McAfee Advanced Correlation Engine

Détection des menaces axée sur vos ressources prioritaires

Aujourd'hui, la sophistication des menaces est telle qu'elle tient en échec les systèmes de détection classiques, fondés sur les règles. En déployant la solution McAfee® Advanced Correlation Engine avec McAfee Enterprise Security Manager, vous pouvez identifier les événements de menace et leur attribuer un score en temps réel à l'aide d'une logique basée à la fois sur les règles et sur les risques. Il vous suffit de définir dans McAfee Advanced Correlation Engine les ressources que vous jugez importantes, par exemple des utilisateurs ou groupes, des applications, des serveurs spécifiques ou des sous-réseaux : la solution vous avertit lorsque ces ressources sont menacées. Les pistes d'audit et les simulations de données historiques permettent les investigations numériques, les évaluations de conformité ainsi que l'optimisation des règles.

La solution McAfee Advanced Correlation Engine complète la corrélation d'événements de McAfee Enterprise Security Manager grâce à deux moteurs de corrélation dédiés et à des fonctions spécialisées :

- Un moteur de détection des risques qui génère un score de risque à l'aide d'une corrélation des scores de risque sans règles
- Un moteur de détection des menaces qui identifie les menaces à l'aide de la corrélation des événements classique, basée sur les règles

Autonome, la solution McAfee Advanced Correlation Engine possède la puissance de traitement nécessaire pour prendre en charge la corrélation complète des événements dans l'ensemble de votre entreprise. Son moteur de traitement des données évolutif lui permet de s'adapter aux plus grands réseaux.

Détection historique et en temps réel des menaces

Vous pouvez déployer la solution McAfee Advanced Correlation Engine en mode historique ou temps réel. En mode temps réel, elle analyse les événements au moment où ils sont collectés afin de détecter immédiatement les risques et les menaces :

- Corrélation, fondée sur les règles et en temps réel, des données d'événements pour détecter les menaces dès leur apparition

Principaux avantages

- Démarrage simplifié : aucune mise à jour de règles, optimisation de signatures ou autre configuration complexe requise
- Génération d'alertes lorsque les menaces visent des utilisateurs, des ressources, des applications et des activités considérés comme prioritaires
- Établissement d'un score précis grâce à des procédures simultanées de corrélation avec et sans règles
- Vérification des nouvelles attaques et vulnérabilités par rapport à votre historique afin d'identifier des événements passés
- Ajout de ressources de traitement et de corrélation spécialisées à McAfee Enterprise Security Manager
- Déploiement possible sous la forme d'une appliance physique ou virtuelle

- Corrélation en temps réel et sans règles des données d'événements pour détecter les menaces à mesure qu'elles évoluent

En mode historique, toutes les données recueillies peuvent être traitées à nouveau par les deux moteurs de corrélation afin de fournir une détection récursive des risques et des menaces. Lors de la détection d'attaques de type « jour zéro », la solution McAfee Advanced Correlation Engine peut réexaminer les données historiques pour déterminer si votre entreprise a été exposée à cette attaque par le passé et révéler l'occurrence de menaces s'étant manifestées avant leur identification formelle.

Aucun impact sur les performances

Comme la solution McAfee Advanced Correlation Engine est une appliance autonome ou virtuelle, elle n'a aucun impact sur les performances de McAfee Enterprise Security Manager en termes de collecte et de gestion des événements. Vous pouvez tirer pleinement parti de toutes les fonctionnalités de McAfee Advanced Correlation Engine tout en optimisant l'outil McAfee Enterprise Security Manager.

Corrélation des événements basée sur des règles

La corrélation des événements basée sur les règles fait appel à une logique de corrélation classique pour analyser les informations recueillies en temps réel. Tous les journaux, événements et flux réseau sont mis en corrélation avec d'autres informations contextuelles telles que les identités, les rôles, les vulnérabilités et d'autres données afin de détecter des comportements susceptibles d'indiquer une menace de plus grande ampleur. Bien que la corrélation fondée sur les règles et mise en œuvre à l'échelle du réseau soit déjà directement prise en charge sur toutes les solutions McAfee Enterprise Security Manager, McAfee Advanced Correlation Engine fournit une ressource de traitement dédiée, capable de corréler des volumes encore plus importants de données. La solution permet donc soit de compléter les processus de corrélation existants, soit de les prendre complètement en charge.

Corrélation des scores de risque sans règles

Même si la corrélation fondée sur les règles constitue une fonctionnalité précieuse et indispensable de n'importe quel système de gestion des événements et des informations de sécurité (SIEM) traditionnel, ces systèmes ne peuvent détecter que les comportements de menaces connus et nécessitent une mise à jour et une optimisation constantes pour être efficaces. La solution consiste à compléter la corrélation classique des événements par une technologie de corrélation dite « sans règles ». Avec de tels systèmes, les signatures de détection sont remplacées par une configuration simple et unique : il suffit d'indiquer à la solution McAfee Advanced Correlation Engine les ressources prioritaires de votre entreprise. Il peut s'agir d'un service ou d'une application particulière, d'un groupe d'utilisateurs ou encore de types de données spécifiques.

