McAfee Global Threat Intelligence for Enterprise Security Manager

Integrazione dell'autorità dei McAfee® Labs nel quadro dettagliato della situazione aziendale.

McAfee® Global Threat Intelligence for Enterprise Security Manager porta l'autorità dei McAfee Labs nel monitoraggio della sicurezza aziendale. Per la prima volta, le reputazioni degli IP - raccolte da McAfee Labs da oltre 100 milioni di sensori delle minacce in tutto il mondo - sono disponibili in una soluzione per la gestione delle informazioni e degli eventi della sicurezza (SIEM). Questo feed costantemente aggiornato per McAfee Enterprise Security Manager migliora la consapevolezza della situazione consentendo la rapida scoperta di eventi che coinvolgono comunicazioni con IP sospetti o dannosi. Ciò consente agli amministratori della sicurezza di stabilire quali host hanno comunicato o stanno comunicando con malintenzionati e identificare rapidamente le condizioni in cui un malintenzionato noto è la fonte di un'attività minacciosa.

La necessità di un contesto esterno

Gli eventi di sicurezza forniscono informazioni sull'attività correlata alla sicurezza sulla base di uno specifico momento temporale. Se una soluzione SIEM ha la capacità di correlare tali eventi, alcune domande sono ancora responsabilità dell'operatore: Questa attività è accettabile? Come stabilisco cosa è più urgente? Come rilevo gli attacchi sofisticati che non sono particolarmente invadenti? Moltiplicando tali domande per gli eventi quotidiani tipici di un'azienda - più di un quarto di miliardo - risulta chiaro che l'individuazione di modelli noti su cui il sistema SIEM legacy si concentra è solo la punta dell'iceberg dell'attività di monitoraggio della sicurezza.

Uno degli elementi contestuali più importanti dietro l'ignoto è la comprensione della reputazione dei sistemi esterni. Fino ad oggi, avere questa chiara comprensione degli eventi di sicurezza è stato impossibile.

L'autorità di McAfee Labs direttamente nella soluzione SIEM

McAfee Global Threat Intelligence per Enterprise Security Manager inse riscel'autorità di McAfee Labs direttamente nel flusso di monitoraggio della sicurezza attraverso la soluzione McAfee SIEM ad alta velocità e intelligente, creata per i big data della sicurezza. L'iscrizione a questo servizio opzionale mette a disposizione e aggiorna con continuità la reputazione di oltre 140 milioni di indirizzi IP,

Vantaggi principali

- Integrazione dell'autorità dei McAfee Labs nella soluzione SIEM
- Comprensione accurata del rischio associato agli eventi
- Utilizzo del sistema di alimentazione di informazioni sulle minacce di McAfee GTI senza influire negativamente sulle prestazioni
- Ricezione ed elaborazione automatica delle reputazioni delle nuove fonti all'interno di McAfee Enterprise Security Manager
- Miglioramento della precisione nel rilevamento delle minacce riducendo i tempi di risposta
- Rapida identificazione dei percorsi d'attacco e delle interazioni passate con malintenzionati noti associati ad attacchi botnet/DDoS (Distributed Denial of Service), malware che invia mail e spam che ospita attacchi network probing, presenza di malware, hosting DNS e attività generate da attacchi intrusivi.

riconducendo il contesto della reputazione dei sistemi esterni direttamente nel flusso degli eventi di sicurezza e identificando prontamente le interazioni passate e presenti con elementi notoriamente dannosi. Le reputazioni IP di McAfee Global Threat Intelligence (GTI) derivano dalla correlazione delle informazioni su tutti i principali vettori delle minacce, provenienti da oltre 100 milioni di sensori sparsi in tutto il mondo e oltre 500 ricercatori.

I benefici di McAfee Global Threat Intelligence for Enterprise Security Manager

- **Protezione migliorata dell'intera rete:** McAfee Global Threat Intelligence for Enterprise Security Manager rileva immediatamente se un nodo della rete aziendale sta comunicando con un elemento sospetto o dannoso e comprende all'istante il percorso seguito dalla minaccia.
- **Prioritizzazione in base al rischio:** la reputazione dell'IP viene integrata automaticamente nell'algoritmo di classificazione dei rischi destrutturati di McAfee Enterprise Security Manager, individuando automaticamente il problema su cui intervenire.
- **Monitoraggio delle minacce 24/7:** McAfee Labs analizza costantemente le informazioni sulle minacce per rilevare i nuovi sistemi infetti e dannosi - e quando tali sistemi sono stati bonificati - fornendo alle aziende una comprensione precisa e aggiornata del panorama globale delle minacce.

Individuazione delle attività dannose in tempo reale

Con McAfee Global Threat Intelligence for Enterprise Security Manager, le aziende ora sono in grado di comprendere la reputazione dell'IP per ogni evento, includendo firewall eterogenei, sistemi per la prevenzione delle intrusioni, router ed endpoint. Sfruttando la funzionalità di watch list dinamico di McAfee Enterprise Security Manager, gli eventi vengono automaticamente associati al punteggio di reputazione della fonte e il rischio viene adeguato di conseguenza. Dal momento che le minacce globali evolvono, McAfee GTI mantiene aggiornato McAfee Enterprise Security Manager, garantendo che server e sistemi dispongano continuamente di un punteggio di reputazione preciso. Ciò non solo aiuta le aziende a comprendere il rischio, ma individua anche le problematiche urgenti in tempo reale, riducendo il tempo di risposta agli incidenti e fornendo un'analisi precisa del rischio.

Informazioni e visibilità complete

Un punto di forza di McAfee Enterprise Security Manager è la possibilità di archiviare, recuperare ed eseguire correlazioni storiche su anni di dati. Ora, con McAfee GTI, gli analisti della sicurezza possono tornare indietro nel tempo, considerando anni di dati preziosi, per comprendere le precedenti interazioni con i malintenzionati. Questo è fondamentale per rilevare attacchi "low and slow", attività ripetute di botnet, scripting cross-site e tentativi di iniezione SQL.

Reazione più rapida

McAfe GTI si integra perfettamente con i meccanismi di allarme e segnalazione di McAfee Enterprise Security Manager, assicurando che le interazioni con sistemi dannosi noti ricevano l'attenzione che meritano.

Supportato dal database Mcafee, creato per i big data della sicurezza

Si è parlato molto dei dati che si stanno ingrandendo, e ciò include l'arricchimento della soluzione SIEM con le conoscenze relative alla sicurezza di McAfee Labs. McAfee Enterprise Security Manager è unico nella sua capacità di archiviare, correlare e aggiornare l'enorme archivio di dati sulla reputazione degli IP di McAfee GTI senza conseguenze inaccettabili sulle prestazioni.

McAfee Enterprise Security Manager adotta un database proprietario che non solo elimina la laboriosa amministrazione database per il sistema SIEM, ma è stato specificamente progettato per acquisizioni ed elaborazioni in massa di eventi e dati relazionali a velocità estremamente elevate. Grazie a McAfee Global Threat Intelligence for Enterprise Security Manager, i clienti hanno la certezza che le informazioni di McAfee GTI saranno rese disponibili in tempo reale.

Specifiche

Versioni supportate
McAfee Enterprise Security Manager 9.4 e McAfee Event Reporter Appliance 9.4

- La rete di intelligence sulle minacce di McAfee Labs: oltre 100 milioni di nodi in più di 120 paesi
- Media reputazioni IP: varia in base al panorama delle minacce

McAfee
Together is power.

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