McAfee Enterprise Log Search

Ispezione più rapida grazie alla ricerca di miliardi di eventi ad alta velocità

I team di sicurezza hanno bisogno di strumenti per muoversi con maggiore velocità in ambienti che generano sempre più spesso troppi avvisi. Gli analisti di questi team devono poter accedere a un contesto più ricco e avere la capacità di individuare rapidamente i dettagli rilevanti di un evento relativi a un incidente. McAfee® Enterprise Log Search accelera il processo di caccia alle minacce grazie a una ricerca ultra rapida di dati grezzi e non compressi relativi agli eventi. Un backend basato su Elasticsearch ottimizza le prestazioni delle query, fornendo un accesso immediato ai registri grezzi. La funzionalità di ricerca avanzata consente di effettuare query sia con input in linguaggio naturale di parole chiave semplici sia con modelli di espressione regolare più sofisticati per il recupero mirato dei dati.

Gestione ottimizzata dei registri

McAfee Enterprise Log Search si basa su Elasticsearch, una tecnologia che utilizza un indice invertito per memorizzare i dati. L'indice invertito cataloga i dati in una struttura che facilita il recupero efficiente dei termini di ricerca. Poiché Elasticsearch è progettato per l'inserimento e l'indicizzazione ad elevate prestazioni, McAfee Enterprise Log Search rende disponibili i dati grezzi per la ricerca ad alta velocità dopo che sono stati catturati e catalogati.

McAfee Enterprise Log Search è un componente di McAfee® Enterprise Security Manager, una soluzione per la gestione delle informazioni e degli eventi di sicurezza (SIEM). Un altro componente complementare è McAfee® Enterprise Log Manager, che è stato progettato per essere lo spazio di archiviazione dei record effettuando l'hashing (MD5) dei registri grezzi in entrata per l'integrità forense e la compressione di tali registri grezzi per l'efficienza dell'archiviazione. Se combinati, questi due componenti forniscono soluzioni di archiviazione create appositamente che possono essere utilizzate simultaneamente per massimizzare una ricerca veloce (tramite McAfee Enterprise Log Search) e la conservazione dei registri per la conformità (tramite McAfee Enterprise Log Manager), in modo che i clienti non debbano scendere a compromessi nella scelta tra l'una o l'altra.

Vantaggi principali

- Gestione ottimizzata dei log per la conservazione dei log e una rapida ricerca
- Un backend basato su Elasticsearch supporta l'inserimento ad alta velocità, l'indicizzazione e le prestazioni della query
- Ricerca in linguaggio naturale
- Passa da viste di dati analizzate a registri non elaborati in modo rapido e semplice
- Completamente integrato con McAfee Enterprise Security Manager
- Opzioni di distribuzione flessibili includono appliance fisiche e virtuali (mix and match)

Seguici su

Con McAfee Enterprise Log Search, le policy di conservazione possono essere personalizzate per memorizzare dati non compressi per diversi periodi in anni (365 giorni), trimestri (90 giorni) o mesi (30 giorni). Gli utenti possono identificare quali fonti di dati associare a McAfee Enterprise Log Search e aggiungere fino a sei policy di conservazione individuali.

Funzionalità di ricerca avanzata

La funzione di ricerca all'interno di McAfee Enterprise Log Search è simile a quella dei più diffusi motori di ricerca, consentendo inserimenti di dati in linguaggio naturale. I risultati della ricerca possono essere recuperati da testo semplice o parole chiave. Inoltre, le ricerche possono essere eseguite con modelli più sofisticati che includono la logica booleana, i caratteri jolly e l'espressione regolare (RegEx). Per restringere ulteriormente i risultati della ricerca, gli utenti possono applicare filtri per fonte dati e data. Il filtro data consente agli utenti di selezionare i periodi di tempo in cui sono stati generati gli eventi di registro, come nell'ultima ora, nel giorno corrente, l'anno precedente o intervalli personalizzati.

Integrato con McAfee Enterprise Security Manager

La stretta integrazione con McAfee Enterprise Security Manager consente agli analisti di passare dai dati analizzati ai dati grezzi con un solo clic. Quando un evento viene generato all'interno di McAfee Enterprise Security Manager, i file degli eventi analizzati vengono collegati direttamente al file del registro di origine e allo specifico record di registro grezzo. Gli analisti che desiderano ulteriore visibilità su quel record o parti di esso possono semplicemente selezionare il registro in questione per suggerire una ricerca di registro grezza. Non ci sono altri passaggi, applicazioni o interfacce da lanciare per scavare più a fondo con la ricerca di registro grezzo.

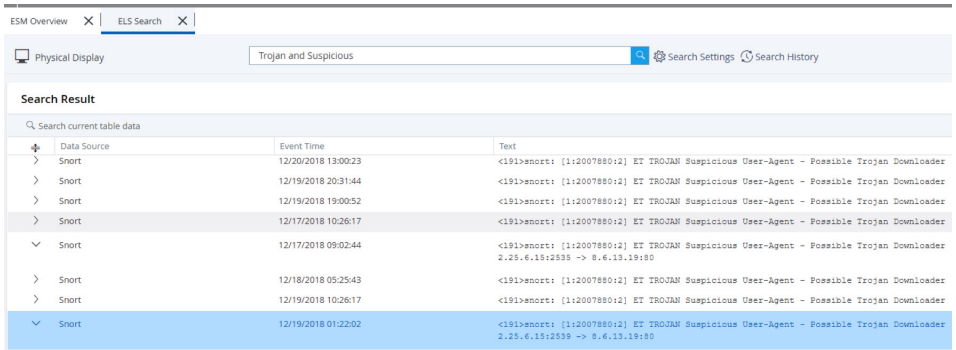

Figura 1. Parole chiave di ricerca utilizzando la logica Booleana per scoprire gli eventi che contengono un Trojan e sono sospetti.

Distribuzione e prezzi flessibili

Le opzioni di consegna flessibili includono appliance fisiche e virtuali. Le appliance sono valutate e vendute in base alla loro capacità di assorbire una certa capacità evento al secondo (EPS) piuttosto che in base a un prezzo per fonte di dati, prezzo per EPS o prezzo per volume di dati indicizzato. Le macchine virtuali (VM) sono concesse in licenza con la stessa filosofia e vendute in base al numero di core di CPU necessari per supportare un dato EPS. Ciò consente ai clienti di aggiungere core aggiuntivi in base alle necessità senza dover sostituire l'hardware.

Raccolta e rapida ricerca dei dati necessari

Quando si distribuisce McAfee Enterprise Log Search, sono disponibili sei tipi di registri che vengono comunemente utilizzati per ricercare le minacce. Questi registri possono fornire dati approfonditi specifici e contesto per gli incidenti di sicurezza.

Tipo di registro	Dati comunemente disponibili
Registri DNS	▪ Nome di dominio richiesto ▪ Indirizzo IP di origine della query DNS ▪ Successo o fallimento delle query DNS ▪ Indirizzo IP risolto se la query ha avuto un esito positivo ▪ Valore di risposta TTL ▪ Server DNS utilizzato
Registri Proxy	▪ Indirizzo di dominio/IP a cui si è collegato ▪ Byte trasferiti ▪ Data e ora della connessione ▪ URL utilizzato ▪ Referente ▪ Stringa agent utente
Registri SMTP	▪ Dominio email del mittente ▪ Oggetto dell'email ▪ Indirizzo IP del mittente
Registri Windows	▪ Eventi del registro di sicurezza di Windows ▪ Eventi del registro delle applicazioni di Windows ▪ Eventi del registro di sistema di Windows ▪ Eventi del registro di integrità del codice di Windows
Registri DHCP	▪ Indirizzo MAC sorgente ▪ Indirizzo IP concesso ▪ Periodo di locazione ▪ Data e ora della richiesta e della concessione della locazione
Registri VPN	▪ Indirizzo IP di origine ▪ Autenticazione identità ▪ Data e ora di creazione della connessione VPN ▪ Tipo di connessione: ripresa o nuova ▪ Tentativi di autenticazione falliti - se del caso - e identità corrispondenti

Ulteriori informazioni

Per maggiori informazioni, visitare **www.mcafee.com/enterprise/it-it/products/siem-products.html**.

McAfee
Together is power.

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