McAfee Advanced Correlation Engine

Rileva le minacce in base alle priorità dell'azienda

Le ingegnose minacce odierne sfuggono al rilevamento standard delle minacce basato su regole. Distribuisci la soluzione McAfee® Advanced Correlation Engine con McAfee Enterprise Security Manager per identificare e classificare gli eventi relativi alle minacce in tempo reale utilizzando logica sia basata su regole che sul rischio. Puoi istruire la soluzione McAfee Advanced Correlation Engine su ciò che per te è prezioso - utenti o gruppi, applicazioni, server specifici o sottoreti - e ti segnalerà se la risorsa è minacciata. La funzionalità di audit trail e di historical replay hanno validità legale, rispondono alle esigenze di conformità e consentono di perfezionare le regole.

La soluzione McAfee Advanced Correlation Engine integra la soluzione di correlazione degli eventi McAfee Enterprise Security Manager con due motori di correlazione dedicati e prestazioni dedicate:

- Un motore di rilevamento del rischio che genera un punteggio di rischio utilizzando correlazione del punteggio di rischio senza regole
- Un motore di rilevamento delle minacce che rileva le minacce utilizzando correlazione tradizionale degli eventi basata su regole

La soluzione McAfee Advanced Correlation Engine stand-alone fornisce la potenza elaborativa richiesta per supportare questa correlazione di eventi in azienda. Il suo motore dei dati si adatta per le reti di più grandi dimensioni.

Rilevamento delle minacce in tempo reale e storiche

La soluzione McAfee Advanced Correlation Engine può essere implementata in modalità tempo reale o storica. In modalità tempo reale, la soluzione McAfee Advanced Correlation Engine analizza gli eventi al momento dell'acquisizione per il rilevamento immediato di minacce e rischi.

- Correlazione basata su regole dei dati degli eventi in tempo reale per il rilevamento delle minacce nel momento in cui si verificano
- Correlazione senza regole dei dati degli eventi in tempo reale per il rilevamento delle minacce nel momento in cui si sviluppano

Vantaggi principali

- Semplifica l'avvio: nessun aggiornamento delle regole, messa a punto delle firme o altre preoccupazioni
- Segnala se le minacce prendono di mira utenti, risorse, applicazioni e attività prioritarie
- Offre classificazioni accurate attraverso correlazione simultanea basata su regole e senza regole
- Permette di controllare i nuovi attacchi e le vulnerabilità rispetto al passato per rilevare gli eventi precedenti
- Aggiunge risorse di correlazione ed elaborazione specializzate a McAfee Enterprise Security Manager
- Disponibile in distribuzioni virtuali o appliance

In modalità storica, è possibile "rispondere" a tutti i dati raccolti attraverso entrambi i motori di correlazione per il rilevamento ricorsivo delle minacce e dei rischi. Quando vengono individuati gli attacchi zero-day, la soluzione McAfee Advanced Correlation Engine può effettuare un'analisi retrospettiva per stabilire se l'azienda è stata o meno esposta a tale attacco nel passato, per il rilevamento di minacce zero-day.

Prestazioni dedicate dove necessario

La soluzione McAfee Advanced Correlation Engine è disponibile come appliance o offerta virtuale, non influisce in alcun modo sulle prestazioni di McAfee Enterprise Security Manager in termini di acquisizione e gestione degli eventi. È possibile utilizzare tutte le funzionalità delle applicazioni di McAfee Advanced Correlation Engine senza compromessi, traendo il massimo dall'utility McAfee Enterprise Security Manager.

Correlazione degli eventi basata su regole

La correlazione basata su regole utilizza la logica di correlazione tradizionale per analizzare le informazioni acquisite in tempo reale. Tutti i log, gli eventi e i flussi di rete vengono correlati tra di loro - unitamente a informazioni contestuali quali identità, ruoli, vulnerabilità e altro - per rilevare schemi indicativi di una minaccia di maggior portata. Mentre la correlazione basata su regole a livello di rete viene già supportata direttamente su tutte le soluzioni McAfee Enterprise Security Manager, la soluzione McAfee Advanced Correlation Engine offre una risorsa di elaborazione dedicata per correlare volumi di dati anche maggiori, integrando le attività di correlazione esistenti o scaricandole completamente.

Correlazione dei punteggi di rischio senza regole

Mentre la correlazione basata su regole è una funzione preziosa e necessaria di qualsiasi soluzione SIEM, questi sistemi possono rilevare solo schemi di minacce note, per cui è necessario che la messa a punto e gli aggiornamenti delle firme siano costanti per essere efficaci. La risposta è integrare la tradizionale correlazione degli eventi con una tecnologia di correlazione "senza regole". Nei sistemi di correlazione senza regole, le firme per il rilevamento vengono sostituite da una semplice configurazione unica: è sufficiente comunicare alla soluzione McAfee Advanced Correlation Engine cosa è importante per l'azienda. Potrebbe essere un servizio o un'applicazione particolare, un gruppo di utenti o tipologie specifiche di dati.

