DATENBLATT

McAfee Global Threat Intelligence for Enterprise Security Manager

Verschaffen Sie sich dank McAfee® Labs einen besseren Überblick über die Sicherheitslage.

McAfee® Global Threat Intelligence for Enterprise Security Manager nutzt die Leistungsfähigkeit von McAfee Labs für die Überwachung der Unternehmenssicherheit. Zum ersten Mal stehen IP-Bewertungen – die McAfee Labs von mehr als 100 Millionen Bedrohungssensoren weltweit sammelt – für eine SIEM-Lösung (Sicherheitsinformations- und Ereignis-Management) zur Verfügung. Dieser fortlaufend aktualisierte, umfangreiche Feed für McAfee Enterprise Security Manager sorgt für einen besseren Überblick über die Sicherheitslage, da er die schnelle Erkennung von Ereignissen ermöglicht, bei denen Kommunikationen mit verdächtigen oder böswilligen IP-Adressen stattfinden. Sicherheitsadministratoren können dann bestimmen, welche Hosts mit böswilligen Akteuren kommuniziert haben oder gerade kommunizieren, und schnell Situationen ermitteln, bei denen ein böswilliger Akteur die Quelle der Bedrohungsaktivität war.

Bedeutung externer Kontextinformationen

Sicherheitsereignisse liefern Informationen über sicherheitsbezogene Aktivitäten zu einem bestimmten Zeitpunkt. Ein SIEM-System kann diese Ereignisse zwar zueinander in Beziehung setzen, aber für den Operator bleiben noch zahlreiche Fragen offen: Ist die Aktivität zulässig? Wie stelle ich fest, was am dringendsten ist? Wie erkenne ich komplexe Angriffe, die kaum Aufsehen erregen? Multiplizieren Sie diese Fragen mit den Ereignissen eines Tages in einem normalen Unternehmen – also mit über einer Viertelmilliarde – und Ihnen ist klar, dass die Erkennung bekannter Muster, auf die sich herkömmliche SIEM-Systeme konzentrieren, bei der Sicherheitsüberwachung nur die Spitze des Eisbergs ausmacht. Zu den wichtigsten Kontextdetails des noch Unbekannten zählt die Bewertung externer Systeme. Bislang war es nicht möglich, sich ein derart klares Verständnis in Bezug auf Sicherheitsereignisse zu verschaffen.

Hauptvorteile

- Nutzen Sie die Leistungsfähigkeit von McAfee Labs für SIEM.
- Machen Sie sich das mit einem Ereignis verbundene Risiko klar.
- Nutzen Sie den umfangreichen Bedrohungsdaten-Feed von McAfee GTI ohne Beeinträchtigung der Systemleistung.
- Empfangen und verarbeiten Sie automatisch neue Quellenbewertungen in McAfee Enterprise Security Manager.
- Erhöhen Sie die Genauigkeit der Bedrohungserkennung bei gleichzeitiger Verringerung der Reaktionszeit.
- Erkennen Sie in kürzester Zeit Angriffspfade und zurückliegende Interaktionen mit als böswillig bekannten Akteuren, die im Zusammenhang stehen mit Botnets, DDoS-Angriffen (Distributed Denial-of-Service), Malware, die E-Mails- und Spam sendet und versucht, auf das Netzwerk zuzugreifen, Malware-Präsenz, DNS-Hosting sowie Aktivitäten, die durch Angriffsversuche generiert wurden.

Leistungsfähigkeit von McAfee Labs direkt in SIEM eingebunden

McAfee Global Threat Intelligence for Enterprise Security Manager wurde für umfangreiche Sicherheitsdaten entwickelt und setzt die Leistung von McAfee Labs per schnellem und hochintelligentem McAfee-SIEM-System direkt in der Sicherheitsüberwachung um. Dieser optionale Abonnement-Service liefert fortlaufend Quellenbewertungen für über 140 Millionen IP-Adressen und passt diese an. So wird der Kontext von Bewertungen externer Systeme direkt in den Sicherheitsereignisstrom aufgenommen, wodurch aktuelle und bereits erfolgte Interaktionen mit bekannten kriminellen Akteuren rasch erkannt werden. Die von McAfee Global Threat Intelligence (GTI) gemeldeten IP-Reputationsdaten sind das Ergebnis der Korrelation von Bedrohungsdaten aus allen wichtigen Bedrohungsvektoren unter Zuhilfenahme von weltweit mehr als 100 Millionen Sensoren und mit Unterstützung von mehr als 500 Forschern.

