McAfee Advanced Correlation Engine

Erkennung von Bedrohungen für Ihre wichtigsten Ressourcen

Heutige Bedrohungen umgehen auf subtile Weise herkömmlichen regelbasierten Bedrohungsschutz. Wenn Sie die Lösung McAfee® Advanced Correlation Engine mit McAfee Enterprise Security Manager kombinieren, können Sie Bedrohungsereignisse mithilfe einer regel- und risikobasierten Logik in Echtzeit identifizieren und bewerten. Zuerst legen Sie fest, welche Ressourcen Sie als besonders wichtig einstufen – Benutzer oder Benutzergruppen, Anwendungen, bestimmte Server oder Subnetze. Anschließend erhalten Sie eine Warnmeldung, wenn diese Ressource gefährdet ist. Dank Audit-Protokollen und Verlaufswiedergaben werden forensische Analysen, Compliance-Vorgänge und Regelanpassungen unterstützt.

Die Lösung McAfee Advanced Correlation Engine ergänzt die Ereigniskorrelation von McAfee Enterprise Security Manager um zwei dedizierte Korrelationsmodule mit speziell angepassten Funktionen:

- Ein Risikoerkennungsmodul, das mithilfe einer regellosen Risikobewertungskorrelation eine Risikoeinstufung generiert
- Ein Bedrohungserkennungsmodul, das Bedrohungen mithilfe herkömmlicher regelbasierter Ereigniskorrelation erkennt

Die eigenständige Lösung McAfee Advanced Correlation Engine bietet die Verarbeitungsleistung, die für die umfassende Ereigniskorrelation im gesamten Unternehmen erforderlich ist. Deren Datenmodul kann auch für die größten Netzwerke skaliert werden.

Echtzeit-Bedrohungserkennung und Erkennung bereits erfolgter Angriffe

Die Lösung McAfee Advanced Correlation Engine kann im Echtzeit- oder Verlaufsmodus eingesetzt werden. Im Echtzeitmodus analysiert sie Ereignisse unmittelbar nach deren Erfassung, um Bedrohungen und Risiken sofort erkennen zu können.

- Regelbasierte Korrelation anhand von Echtzeit-Ereignisdaten zur Erkennung von Bedrohungen sofort nach deren Eintreten
- Regellose Korrelation anhand von Echtzeit-Ereignisdaten zur Erkennung von Bedrohungen, die sich gerade entwickeln

Hauptvorteile

- Vereinfachte Einrichtung: keine Regelaktualisierungen, Signaturanpassungen oder anderen Probleme
- Warnmeldungen bei Auftreten von Bedrohungen, die Ihre wichtigsten Benutzer, Ressourcen, Anwendungen und Aktivitäten gefährden
- Genaue Bewertungen dank gleichzeitig regelbasierter und regelloser Korrelation
- Prüfung vergangener Ereignisse bei Auftreten neuer Angriffe und Schwachstellen, um bereits erfolgte Angriffe zu erkennen
- Zusätzliche Korrelations- und Verarbeitungs-Ressourcen für McAfee Enterprise Security Manager
- Als Hardware- und virtuelle Appliance erhältlich

Im Verlaufsmodus können Sie erfasste Daten mithilfe beider Korrelationsmodule „nachspielen“, um Bedrohungen und Risiken im Nachhinein zu erkennen. Wenn Zero-Day-Angriffe erkannt werden, ermittelt McAfee Advanced Correlation Engine anhand von Verlaufsdaten, ob Ihr Unternehmen bereits über diese Schwachstelle angegriffen wurde (Erkennung potenzieller Zero-Day-Angriffe).

Leistung genau dort, wo Sie sie benötigen

Da McAfee Advanced Correlation Engine als eigenständige Hardware oder virtuelle Appliance angeboten wird, beeinträchtigt sie die Leistung der Ereigniserfassung und -verwaltung von McAfee Enterprise Security Manager in keiner Weise. Sie können alle Funktionen der McAfee Advanced Correlation Engine nutzen, ohne Kompromisse eingehen zu müssen, und gleichzeitig den vollen Nutzen aus McAfee Enterprise Security Manager ziehen.

Regelbasierte Ereigniskorrelation

Bei der regelbasierten Ereigniskorrelation wird zur Analyse in Echtzeit erfasster Informationen herkömmliche Korrelationslogik eingesetzt. Alle Protokolle, Ereignisse und Netzwerkdatenflüsse werden – zusammen mit Kontext-informationen wie Identität, Rollen, Schwachstellen und anderen Faktoren – zueinander in Beziehung gesetzt, um Muster zu erkennen, die auf größere Bedrohungen hinweisen. Während die netzwerkweite, regelbasierte Korrelation bereits direkt von allen McAfee Enterprise Security Manager-Lösungen unterstützt wird, stellt McAfee Advanced Correlation Engine eine dedizierte Verarbeitungs-Ressource dar, die noch umfangreichere Datenvolumina analysiert und wahlweise vorhandene Korrelations-Ressourcen ergänzt oder komplett ersetzt.

Regellose Korrelation mit Risikobewertungen

Die regelbasierte Korrelation ist eine wichtige und wertvolle Funktion für alle SIEM-Systeme (Sicherheits-informations- und Ereignis-Management). Mit dieser Funktion können jedoch nur bekannte Bedrohungs-muster erkannt werden, sodass sie nur dann effektiv ist, wenn die Signatur permanent angepasst und aktualisiert wird. Der richtige Weg besteht folglich darin, herkömmliche Ereigniskorrelation durch „regellose“ Korrelation zu ergänzen. Bei diesen Systemen werden die Erkennungssignaturen durch eine einfache, einmalig durchzuführende Konfiguration ersetzt: Sie legen in den Einstellungen von McAfee Advanced Correlation Engine fest, welche Ressourcen in Ihrem Unternehmen besonders wichtig sind. Hierbei kann es sich um einen bestimmten Dienst oder eine Anwendung, eine Benutzer-gruppe oder einen bestimmten Datentyp handeln.