Localizzazione e allarmi in tempo reale

La soluzione McAfee Advanced Correlation Engine inizia poi a localizzare tutte le attività legate a tali elementi, creando un punteggio di rischio dinamico che aumenta o diminuisce sulla base dell'attività in tempo reale. Quando un punteggio di rischio supera una certa soglia, viene generato un evento all'interno della soluzione McAfee Advanced Correlation Engine. Quest'evento può essere utilizzato per segnalare a un analista di sicurezza l'aumento di una minaccia o dal motore di correlazione tradizionale basato su regole come condizione di un incidente di più vasta portata. La soluzione McAfee Advanced Correlation Engine tiene una registrazione completa di tutte le operazioni effettuate per i punteggi di rischio per consentire un'analisi completa dello stato delle minacce nel tempo.

Casi di utilizzo

Raffigurazione del rischio aziendale

La soluzione McAfee Advanced Correlation Engine offre una piattaforma per raffigurare con efficacia il rischio aziendale. L'accesso a documenti estremamente riservati da parte dei dipendenti con un livello elevato di autorizzazione può rappresentare un rischio per un ente che si occupa di difesa mentre la perdita dei file relativi a pazienti celebri cui è stata diagnostica una grave malattia potrebbe essere un rischio per un ospedale. La soluzione McAfee Advanced Correlation Engine offre una raffigurazione perfetta dei rischi per l'azienda classificando le caratteristiche importanti, sviluppando una base di riferimento e inviando segnalazioni quando vengono superate le soglie ordinarie.

Valutazioni del rischio proattive per i dati critici

La soluzione McAfee Advanced Correlation Engine monitora i dati in tempo reale, quindi entrambi i motori di correlazione possono essere utilizzati contemporaneamente per rilevare rischi e minacce prima che si verifichino. I punteggi di rischio possono essere utilizzati all'interno della logica di correlazione tradizionale. Per esempio, una firma tradizionale per il rilevamento delle minacce basata su regole potrebbe essere "un evento malware verificatosi a seguito di un evento di login con metodo forza bruta". Solitamente, quando questa firma si attiva, si è già verificato un evento. Invece, con la soluzione McAfee Advanced Correlation Engine, puoi incorporare un fattore di rischio come un aumento del 20% del punteggio di rischio a seguito di un evento di login forzato.

Quando viene rilevato tale evento, la soluzione McAfee Advanced Correlation Engine può lanciare un allarme proattivo di un incidente invalidante, consentendo di intervenire prima che il danno sia fatto.

Valutazione delle minacce ricorrenti

Non è raro identificare una minaccia o scoprire una violazione, solo per domandarsi se era sempre stata lì. Implementando la soluzione McAfee Advanced Correlation Engine in modalità storica, qualsiasi serie di dati del passato al suo interno può essere riesaminata attraverso i motori di correlazione tradizionali e senza regole.

Stabilendo quando una nuova minaccia si è materializzata la prima volta, è molto più probabile che la causa originaria di tale condizione possa essere identificata.

Modalità operative

Modalità di correlazione in tempo reale:

- Correlazione basata su regole dei dati degli eventi in tempo reale per il rilevamento delle minacce nel momento in cui si verificano
- Correlazione senza regole dei dati degli eventi in tempo reale per il rilevamento delle minacce nel momento in cui si sviluppano

Modalità di correlazione dello storico:

- Correlazione basata su regole dei dati degli eventi storici per il rilevamento delle minacce ricorrenti
- Correlazione senza regole dei dati degli eventi storici per la valutazione delle minacce ricorrenti

Funzionalità di correlazione

- Correlazione simultanea basata su regole e senza regole
- Correlazione dei dati da qualsiasi fonte dati supportata
- Correlazione dei dati su reti distribuite e collettori
- Centinaia di regole di correlazione degli eventi predefinite
- Editor di configurazione per la correlazione senza regole
- Editor delle regole di correlazione degli eventi dell'interfaccia grafica utente (GUI) di semplice utilizzo per personalizzare le regole o crearne di nuove

Figura 1. La correlazione basata sui rischi aiuta a rilevare le minacce incombenti rispetto alle risorse prioritarie.

Ulteriori informazioni

Ulteriori informazioni sono disponibili sul sito **www.mcafee.com/it/products/siem/index.aspx**.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it