Vorteile von McAfee Global Threat Intelligence for Enterprise Security Manager

- **Besserer Schutz für das gesamte Netzwerk:** McAfee Global Threat Intelligence for Enterprise Security Manager erkennt sofort, wenn ein Node in Ihrem Netzwerk mit einem verdächtigen oder bekannten kriminellen Akteur kommuniziert und identifiziert den Bedrohungspfad im Nu.
- **Nutzung risikobasierter Priorisierung:** Die IP-Bewertung wird automatisch in den regellosen Algorithmus zur Risikoeinstufung von McAfee Enterprise Security Manager integriert, um so den Reaktionsbedarf zu identifizieren.
- **Bedrohungsüberwachung rund um die Uhr:** McAfee Labs erfasst fortlaufend Bedrohungsinformationen, um neu infizierte und böswillige Systeme zu identifizieren. Nach der Bereinigung dieser Systeme versorgt es Unternehmen mit einer präzisen, aktuellen Übersicht über die globale Bedrohungslandschaft.

Identifizierung böswilliger Aktivitäten in Echtzeit

Mit McAfee Global Threat Intelligence for Enterprise Security Manager haben Unternehmen nun die Möglichkeit, die IP-Bewertung für jedes Ereignis zu verstehen, etwa in heterogenen Firewalls, Eindringungsschutzsystemen, auf Routern und Endgeräten. Dank der dynamischen Watchlists von McAfee Enterprise Security Manager werden Ereignisse automatisch mit dem Reputationsfaktor für die Quelle verknüpft und das Risiko angepasst. Da sich die globalen Bedrohungen kontinuierlich verändern, versorgt McAfee GTI McAfee Enterprise Security Manager fortlaufend mit aktuellen Informationen, damit Server und Systeme immer über präzise Informationen zum Reputationsfaktor verfügen. Dadurch können Unternehmen nicht nur Risiken besser verstehen, sondern sie erhalten zudem Echtzeitinformationen zu dringenden Problemen, sodass bei Vorfällen das Reaktionszeitfenster verkleinert und eine genaue Risikoanalyse möglich werden.

Finden Sie heraus, was Sie nicht wussten

Eine wesentliche Stärke von McAfee Enterprise Security Manager besteht darin, dass über Jahre gesammelte und gespeicherte Daten jederzeit abgerufen und als Verlaufsdaten korreliert werden können. Mit McAfee GTI haben Sicherheitsanalysten nun die Möglichkeit, auf Daten aus mehreren Jahren zurückzugreifen, um vergangene Interaktionen mit böswilligen Akteuren zu verstehen. Damit ist eine wichtige Voraussetzung erfüllt, um heimlich und langsam ausgeführte Angriffe, wiederholte Aktivitäten von Botnets, siteübergreifende Skripterstellung sowie SQL-Injektionsangriffsversuche zu erkennen.

Verkürzte Reaktionszeiten

McAfee GTI ist nahtlose in die Alarm- und Benachrichtigungsmechanismen von McAfee Enterprise Security Manager eingebunden, damit Interaktionen mit bekannten böswilligen Systemen die notwendige Aufmerksamkeit erhalten.

Unterstützung durch die McAfee-Datenbank und Auslegung für umfangreiche Sicherheitsdaten

Das wachsende Datenvolumen ist ein häufiges Gesprächsthema. Dies betrifft auch die Bereitstellung der Fülle an sicherheitsbezogenen Informationen von McAfee Labs für SIEM. McAfee Enterprise Security Manager kommt hierbei eine einzigartige Aufgabe zu, da diese Lösung den enorm großen IP-Bewertungsdatenspeicher von McAfee GTI ohne unannehmbare Beeinträchtigungen der Systemleistung speichern, korrelieren und aktualisieren kann. Dank der proprietären Datenbank von McAfee Enterprise Security Manager entfällt die zeitaufwändige Datenbank-administration für SIEM. Diese Datenbank ist zudem speziell für die massive Zufuhr und Verarbeitung von Ereignissen und relationalen Daten in extrem hoher Geschwindigkeit ausgelegt. Mit McAfee Global Threat Intelligence for Enterprise Security Manager können Kunden sicher sein, dass die Informationen von McAfee GTI in Echtzeit zur Verfügung stehen.

Spezifikationen

Unterstützte Versionen
McAfee Enterprise Security Manager 9.4 und McAfee Event Reporter Appliance 9.4

- Bedrohungsanalyse-Netzwerk von McAfee Labs: über 100 Millionen Knoten in mehr als 120 Ländern
- Durchschnittliche Zahl der IP-Bewertungen: ist von der Bedrohungslandschaft abhängig

McAfee
Together is power.

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