McAfee Enterprise Security Manager

Priorisation, investigation, correction

Une sécurité d'une efficacité optimale nécessite avant tout une parfaite visibilité sur toutes les activités des systèmes, réseaux, bases de données et applications. Elle exige également un cadre de sécurité qui soit lui aussi efficace, avec pour pièce maîtresse une solution de gestion des événements et des informations de sécurité (SIEM, Security Information and Event Management). McAfee® Enterprise Security Manager, le produit phare de la gamme de solutions SIEM de McAfee, offre des performances élevées, des renseignements directement exploitables et une intégration transparente aux solutions, alliés à la vitesse et à l'évolutivité requises par les équipes de sécurité. Il vous permet de prioriser, d'analyser et de contrer rapidement les menaces dissimulées, tout en assurant la conformité.

Principaux avantages

- **Fonctions intelligentes** — Des informations contextuelles très complètes couplées à l'analyse avancée vous permettent de détecter et de prioriser les menaces.
- **Données pertinentes et directement exploitables** — Les données dont vous avez besoin sont présentées dans des vues dynamiques, permettant de choisir entre plusieurs actions : investigation, confinement, correction ou encore adaptation de la réponse en fonction du niveau d'importance des alertes et des modèles de comportement de la menace.
- **Intégration** — La solution surveille et analyse les données issues d'une vaste infrastructure de sécurité hétérogène et propose une intégration bidirectionnelle au moyen d'interfaces ouvertes. Elle permet également d'automatiser de nombreuses mesures immédiates de réponse aux incidents.

McAfee Enterprise Security Manager assure à l'entreprise une connaissance en temps réel du monde extérieur, par des informations sur les menaces et des flux de données de réputation. Il lui procure en outre une visibilité sur ses systèmes, ses données, les risques qu'elle court et les activités se produisant en interne. Votre équipe de sécurité bénéficie d'un accès complet et corrélé au contenu et au contexte nécessaires pour prendre rapidement des décisions sur la base des risques, et ainsi investir au mieux ses ressources dans un paysage des menaces en perpétuelle mutation et un contexte opérationnel dynamique. Disposer de telles informations est indispensable pour étudier les attaques lentes et furtives, rechercher les indicateurs de compromission ou corriger les problèmes mis au jour par les audits. Afin d'intégrer pleinement la gestion des menaces et de la conformité aux opérations de sécurité, McAfee Enterprise Security Manager offre également des outils intégrés conçus pour la gestion de la configuration et des modifications, la gestion des cas et la gestion centralisée des stratégies — tout ce dont vous avez besoin pour améliorer l'efficacité des workflows et de l'équipe chargée des opérations de sécurité. Enfin, pour simplifier les opérations de sécurité, les Content Packs (packs de contenu) disponibles pour McAfee Enterprise Security Manager contiennent des configurations prédéfinies spécialement conçues pour des scénarios de sécurité avancés.

Une solution conçue pour évoluer avec les entreprises

Les équipes chargées des opérations de sécurité doivent sans cesse gagner en efficacité pour collecter et examiner rapidement des volumes croissants de données brutes et analysées à partir des architectures d'entreprise d'aujourd'hui, à la fois dynamiques et distribuées. Pour relever ce défi, McAfee Enterprise Security Manager utilise un système

Déploiement flexible et évolutif

- Grâce à notre modèle de déploiement hybride, vous avez le choix : vous pouvez combiner des appliances physiques et virtuelles avec des options de haute disponibilité, et ajouter des solutions proposées en option par les fournisseurs MSSP (Managed Security Services Provider).
- Nos solutions évoluent avec votre entreprise : les options de déploiement vont d'une appliance individuelle pour les petites entreprises à des solutions distribuées pour les grandes structures.
- Les appliances fortement évolutives permettent une collecte massive de données sur une large gamme de ressources de sécurité et d'infrastructure, et les transforment en informations hiérarchisées et directement exploitables.

de gestion des données (reconnu par les analystes du secteur et les clients comme un point fort des solutions SIEM de McAfee®), élaboré expressément pour le traitement d'importants volumes de données. De plus, son architecture de données hautement évolutive prend en charge l'acquisition, la gestion et l'analyse des données de manière à empêcher que leur collecte, leur recherche et leur conservation ne soient compromises. Cela pourrait en effet mettre en péril les investigations en cas d'indisponibilité ultérieure des données cruciales, de ralentissement des analyses dû aux réponses aux requêtes ou de baisses de performances qui limitent fortement la portée des recherches.

Des informations essentielles disponibles en quelques minutes

Dans certains cas, il est essentiel de pouvoir accéder rapidement aux données d'événements stockées à long terme : par exemple, lorsque vous enquêtez sur des incidents, que vous recherchez des preuves d'attaques avancées ou que vous tentez d'apporter les corrections requises après l'échec d'un audit de conformité. Ces activités nécessitent une visibilité sur les données historiques et un accès complet à tous les détails de chaque événement.

Nos appliances optimisées répondent à ce besoin : elles sont à même de rassembler et de traiter des milliards d'entrées de journal portant sur plusieurs années et de les mettre en corrélation avec d'autres flux de données (y compris des fichiers STIX d'informations sur les menaces), en un minimum de temps. McAfee Enterprise Security Manager est capable de conserver des milliards d'événements et de flux, afin que toutes ces informations soient disponibles immédiatement pour des requêtes ponctuelles, des investigations numériques, des validations de règles ou des vérifications de conformité.

Sensibilité au contexte et au contenu

Des informations contextuelles issues de diverses sources (cyberveille, flux de données de réputation, systèmes de gestion des identités et de l'accès, solutions de gestion de la confidentialité et autres systèmes pris en charge) viennent enrichir l'événement correspondant. Ce contexte offre une meilleure compréhension des événements réseau et de sécurité grâce à un tri précis de leurs données en fonction des liens établis entre ceux-ci et les attributs des ressources ainsi que les stratégies et processus métier.

L'évolutivité et le niveau de performances de McAfee Enterprise Security Manager permettent de collecter davantage d'informations à partir de sources plus nombreuses (documents, transactions, communications et autres contenus applicatifs), ce qui améliore les investigations numériques. Toutes ces données sont rigoureusement indexées, normalisées et corrélées pour garantir la détection d'un éventail plus vaste de risques et de menaces.

Un contexte qui déchiffre les menaces avancées

Tout écart par rapport aux activités normales, qu'il s'agisse du trafic réseau, des actions des utilisateurs ou de l'utilisation des applications, peut indiquer une menace imminente susceptible de mettre à mal vos données ou votre infrastructure. McAfee Enterprise Security Manager mesure l'activité de base relative à toutes les informations collectées et propose des alertes hiérarchisées dans le but de mettre au jour les menaces potentielles avant qu'elles ne frappent, tout en recherchant parmi ces données des comportements pouvant indiquer un danger plus important. De plus, la solution exploite un large éventail d'informations contextuelles, dont elle enrichit chaque événement, vous permettant ainsi de mieux comprendre comment les événements de sécurité peuvent affecter vos processus métier.

Les tableaux de bord de la fonctionnalité Cyber Threat Manager de McAfee Enterprise Security Manager offrent des fonctions améliorées pour surveiller en temps réel et analyser les menaces émergentes. Les informations sur les menaces (qu'elles soient suspectées ou avérées) transmises au moyen de flux STIX et TAXII, par McAfee Advanced Threat Defense et/ou via des URL de sites web de tiers peuvent être agrégées et corrélées en temps quasi réel aux données d'événement ou, au moyen de la fonctionnalité Backtrace, à celles présentes dans l'historique. Les équipes de sécurité peuvent ainsi cerner plus clairement la propagation des menaces au sein de l'environnement. Grâce à cette cyberveille, les entreprises peuvent associer les données pertinentes au personnel adéquat, qui pourra dès lors appliquer les mesures requises quasi instantanément et prendre des décisions plus éclairées.

Optimisation des opérations de sécurité

Spécialement axée sur l'analyse, l'interface utilisateur de McAfee Enterprise Security Manager est plus flexible et facile à personnaliser, et permet de réagir rapidement lors des investigations. Grâce à la rationalisation des workflows, les incidents peuvent être gérés de manière plus efficace et dans des délais plus brefs. L'accès aux informations sur les menaces est bien pensé et rapide, de sorte que les analystes, qu'ils soient novices ou experts, peuvent plus facilement venir à bout des menaces en perpétuelle évolution, de leur priorisation à leur neutralisation en passant par l'investigation.

McAfee Enterprise Security Manager est efficace dès l'installation, sans étape de configuration supplémentaire ; les centaines de rapports, de vues, de règles et d'alertes qu'il propose sont utilisables tels quels, tout en étant faciles à personnaliser si nécessaire. Qu'il s'agisse d'établir une ligne de base de l'utilisation standard du réseau ou simplement de personnaliser les alertes, le tableau de bord de McAfee Enterprise Security Manager permet aisément de visualiser les informations de sécurité, de les étudier et de créer des rapports pour les plus pertinentes d'entre elles. Les entreprises bénéficient désormais d'un accès complet et corrélé aux données et au contexte nécessaires pour prendre rapidement des décisions avisées.

De plus, McAfee Enterprise Security Manager simplifie les opérations de sécurité grâce à ses Content Packs. Ces scénarios de sécurité « prêts à l'emploi » sont préconfigurés et permettent d'accéder rapidement à des fonctions avancées de gestion de la conformité ou des menaces. Ces configurations prédéfinies pour des scénarios courants contiennent des ensembles de règles, d'alertes, de vues, de rapports, de variables et de listes de suivi. De nombreux Content Packs offrent des déclencheurs prédéfinis pour les comportements qui peuvent exiger un examen plus approfondi ou une correction automatique.

Simplification de la mise en conformité

En centralisant et en automatisant la surveillance et les rapports sur la conformité, McAfee Enterprise Security Manager élimine les processus manuels chronophages. De plus, l'intégration au cadre UCF (Unified Compliance Framework) offre une méthodologie commune, sur le principe d'une collecte de données unique mais servant divers objectifs de conformité, qui permet de respecter les obligations de conformité tout en limitant autant que possible les dépenses et les tâches liées aux audits. La prise en charge du cadre UCF optimise le processus de conformité en normalisant les points caractéristiques de chaque réglementation, ce qui permet ensuite de faire correspondre la série unique d'événements collectés aux réglementations individuelles.

McAfee Enterprise Security Manager simplifie et accélère la gestion de la conformité grâce à des centaines de tableaux de bord prédéfinis, des pistes d'audit complètes et des rapports destinés à satisfaire les exigences de plus de 240 réglementations et cadres de contrôle nationaux et internationaux tels que PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX et SOX. En plus de cette prise en charge sans configuration supplémentaire, tous les tableaux de bord, règles et rapports de conformité de McAfee Enterprise Security Manager sont personnalisables à volonté.

Une infrastructure informatique connectée

La solution s'intègre à l'ensemble de votre infrastructure de sécurité, offrant ainsi une visibilité sans précédent et en temps réel sur le niveau de sécurité de votre entreprise. McAfee Enterprise Security Manager est capable de collecter des données pertinentes à partir d'équipements d'autres fournisseurs de solutions de sécurité, de même que des flux de cyberveille sur les menaces. Étant donné qu'elle est intégrée avec McAfee Global Threat Intelligence (McAfee GTI), la solution peut s'enrichir des données recueillies par McAfee Labs à partir de ses sondes réparties à travers le monde (plus de 100 millions) et ainsi bénéficier d'un flux d'informations constamment actualisé sur les adresses IP malveillantes connues. Elle peut également assimiler les informations sur les menaces transmises au format STIX/TAXII et/ou par le biais d'URL de sites web de tiers, et ensuite les analyser pour appliquer les mesures appropriées.

McAfee Enterprise Security Manager propose en outre des intégrations actives avec des dizaines d'autres solutions d'analyse et de gestion des incidents, proposées notamment par McAfee et des partenaires McAfee Security Innovation Alliance.

Par exemple, McAfee Threat Intelligence Exchange, basé sur la surveillance des terminaux, regroupe les informations sur les attaques à faible prévalence, exploitant ainsi une cyberveille sur les menaces issue de sources locales, mondiales et de tiers. De plus, McAfee Threat Intelligence Exchange peut utiliser d'autres produits intégrés, tels que McAfee Advanced Threat Defense, pour analyser les fichiers et déterminer leur caractère malveillant.

Les administrateurs et les équipes chargées de la réponse aux incidents peuvent recourir à McAfee Active Response pour rechercher les fichiers de menaces « jour zéro » qui restent en sommeil sur les systèmes, ainsi que les processus actifs en mémoire. De plus, McAfee Active Response utilise des collecteurs persistants qui surveillent en continu les terminaux pour y rechercher des indicateurs de compromission spécifiques, et vous avertit automatiquement si un tel indicateur est détecté au sein de votre environnement. Contrairement aux approches standard de la sécurité, cette combinaison procure aux entreprises un workflow détaillé en boucle fermée, de la découverte de la menace à l'endiguement de l'attaque et à sa neutralisation.

McAfee propose un système de sécurité intégré qui vous permet de prévenir et de juguler les menaces émergentes. Nous vous aidons à éliminer des menaces plus nombreuses, plus rapidement et avec moins de ressources. Notre architecture connectée et notre gestion centralisée réduisent la complexité et améliorent l'efficacité opérationnelle dans l'ensemble de votre infrastructure de sécurité. Avec ses fonctionnalités de protection complètes et intégrées, McAfee s'engage à être votre partenaire de sécurité privilégié.

En savoir plus

Pour plus d'informations sur McAfee Enterprise Security Manager, visitez le site à l'adresse **www.mcafee.com/fr/products/siem/index.aspx**.

Pour plus d'informations sur nos solutions intégrées, visitez notre site à l'adresse **www.mcafee.com/fr/solutions/intelligent-security-operations.aspx**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/fr