McAfee Enterprise Security Manager

Fissa le priorità. Indaga. Interviene.

La sicurezza più efficace inizia con la visibilità dell'attività complessiva sui sistemi, le reti, i database e le applicazioni. Le soluzioni per la gestione delle informazioni e degli eventi di sicurezza (SIEM) costituiscono la base di una struttura di sicurezza efficace. McAfee® Enterprise Security Manager, il fulcro della soluzione McAfee SIEM, offre prestazioni, intelligence fruibile e integrazione della soluzione con la velocità e la scalabilità richieste dalle organizzazioni di sicurezza. Permette di assegnare le priorità, effettuare analisi e reagire rapidamente alle minacce nascoste e di soddisfare i requisiti in termini di conformità.

McAfee Enterprise Security Manager permette di capire in tempo reale quello che accade nel mondo esterno — dati sulle minacce e feed sulla reputazione — e offre un quadro della situazione dei sistemi, dei dati, dei rischi e delle attività all'interno dell'azienda. I team della sicurezza possono finalmente attingere in modo completo e correlato ai contenuti e al contesto necessari per prendere decisioni rapide in base ai rischi, e tu puoi investire le risorse in modo ottimale in un panorama operativo e delle minacce dinamico. Questo è fondamentale per indagare sugli attacchi "low and slow", alla ricerca di indicatori di compromissione (IoC) o intervenendo sui risultati delle verifiche. Per rendere la gestione delle minacce e della conformità una parte integrante delle operazioni di sicurezza, McAfee Enterprise Security Manager offre strumenti integrati per la gestione della configurazione e delle modifiche, gestione dei casi e gestione centralizzata delle policy: tutto quanto necessario per migliorare il flusso di lavoro e l'efficienza del team delle operazioni di sicurezza. Inoltre, i Content Pack disponibili per McAfee Enterprise Security Manager offrono configurazioni predefinite per casi d'uso di sicurezza avanzati che aiutano a semplificare le operazioni di sicurezza.

Creato per essere scalabile

I team delle operazioni di sicurezza richiedono sempre più una maggiore efficienza poiché acquisiscono ed esaminano velocemente quantità sempre maggiori di dati non elaborati e dati analizzati provenienti dalle

Vantaggi principali

- **Intelligente:** analisi avanzate e rich context aiutano a individuare e assegnare le priorità alle minacce.
- **Fruibile:** i dati necessari vengono presentati in visualizzazioni dinamiche che includono la possibilità di agire per investigare, arginare, porre rimedio e adattarsi ad avvisi e schemi importanti.
- **Integrata:** la soluzione controlla e analizza i dati provenienti da un'ampia infrastruttura eterogenea di sicurezza e offre integrazione bidirezionale tramite interfacce aperte. Permette inoltre di automatizzare molte azioni di primo intervento.

Seguici su:

odierne architetture aziendali dinamiche e distribuite. Per vincere quasta sfida, McAfee Enterprise Security Manager utilizza un databus aperto e scalabile creato appositamente per l'elaborazione di dati ad alto volume. Inoltre, un'architettura dati altamente scalabile supporta l'inserimento, la gestione e l'analisi per prevenire violazioni delle attività di acquisizione, ricerca e conservazione dei dati. Tali violazioni possono mettere in pericolo le indagini quando i dati critici non sono disponibili successivamente, quando la risposta alle query rallenta l'analisi o quando è possibile solo una ricerca parziale a causa delle prestazioni.

I fatti cruciali nel giro di pochi minuti

L'accesso rapido allo storage dei dati relativi agli eventi sul lungo periodo è fondamentale per esaminare gli incidenti, per ricercare prove di attacchi avanzati o tentare di porre rimedio a verifiche di conformità non andate a buon fine, tutte attività che richiedono visibilità dei dati storici e pieno accesso ai dettagli completi di ogni evento specifico.

Le appliance ottimizzate possono acquisire, elaborare e correlare gli eventi del log di svariati anni con altri flussi di dati, fra cui i feed di informazioni sulle minacce basati su STIX, alla velocità giusta per te. McAfee Enterprise Security Manager è in grado di memorizzare miliardi di eventi e di flussi, mantenendo disponibili tutte le informazioni per query immediate ad hoc, e conservando i dati per un lungo periodo di tempo per analisi forense, convalida delle regole e conformità. Inoltre, i dati possono essere replicati immediatamente in più posizioni di archiviazione, mantenendo la business continuity.

Corretta percezione di contesto e contenuti

Quando sono disponibili informazioni sul contesto - tra cui dati sulle minacce e feed sulla reputazione, sistemi di gestione di identità e accessi, soluzioni per la privacy o altri sistemi supportati - ogni evento viene arricchito con tale contesto. Questo arricchimento permette una miglior comprensione e una valutazione delle priorità basato su come gli eventi relativi alla rete e alla sicurezza sono in correlazione con gli attributi delle risorse e con i processi e le policy aziendali reali.

Le prestazioni e la scalabilità di McAfee Enterprise Security Manager consentono di acquisire più informazioni da un numero maggiore di fonti, compresi i contenuti delle applicazioni come documenti, transazioni e comunicazioni, offrendo un prezioso valore forense. Queste informazioni sono indicizzate, normalizzate e correlate sistematicamente per consentire di rilevare una più ampia gamma di rischi e di minacce.

Interpretazione avanzata delle minacce

Che si tratti di traffico di rete, attività degli utenti o utilizzo delle applicazioni, qualsiasi variazione rispetto alle normali attività potrebbe indicare una minaccia imminente e, quindi, che i dati o le infrastrutture sono in pericolo. McAfee Enterprise Security Manager calcola l'attività di riferimento per tutte le informazioni acquisite e genera avvisi in base alle priorità allo scopo di rilevare le potenziali minacce prima che si manifestino, analizzando contemporaneamente i dati alla ricerca di schemi che potrebbero indicare una minaccia di portata più vasta. Inoltre, McAfee Enterprise Security Manager

sfrutta le informazioni contestuali e arricchisce ogni evento con il relativo contesto, per consentire di capire meglio l'impatto degli eventi di sicurezza sui processi aziendali reali.

Le dashboard della funzionalità Cyber Threat Manager di McAfee Enterprise Security Manager offrono funzioni potenziate di monitoraggio e comprensione in tempo reale delle minacce emergenti. Informazioni relative a minacce sospette o confermate segnalate tramite STIX/TAXII, McAfee Advanced Threat Defense e/o URL web di terze parti possono essere aggregate e correlate in tempo reale o cronologicamente (utilizzando la funzione Backtrace) rispetto ai dati degli eventi, fornendo ai team della sicurezza una miglior comprensione della diffusione delle minacce all'interno di un ambiente. Queste informazioni permettono alle organizzazioni di fornire i dati giusti alle persone giuste per intervenire quasi in tempo reale e prendere decisioni più intelligenti.

Operazioni di sicurezza ottimizzate

L'esperienza dell'utente ottimizzata per gli analisti di McAfee Enterprise Security Manager offre una maggior flessibilità, semplicità di personalizzazione e una risposta più rapida alle indagini. Flussi di lavoro ottimizzati permettono una gestione degli incidenti più efficace e tempestiva. Grazie all'accesso veloce e intelligente alle informazioni sulle minacce, gli analisti con qualsiasi livello di competenza, dal principiante all'esperto, troveranno più facile ordinare per priorità le minacce in evoluzione, indagarle e rispondere.

McAfee Enterprise Security Manager è già pronto all'uso, con centinaia di rapporti, visualizzazioni, regole e avvisi utilizzabili fin da subito e facilmente personalizzabili. Che si tratti di configurare le impostazioni di base per capire qual è l'utilizzo tipico di una rete o semplicemente di personalizzare gli avvisi, la dashboard di McAfee Enterprise Security Manager garantisce facilità di visualizzazione, di indagine e di compilazione di rapporti sulle informazioni di sicurezza più rilevanti. Ora le aziende possono attingere in modo completo e correlato ai dati e al contesto necessari per prendere decisioni intelligenti in tempi brevi.

Inoltre, McAfee Enterprise Security Manager offre Content Pack per semplificare le operazioni di sicurezza con casi d'uso di protezione "ready-to-go" che sono preconfigurati e offrono un rapido accesso alle funzionalità di gestione delle minacce avanzate o della conformità. I Content Pack sono configurazioni predefinite per casi d'uso di sicurezza comune che forniscono una serie di regole, allarmi, visualizzazioni, report, variabili e liste di controllo. Molti Content Pack forniscono attivatori preconfezionati per comportamenti che potrebbero richiedere ulteriori controlli o rimedi automatici.

Conformità semplificata

Grazie alle funzioni di reportistica e monitoraggio della conformità automatizzate e centralizzate, McAfee Enterprise Security Manager elimina le lunghe procedure manuali. Inoltre, l'integrazione con Unified Compliance Framework (UCF) permette di adottare una metodologia in cui una sola acquisizione di dati consenta di conformarsi a più normative, riducendo

al minimo le verifiche e le relative spese. Il supporto per l'UCF rende più efficiente il rispetto degli standard e delle procedure consigliate normalizzando i dettagli di ogni disposizione, in modo da poter associare facilmente il singolo insieme di eventi acquisiti alle singole norme.

Con McAfee Enterprise Security Manager, la gestione della conformità è semplice e rapida grazie a centinaia di dashboard predefinite, audit trail completi e rapporti per più di 240 norme e sistemi di controllo, compresi PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX e SOX. Oltre all'ampio supporto garantito dalle dotazioni iniziali del prodotto, tutti i rapporti sulla conformità, le regole e le dashboard di McAfee Enterprise Security Manager sono totalmente personalizzabili.

Un'infrastruttura IT collegata

L'integrazione nell'infrastruttura di sicurezza offre un livello senza precedenti di visibilità in tempo reale dello stato di sicurezza dell'azienda. McAfee Enterprise Security Manager può acquisire dati preziosi da centinaia di dispositivi di fornitori di sicurezza terze parti e feed di intelligence sulle minacce. L'integrazione con McAfee Global Threat Intelligence (McAfee GTI) comprende dati provenienti da oltre 100 milioni di sensori di minacce McAfee Labs dislocati ovunque nel mondo, che garantiscono un flusso costantemente aggiornato di informazioni sugli indirizzi IP pericolosi già noti. McAfee Enterprise Security Manager è inoltre in grado di inserire le informazioni sulle minacce segnalate tramite STIX/TAXII e/o URL web di terze parti e agire in base all'analisi.

McAfee Enterprise Security Manager offre anche integrazioni attive con dozzine di soluzioni complementari per l'analisi e la gestione degli incidenti, tra cui soluzioni di McAfee e di partner McAfee Security Innovation Alliance.

Per esempio, McAfee Threat Intelligence Exchange, basato sul monitoraggio degli endpoint, aggrega gli attacchi a bassa diffusione, sfruttando intelligence sulle minacce globali, locali e di terze parti. McAfee Threat Intelligence Exchange può utilizzare anche altri prodotti integrati, come ad esempio McAfee Advanced Threat Defense, per analizzare ulteriormente i file e classificarli come dannosi.

Gli analisti traggono inoltre vantaggio dall'integrazione con McAfee Behavioral Analytics, una soluzione di analisi del comportamento di utenti ed entità che sintetizza miliardi di eventi di sicurezza in centinaia di anomalie per produrre una manciata di indizi prioritari relativi alle minacce e consente agli analisti di individuare minacce di sicurezza insolite e ad alto rischio, spesso non identificabili da altre soluzioni. Analogamente, McAfee Enterprise Security Manager si integra con McAfee Investigator per trasformare gli analisti in investigatori esperti e consentire loro di chiudere un maggior numero di casi, più velocemente, con maggiore sicurezza di aver stabilito la causa principale.

I team di risposta agli eventi e gli amministratori possono utilizzare McAfee Active Response per ricercare file zero-day pericolosi che sono in attesa sui sistemi e i processi attivi nella memoria. McAfee Active Response utilizza inoltre strumenti di raccolta di informazioni costanti per

monitorare continuamente gli endpoint alla ricerca di IoC specifici, segnalando automaticamente se un IoC appare da qualche parte all'interno dell'ambiente aziendale. A differenza dei metodi standard adottati da altri prodotti per la sicurezza, questa combinazione garantisce alle aziende un flusso di lavoro dettagliato e a ciclo chiuso, dal contenimento al processo di remediation.

McAfee offre un sistema di sicurezza integrato che permette di prevenire e rispondere alle minacce emergenti. Aiutiamo a porre rimedio a un maggior numero di minacce in modo più rapido e con un minor numero di risorse. La nostra architettura connessa e la gestione centralizzata riducono la complessità e migliorano l'efficienza operativa nell'intera infrastruttura di sicurezza. McAfee si impegna a essere il tuo partner di sicurezza numero uno, fornendoti una serie completa di funzionalità di sicurezza integrate.

Ulteriori informazioni

Ulteriori informazioni su McAfee Enterprise Security Manager sono disponibili all'indirizzo **www.mcafee.com/it/products/siem/index.aspx**.

Ulteriori informazioni sulle soluzioni integrate: **www.mcafee.com/it/solutions/intelligent-security-operations.aspx**.

McAfee
Together is power.

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