Suivi et alertes en temps réel

La solution McAfee Advanced Correlation Engine commence ensuite à effectuer un suivi de toutes les activités liées à ces ressources et crée un score de risque dynamique qui augmente ou diminue en fonction des activités en temps réel. Lorsqu'un score de risque dépasse un certain seuil, McAfee Advanced Correlation Engine génère un événement. Ce dernier peut servir à avertir un analyste en sécurité d'une probabilité croissante de la présence de menaces, ou être utilisé par le moteur de corrélation classique, fondé sur les règles, comme condition d'un incident de plus grande ampleur. La solution McAfee Advanced Correlation Engine conserve une piste d'audit complète des scores de risque, qui permet de procéder à des analyses et à des investigations approfondies sur les facteurs de menace au fil du temps.

Cas d'utilisation

Modélisation des risques de l'entreprise

La solution McAfee Advanced Correlation Engine offre une plate-forme de modélisation efficace des risques propres à votre entreprise. L'accès à des documents ultraconfidentiels par des employés possédant une habilitation de sécurité élevée peut constituer un risque pour un organisme de défense, au même titre que la divulgation du dossier médical d'un patient célèbre atteint d'une maladie grave pour un établissement hospitalier. La solution McAfee Advanced Correlation Engine assure une modélisation parfaite de vos risques organisationnels en attribuant des scores aux critères pertinents, ce qui permet de créer une référence et d'envoyer des notifications en cas de dépassement des seuils normaux.

Évaluations proactives des risques portant sur des données critiques

Dans la mesure où McAfee Advanced Correlation Engine surveille les données en temps réel, il est possible d'utiliser simultanément les deux moteurs de corrélation pour détecter les risques et les menaces avant qu'ils n'affectent vos systèmes. Les scores de risque peuvent être intégrés à la logique de corrélation traditionnelle. Ainsi, une signature de détection de menace traditionnelle (basée sur des règles) peut être un « événement lié à un logiciel malveillant se produisant après une attaque en force ». Normalement, cette signature n'est déclenchée qu'après la survenue d'un événement. Par contre, avec la solution McAfee Advanced Correlation Engine, vous pouvez désormais incorporer un facteur de risque, telle qu'une augmentation de 20 % du score de risque à la suite d'un événement d'attaque en force. Lorsque cet événement est détecté, McAfee Advanced Correlation Engine peut générer une alerte proactive d'un incident imminent, ce qui permet d'intervenir avant tout dommage.

Évaluation récursive des menaces

Lorsqu'une menace ou une compromission est mise au jour, il est logique de se demander à quand remonte son existence. En déployant la solution McAfee Advanced Correlation Engine en mode historique, vous pouvez réanalyser des données historiques dans les deux moteurs de corrélation (avec et sans règles).

L'identification du moment précis de l'apparition d'une menace récemment découverte permet de déterminer plus facilement la cause de cette situation.

Modes de fonctionnement

Mode de corrélation en temps réel :

- Corrélation, fondée sur les règles et en temps réel, des données d'événements pour détecter les menaces dès leur apparition
- Corrélation en temps réel et sans règles des données d'événements pour détecter les menaces à mesure qu'elles évoluent

Mode de corrélation historique :

- Corrélation, fondée sur les règles, des données d'événements historiques pour une détection récursive des menaces
- Corrélation sans règles des données d'événements historiques pour une évaluation récursive des menaces

Fonctionnalités de corrélation

- Procédures simultanées de corrélation avec et sans règles
- Corrélation des données issues de n'importe quelle source de données prise en charge
- Corrélation des données recueillies dans des réseaux distribués et auprès de systèmes de collecte
- Inclusion de centaines de règles prédéfinies de corrélation des événements
- Éditeur de configurations pour la corrélation sans règles
- Éditeur de règles de corrélation des événements doté d'une interface utilisateur graphique conviviale pour personnaliser ou créer des règles

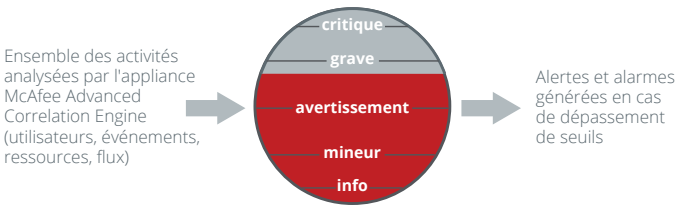

Figure 1. La corrélation fondée sur les risques permet de détecter des menaces imminentes sur les ressources prioritaires.

En savoir plus

Pour en savoir plus, visitez notre site à l'adresse : **www.mcafee.com/fr/products/siem/index.aspx**.

McAfee
Together is power.

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

McAfee et le logo McAfee sont des marques commerciales ou des marques commerciales déposées de McAfee, LLC ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs. Copyright © 2017 McAfee, LLC
41606ds_adv-corr-engine_1112B
NOVEMBRE 2012