Echtzeitüberwachung und Warnmeldungen

McAfee Advanced Correlation Engine überwacht anschließend alle Aktivitäten, die mit diesen Ressourcen in Zusammenhang stehen, und erstellt einen dynamischen Risikowert, der stets an die tatsächlichen Echtzeitaktivitäten angepasst wird. Wenn das Risiko einen bestimmten Schwellenwert überschreitet, wird in McAfee Advanced Correlation Engine ein Ereignis generiert, das als Auslöser für eine Warnung über wachsende Bedrohungen an einen Sicherheitsanalysten dient oder vom herkömmlichen Korrelationsmodul als Bedingung für einen größeren Zwischenfall eingesetzt wird. McAfee Advanced Correlation Engine speichert ein vollständiges Audit-Protokoll der Risikowerte, damit der Verlauf der Bedrohungsbedingungen vollständig analysiert und untersucht werden kann.

Anwendungsszenarien

Darstellung des Unternehmensrisikos

McAfee Advanced Correlation Engine bietet eine Möglichkeit, das Risiko Ihres Unternehmens effektiv abzubilden. Für ein Unternehmen ist der Zugriff auf streng vertrauliche Dokumente durch Mitarbeiter mit weit reichenden Zugriffsberechtigen genauso risikoreich wie die Kompromittierung der Patientenakte eines schwer erkrankten Prominenten für ein Krankenhaus. Da McAfee Advanced Correlation Engine bei der Darstellung von Unternehmensrisiken die für Sie wesentlichen Faktoren berücksichtigt, ist diese Übersicht besonders hilfreich. Zudem werden eine Basislinie entwickelt und bei Überschreitung eines bestimmten Werts Benachrichtigungen gesendet.

Präventive Risikobewertungen zum Schutz wichtiger Daten

Da McAfee Advanced Correlation Engine Echtzeitdaten überwacht, können beide Korrelationsmodule gleichzeitig zur Erkennung von Risiken und Bedrohungen noch vor ihrem Eintreten eingesetzt werden. Innerhalb der herkömmlichen Korrelationslogik werden Risikowerte verwendet. Beispielsweise kann eine herkömmliche regelbasierte Bedrohungssignatur auf ein „Malware-Ereignis nach einem Brute-Force-Anmeldeversuch“ hinweisen. Wenn diese Bedingung erfüllt wird, ist ein solches Ereignis normalerweise bereits eingetreten. Mit McAfee Advanced Correlation Engine können Sie jetzt einen Risikofaktor einbeziehen und beispielsweise festlegen, dass der Risikowert nach einem Brute-Force-Angriff um 20 Prozent steigt. In diesem Fall sendet McAfee Advanced Correlation Engine proaktiv eine Warnmeldung über einen anstehenden Zwischenfall, sodass noch vor Auftreten eines Schadens Gegenmaßnahmen ergriffen werden können.

Nachträgliche Bedrohungsbewertung

Nach der Bekanntgabe einer Bedrohungen oder Kompromittierung tritt immer wieder die Frage auf, ob diese Schwachstelle schon länger besteht. Wenn Sie McAfee Advanced Correlation Engine im Verlaufsmodus einsetzen, können die gespeicherten Verlaufsdaten mithilfe der herkömmlichen und der regellosen Module „nachgespielt“ werden.

Wenn Sie feststellen können, wann eine Bedrohung zum ersten Mal auftrat, steigt die Wahrscheinlichkeit, dass die eigentliche Ursache hierfür gefunden werden kann.

Betriebsmodi

Echtzeit-Korrelation:

- Regelbasierte Korrelation anhand von Echtzeit-Ereignisdaten zur Erkennung von Bedrohungen sofort nach deren Eintreten
- Regellose Korrelation anhand von Echtzeit-Ereignisdaten zur Erkennung von Bedrohungen, die sich gerade entwickeln

Verlaufskorrelation:

- Regelbasierte Korrelation von Verlaufsdaten zur Erkennung rekursiver Bedrohungen
- Regellose Korrelation von Verlaufsdaten zur Analyse rekursiver Bedrohungen

Korrelationskapazität

- Gleichzeitige Durchführung regelbasierter und regelloser Korrelation
- Korrelation von Daten aus allen unterstützten Datenquellen
- Korrelation von Daten über verteilte Netzwerke und Erfassungssysteme hinweg
- Beinhaltet hunderte vordefinierter Ereigniskorrelationsregeln
- Beinhaltet Konfigurations-Editor zur Anpassung der regellosen Korrelation
- Beinhaltet Ereigniskorrelationsregel-Editor mit einfach bedienbarer Benutzeroberfläche zur Anpassung vorhandener oder Erstellung neuer Regeln

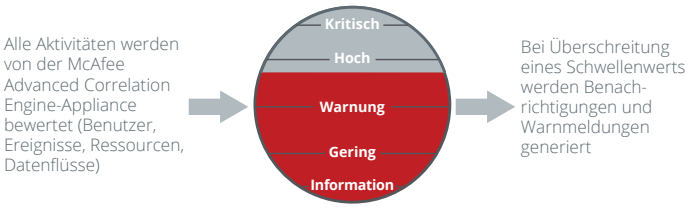

Abbildung 1. Die risikobasierte Korrelation ermöglicht die Erkennung von Bedrohungen in Ihren wichtigsten Ressourcen.

Weitere Informationen

Weitere Informationen finden Sie unter **www.mcafee.com/de/products/siem/index.aspx**.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de

41606ds_adv-corr-engine_1112B
NOVEMBER 2012