin de réduire ces risques, les entreprises de sécurité ont besoin d'outils capables d'identifier et de réagir rapidement aux attaques.

Tivoli Security Operations Manager offre une approche holistique de votre situation de sécurité et toutes les fonctionnalités nécessaires pour analyser et rechercher rapidement les attaques. Vous disposez donc d'un outil performant pour prévenir les intrusions et optimiser la sécurité de votre entreprise.

A propos des logiciels IBM Tivoli

Les logiciels IBM Tivoli aident les entreprises à gérer efficacement les ressources, tâches et processus informatiques afin de répondre aux besoins toujours fluctuants des entreprises et de fournir une gestion de service informatique souple et réactive, tout en réduisant les coûts. Le portefeuille Tivoli comprend des logiciels de sécurité, de conformité, de stockage, d'exécution, de disponibilité, de configuration, d'exploitation et de gestion du cycle de vie informatique, et est appuyé par des services ainsi que des équipes d'assistance technique et de recherche IBM de niveau international.

Pour en savoir plus

Pour en savoir plus sur la manière dont Tivoli Security Operations Manager peut vous permettre de gérer et surveiller les opérations de sécurité de façon centralisée, contactez votre représentant ou partenaire commercial IBM ou visitez le site **ibm.com**/software/fr/tivoli

IBM Corporation
Software Group
Route 100
Somers, NY 10589
Etats-Unis

Produit aux Etats-Unis

6-06

GC28-8415-00