FICHE TECHNIQUE

McAfee Global Threat Intelligence for Enterprise Security Manager

Le fruit des recherches de McAfee® Labs au service de la connaissance situationnelle

McAfee® Global Threat Intelligence for Enterprise Security Manager met les compétences de McAfee Labs au service de la surveillance de la sécurité d'entreprise. Pour la première fois, une solution SIEM peut disposer d'une évaluation des réputations des adresses IP, déterminées par McAfee Labs à partir de plus de 100 millions de sondes à travers le monde chargées de collecter des informations sur les menaces. Ce flux d'informations riche et constamment mis à jour dont bénéficie McAfee Enterprise Security Manager améliore la connaissance situationnelle en permettant une détection rapide des événements impliquant une communication avec des adresses IP suspectes ou malveillantes. Les administrateurs responsables de la sécurité peuvent ainsi déterminer quels hôtes ont communiqué ou communiquent avec des interlocuteurs malveillants. Ils identifient rapidement les situations dans lesquelles une entité cybercriminelle connue a été la source d'une menace.

Nécessité d'un contexte externe

Les événements de sécurité fournissent des informations sur les activités liées à la sécurité au moment où elles se produisent. Même si une solution SIEM est capable de corréler ces événements, l'opérateur doit néanmoins répondre à une série de questions : Cette activité est-elle acceptable ? Qu'est-ce qui est le plus urgent ? Comment détecter des attaques sophistiquées qui laissent peu de traces ? Multipliez ces questions par le nombre d'événements quotidiens d'une entreprise normale (plus de 250 millions) et il est clair que la détection de comportements connus, sur lesquels se concentrent les anciennes solutions SIEM, ne représentent que le sommet de l'iceberg en matière de surveillance de la sécurité. L'un des éléments contextuels les plus importants derrière cette inconnue est la compréhension de la réputation des systèmes externes. Jusqu'ici, il était impossible d'appréhender clairement les événements de sécurité.

Principaux avantages

- Le fruit des recherches de McAfee Labs au profit des solutions SIEM
- Compréhension des risques liés aux événements
- Exploitation du flux massif de données sur les menaces de McAfee GTI sans affecter les performances
- Réception et traitement automatique d'informations sur la réputation de nouvelles sources dans McAfee Enterprise Security Manager
- Amélioration de la précision de détection des menaces et diminution des temps de réponse
- Identification rapide des vecteurs d'attaque et des interactions passées avec des intervenants malveillants connus, associées à toutes sortes d'activités malveillantes (botnets, attaques DDoS, expéditeurs de spam/e-mails dissimulant du sondage réseau, logiciels malveillants, hébergement DNS, intrusions, etc.)

Les compétences de McAfee Labs intégrées aux solutions SIEM

McAfee Global Threat Intelligence for Enterprise Security Manager intègre directement le fruit des recherches de McAfee Labs au flux de surveillance de la sécurité grâce aux solutions SIEM ultrarapides et extrêmement intelligentes de McAfee, conçues pour les gros volumes de données de sécurité. Ce service par abonnement en option évalue et adapte la réputation des sources pour plus de 140 millions d'adresses IP, en injectant directement le contexte des réputations des systèmes externes dans le flux d'événements de sécurité. De cette manière, il permet l'identification rapide des interactions présentes et passées avec des intervenants connus pour leur comportement délictueux. Dans McAfee Global Threat Intelligence (GTI), la réputation des adresses IP provient de la mise en corrélation des renseignements provenant des principaux vecteurs de menaces. Cette fonction exploite plus de 100 millions de sondes dans le monde entier et s'appuie sur le travail de plus de 500 chercheurs.

Avantages de McAfee Global Threat Intelligence for Enterprise Security Manager

- **Protection renforcée de l'ensemble du réseau :** McAfee Global Threat Intelligence for Enterprise Security Manager détecte instantanément toute communication d'un nœud de votre réseau avec un intervenant suspect ou connu pour son comportement délictueux, ainsi que la voie empruntée par la menace.
- **Priorisation selon le niveau de risque :** La réputation des adresses IP est intégrée automatiquement dans l'algorithme d'évaluation du risque de McAfee Enterprise Security Manager, qui fonctionne indépendamment de règles, afin de déterminer automatiquement la nécessité d'une réponse.
- **Surveillance des menaces 24 h/24 et 7 j/7 :** McAfee Labs analyse en permanence les informations sur les menaces afin de détecter les systèmes malveillants et infectés depuis peu. Ensuite, après le nettoyage des systèmes compromis, McAfee Labs fournit des informations précises et à jour sur le paysage mondial des menaces.

Détection des activités malveillantes en temps réel

Grâce à McAfee Global Threat Intelligence for Enterprise Security Manager, les entreprises peuvent connaître la réputation de l'adresse IP impliquée dans n'importe quel événement, qu'il concerne les pare-feux, les systèmes de prévention des intrusions, les routeurs ou les terminaux de tous types. En se fondant sur les listes de surveillance de McAfee Enterprise Security Manager, les événements sont automatiquement associés au score de réputation de la source et le risque est ajusté. À mesure que le paysage mondial des menaces évolue, McAfee GTI met à jour McAfee Enterprise Security Manager pour garantir aux serveurs et systèmes des scores de réputation toujours fiables. Les entreprises peuvent ainsi mieux appréhender le risque, mais aussi identifier les problèmes urgents en temps réel, ce qui réduit le délai de réponse aux incidents et fournit une analyse précise des risques.

Découverte d'éléments inconnus

Un des principaux atouts de McAfee Enterprise Security Manager est sa capacité à stocker et à récupérer des années de données et à effectuer une corrélation historique. En outre, avec McAfee GTI, les analystes en sécurité peuvent remonter dans le temps et analyser des données sur plusieurs années pour comprendre les interactions passées avec des entités malveillantes. De telles fonctions sont essentielles pour détecter les attaques discrètes et lentes, les activités répétées des botnets, les scripts intersites et les tentatives d'injection SQL.

Réduction du temps de réponse

L'intégration transparente de McAfee GTI avec les mécanismes d'alarme et d'alerte de McAfee Enterprise Security Manager permet de s'assurer que les interactions avec des systèmes malveillants connus reçoivent l'attention qu'elles méritent.

Une solution alimentée par la base de données McAfee et conçue pour le Big Data en sécurité

On a beaucoup parlé de la croissance explosive des données. L'un des points positifs du phénomène des Big Data est l'intégration possible aux solutions SIEM de la mine de connaissances sur la sécurité produites par McAfee Labs. McAfee Enterprise Security Manager est unique en cela qu'il peut stocker, corréler et mettre à jour l'énorme base de données des réputations IP de McAfee GTI, sans grand impact sur les performances. McAfee Enterprise Security Manager possède une base de données propriétaire qui allège la charge d'administration de la base de données pour la solution SIEM. Cette base de données a été spécialement conçue pour la réception et le traitement en masse de données relationnelles et d'événements à des débits extrêmement élevés. Avec McAfee Global Threat Intelligence for Enterprise Security Manager, les clients sont assurés de recevoir la cyberveille de McAfee GTI en temps réel.

Spécifications

Versions prises en charge
McAfee Enterprise Security Manager 9.4 et McAfee Event Reporter Appliance 9.4

- Réseau de cyberveille de McAfee Labs : plus de 100 millions de postes dans plus de 120 pays
- Scores de réputation moyens des adresses IP : varient selon le paysage des menaces

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr