Wüstenrot Gruppe

Profil client
- Grande compagnie autrichienne de services financiers avec une société de prêt immobilier et un groupe d'assurance

Secteur d'activité
- Services financiers

Environnement informatique
- 3 500 employés

Défi
- Remplacer l'ancienne solution SIEM par une nouvelle capable de supporter efficacement l'évolution des besoins de la société

Solution de McAfee
- McAfee Enterprise Security Manager

Résultats
- Implémentation en quinze jours à peine
- Journalisation ultraperformante et précise des données issues de 100 sources
- Gestion de plus de 1 000 événements par minute
- Fonctionnalités robustes de chiffrement et d'archivage des journaux
- Tableaux de bord configurables pour prendre en charge un large éventail de types de données et de rapports

La solution ESM de McAfee garantit une visibilité renforcée sur la sécurité de la société de banque et d'assurance

Forte de plus de 3 500 employés et de 3,5 millions de clients, Wüstenrot Gruppe est l'une des plus grandes sociétés de services financiers d'Autriche. La société comporte deux divisions : une société de crédit immobilier qui offre des services bancaires et des prêts hypothécaires axés sur les projets de construction résidentielle et un groupe d'assurance. Wüstenrot possède des filiales en République tchèque, en Slovaquie, en Hongrie, en Slovénie et en Croatie.

Préoccupation de l'entreprise : sécuriser les activités bancaires et d'assurance

La sécurité des données et des réseaux est un facteur essentiel du succès d'une entreprise active dans les secteurs de la banque et de l'assurance. Pour préserver sa réputation et conserver la confiance de ses clients, Wüstenrot se doit de garantir des niveaux de sécurité optimaux, surtout en ce qui concerne les données clients sensibles et la gestion des réseaux et systèmes bancaires.

Jusque-là, Wüstenrot utilisait IBM Tivoli Compliance Insight Manager pour traiter et analyser les journaux des événements de sécurité, mais cette solution ne parvenait plus à suivre la croissance et l'évolution de la société. Wüstenrot a donc recensé les exigences auxquelles devrait répondre une nouvelle solution de gestion des événements et des informations de sécurité (SIEM). La société était en quête d'une solution « prête à l'emploi » complète, incluant le matériel et le système d'exploitation, qui offrirait des rapports simplifiés, une collecte des journaux sans agent et la prise en charge de normes de surveillance telles que BASEL II, PCI DSS et ISO 27002. Par ailleurs, elle cherchait une solution qui puisse immédiatement mettre à disposition tous les événements survenus au cours des cinq derniers jours et consignerait les données issues d'Oracle HPUX, de Windows Server, de Microsoft SQL Server, de CheckPoint et de McAfee ePolicy Orchestrator (ePO). Wüstenrot souhaitait en outre que le fournisseur de la solution SIEM n'impose pas de restriction de licence sur le nombre de sources de journalisation et donne des garanties quant aux coûts de maintenance.

Pourquoi McAfee : une solution SIEM ultraperformante

Sur la base de ces exigences, McAfee Enterprise Security Manager (ESM) a rapidement fait figure de favori. Mais, avant de prendre sa décision finale, Wüstenrot a décidé de réaliser une preuve de concept (POC) pour tester la solution SIEM. En mode POC, McAfee ESM devait consigner les données de chaque source dans son propre environnement et vérifier que les résultats et performances étaient conformes aux spécifications internes de Wüstenrot. Les intégrateurs systèmes Auriga Systems et COMGUARD ont déployé McAfee ESM en à peine une journée, au cours de laquelle ils ont par ailleurs organisé un bref atelier sur les fonctionnalités avancées de la solution et approuvé conjointement les paramètres à utiliser pour mesurer la réussite du POC. Un mois de fonctionnement a permis à McAfee ESM de démontrer sa capacité à communiquer avec toutes les sources de journalisation requises.

La solution de McAfee

Compte tenu de la réussite du POC et du modèle de tarification favorable de McAfee, Wüstenrot a opté pour le modèle ETM-4600-ELM de McAfee ESM. À même de consigner au moins 1 000 événements par seconde, McAfee ESM était le choix idéal pour répondre aux exigences de Wüstenrot.

L'équipe informatique de Wüstenrot, soutenue par les intégrateurs systèmes, a pu implémenter McAfee ESM en seulement quinze jours ouvrables. La solution a démontré d'excellentes performances et une très grande précision dans l'analyse des journaux en assurant l'extraction à partir de 100 sources de journalisation différentes.

« McAfee Enterprise Security Manager est une solution à la fois très flexible et très efficace, qui nous permet de gérer les événements de plusieurs mois en quelques secondes et d'obtenir immédiatement les informations pertinentes. Les tableaux sont très intuitifs et directement exploitables par l'équipe de sécurité et moi-même. Ils me permettent d'identifier facilement les problèmes et de les résoudre en temps et en heure. »

— Bc. Jiří Dolejš,
Directeur de la sécurité,
Wüstenrot

Une fois toutes les sources de journalisation implémentées, l'équipe chargée de l'implémentation a configuré les tableaux de bord et les rapports conformément aux spécifications convenues au préalable dans plusieurs domaines clés. Parmi celles-ci, citons la modification des niveaux d'autorisation pour Active Directory, les pannes et les redémarrages des serveurs et des services, les événements signalés par l'antivirus dans l'infrastructure et les nouveaux périphériques détectés sur le réseau.

Le support technique de McAfee a apporté une solution rapide et efficace à l'unique problème qui se soit posé pendant l'implémentation, à savoir une incompatibilité de format d'horodatage pour le journal d'audit de la base de données Oracle. McAfee a pu élaborer un format d'horodatage spécial dans le cadre de l'environnement Oracle natif.

Projets futurs

McAfee ESM dépasse largement les attentes initiales de Wüstenrot. En effet, la société, qui voulait pouvoir disposer directement des événements survenus au cours des cinq derniers jours, peut désormais accéder aux informations agrégées des journaux remontant jusqu'à un an pour un traitement immédiat.

La première phase d'implémentation a consisté à lancer la solution SIEM et à injecter les données requises. À présent, Wüstenrot travaille à l'ajout de tableaux de bord analytiques pour certains domaines sur lesquels il est essentiel que le service de sécurité informatique dispose de visibilité. Par ailleurs, la société se concentre sur l'affinage des règles de corrélation, de manière à éliminer les faux positifs en lien avec les règles par défaut.

L'archivage des journaux n'est limité que par la quantité d'espace de stockage disponible. Wüstenrot applique des normes élevées en matière d'intégrité et de confidentialité de ses journaux archivés — raison pour laquelle la société leur a dédié un matériel de stockage spécifique, appliquant les fonctionnalités cryptographiques certifiées de McAfee Enterprise Log Manager (ELM). Wüstenrot, qui entend dans un premier temps archiver ses journaux pour une durée d'un an, est actuellement à pied d'œuvre pour préparer les baies de stockage. La prochaine étape consistera à activer la fonctionnalité d'archivage des journaux avec une indexation pour la recherche en texte intégral proposée par McAfee ELM.

McAfee
An Intel Company

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr