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, applications et cloud. 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 composant phare de la solution SIEM de McAfee, offre des performances élevées, une cyberveille directement exploitable et une intégration transparente aux solutions, avec la vitesse et 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.

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. Elle peut ainsi investir au mieux ses ressources dans un contexte opérationnel dynamique et un paysage des menaces en perpétuelle mutation. Disposer de telles informations est indispensable pour étudier les attaques lentes et furtives, rechercher les indicateurs de compromission ou corriger les problèmes révélés 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. En bref, 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.

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 des menaces.

Gardez le contact

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.

McAfee Enterprise Security Manager est une solution optimisée, conçue pour rassembler et traiter des entrées de journal portant sur plusieurs années et les mettre en corrélation avec d'autres flux de données (au format STIX notamment), 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. Parallèlement, la solution conserve les données à long terme pour les investigations numériques, les validations de règles ou les vérifications de conformité. Par ailleurs, les données peuvent être immédiatement répliquées dans plusieurs emplacements de stockage, assurant la continuité des activités.

Flexibilité de déploiement

McAfee Enterprise Security Manager peut être déployé dans le centre de données du client, soit sous la forme d'une solution matérielle installée sur site, soit dans le cloud via McAfee Enterprise Security Manager Cloud.

Le déploiement sur site est l'option recommandée pour les clients traitant d'importants volumes de données ou soumis à des législations en matière de confidentialité des données qui leur imposent de conserver les informations au sein de leur entreprise. Par ailleurs, ces clients possèdent généralement le personnel nécessaire au déploiement, à l'utilisation et à la gestion de la solution.

La seconde option de déploiement, McAfee Enterprise Security Manager Cloud, convient mieux aux clients dotés de plus petites équipes et ayant des besoins plus limités en matière de collecte de données. La solution élimine les obstacles opérationnels en assurant un déploiement automatisé, une surveillance ininterrompue de l'intégrité des systèmes, des mises à jour logicielles régulières, l'application automatisée des patchs, laissant ainsi à ces équipes plus réduites la possibilité de concentrer leurs efforts sur les tâches de sécurité.

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 les énormes volumes de données brutes et analysées que génèrent les architectures d'entreprise modernes, à la fois dynamiques et distribuées. Pour relever ce défi, McAfee Enterprise Security Manager utilise un bus de données ouvert et évolutif, 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.

Principaux avantages (suite)

- **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.
- **Flexibilité de déploiement :** La solution peut être déployée sur site ou dans le cloud, en fonction des exigences, besoins et préférences des clients.

De telles compromissions portent préjudice aux investigations dès lors que les données cruciales sont indisponibles, les analyses sont ralenties par les requêtes ou les faibles performances limitent la portée des recherches.

Sensibilité au contexte et au contenu

Chaque événement est enrichi par 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). Cet enrichissement des informations permet de mieux comprendre la relation entre les événements réseau et de sécurité d'une part, et les ressources, les stratégies et les processus métier d'autre part.

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.

Une analyse approfondie pour une interprétation judicieuse

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 avec niveau de priorité, dans le but d'identifier 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 enrichit chaque événement par des informations contextuelles, vous permettant ainsi de mieux comprendre comment les événements de sécurité peuvent affecter vos processus métier.

La fonctionnalité Cyber Threat Manager propose des tableaux de bord qui assurent une surveillance en temps réel et une analyse pointue des menaces émergentes. Les informations sur les menaces, qu'elles soient suspectées ou avérées, sont transmises au moyen de flux STIX et TAXII, McAfee® Advanced Threat Defense et/ou des sites web externes. Elles peuvent être agrégées et corrélées en temps quasi réel aux données d'événement ou, au moyen de la fonctionnalité Backtrace, aux données d'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 des mesures quasi instantanément et prendre des décisions plus éclairées.

Optimisation des opérations de sécurité

Adaptée aux besoins des analystes, l'interface utilisateur de McAfee Enterprise Security Manager est 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. Les analystes de tout niveau de compétence, débutants ou experts, pourront ainsi plus facilement prioriser, analyser et contrer les menaces en évolution constante.

McAfee Enterprise Security Manager est efficace dès l'installation, sans étape de configuration supplémentaire. Les centaines de rapports, vues, règles et alertes prédéfinis 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 de visualiser aisément 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 « prêts à l'emploi » qui permettent d'accéder rapidement à des fonctions avancées de gestion de la conformité ou des menaces. Ces configurations prédéfinies correspondant à des cas d'utilisation courants contiennent des ensembles de règles, alertes, vues, rapports, variables et 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. Cette approche 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 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. Intégrée avec McAfee® Global Threat Intelligence (McAfee® GTI), la solution peut s'enrichir des données sur les menaces recueillies par McAfee® Labs à partir de ses sondes 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 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 externes. 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 analystes bénéficient également de l'intégration avec McAfee® Behavioral Analytics, une solution dédiée d'analyse du comportement des utilisateurs et des entités qui réduit plusieurs milliards d'événements de sécurité à quelques centaines d'anomalies et une poignée de pistes de menaces priorisées. Cette technologie permet aux analystes de découvrir les menaces de sécurité à haut risque et inhabituelles, souvent impossibles à identifier pour les autres solutions. De même, McAfee Enterprise Security Manager s'intègre à McAfee® Investigator pour transformer les analystes en enquêteurs chevronnés : ils peuvent résoudre les incidents plus rapidement et en déterminer la cause sous-jacente avec un plus grand degré de certitude.

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 à la recherche d'indicateurs de compromission précis, et vous avertit automatiquement si ces indicateurs sont détectés 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 plus de menaces, 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 est votre partenaire de sécurité privilégié.

En savoir plus

Pour plus d'informations sur McAfee Enterprise Security Manager, consultez les pages suivantes : **www.mcafee.com/siem** et **www.mcafee.com/esm**.

Pour plus d'informations sur nos solutions intégrées, visitez notre site à l'adresse **www.mcafee.com/secops**.

1-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr