McAfee Threat Intelligence Exchange

Informazioni sulle minacce distribuite fra le soluzioni di sicurezza

McAfee® Threat Intelligence Exchange effettua l'intermediazione della reputazione per abilitare il rilevamento delle minacce adattive e la conseguente risposta. Combina le informazioni locali provenienti dalle soluzioni di sicurezza presenti in azienda con dati esterni sulle minacce globali e condivide immediatamente queste informazioni collettive all'interno del tuo ecosistema di sicurezza, permettendo alle soluzioni di scambiare le informazioni condivise e agire.

Creare un ecosistema collaborativo di informazioni sulle minacce

McAfee Threat Intelligence Exchange, un programma di intermediazione della reputazione, combina informazioni sulle minacce provenienti da fonti globali importate, come McAfee Global Threat Intelligence (McAfee GTI), e informazioni sulle minacce di terze parti (come VirusTotal) con informazioni provenienti dalle fonti locali, inclusi endpoint, gateway e soluzioni di analisi avanzata. Data Exchange Layer (DXL) condivide immediatamente queste informazioni collettive all'interno del tuo ecosistema di sicurezza, permettendo alle soluzioni di sicurezza di operare come un tutt'uno per migliorare la protezione all'interno dell'azienda.

La semplicità dell'integrazione, abilitata da DXL, riduce in modo significativo i costi di implementazione e operativi di numerose integrazioni di API (Application Programming Interface) dirette e fornisce protezione, efficienza operativa ed efficacia senza pari. Progettato come una struttura aperta, DXL permette a tutte le soluzioni di sicurezza di entrare a far parte in modo dinamico dell'ecosistema di McAfee Threat Intelligence Exchange, inclusi i prodotti di sicurezza di terze parti.

Adattamento e immunizzazione contro le minacce

Ogni approfondimento condiviso, rilevato da tutte le posizioni sulla rete, stimola una maggior consapevolezza nella lotta contro gli attacchi mirati. Dato che, per loro natura, questi sono attacchi estremamente precisi, le organizzazioni hanno bisogno di un sistema di sorveglianza locale per rilevare le tendenze e ogni singolo assalto in cui incappano. Questi dati sul contesto locale acquisiti al momento dell'incontro, combinati con informazioni sulle minacce globali, permettono di prendere decisioni migliori relativamente a file mai rilevati in precedenza, velocizzando i tempi di protezione e rilevamento.

Vantaggi principali

- La protezione adattiva dalle minacce riduce il ritardo fra l'individuazione e il contenimento degli attacchi mirati avanzati da giorni, settimane e mesi a pochi millisecondi.
- Le informazioni collaborative sulle minacce sono basate sulla combinazione di fonti di dati globali con le informazioni sulle minacce raccolte a livello locale.
- Informazioni di sicurezza rilevanti vengono condivise in tempo reale tra le soluzioni di sicurezza per endpoint, gateway, rete e centri dati.
- Puoi prendere decisioni su file mai osservati in precedenza, combinando una logica basata su regole a seconda del contesto (file, processi e attributi ambientali) con le informazioni collettive sulle minacce.
- L'integrazione viene semplificata attraverso il DXL. I costi d'implementazione e operativi vengono ridotti collegando tra loro soluzioni di sicurezza di McAfee e di altri fornitori per rendere operative le informazioni sulle minacce in tempo reale.

Quando ci si imbatte in un file non identificato sulla rete, McAfee Threat Intelligence Exchange viene contattato per stabilire se è disponibile una reputazione su tale file. I metadati descrittivi, come la prevalenza organizzativa e l'età, vengono mantenuti e riflessi anche nelle informazioni collettive. Oltre a richiedere le reputazioni, le soluzioni di sicurezza integrate possono anche contribuire agli aggiornamenti della reputazione di McAfee Threat Intelligence Exchange in base alle valutazioni locali. Le reputazioni aggiornate vengono quindi diffuse su tutti i sistemi in tempo reale. Queste informazioni locali sulle minacce vengono archiviate per successivi rilevamenti, in modo tale che alla successiva localizzazione su un altro dispositivo o server, non saranno più sconosciute, ma immediatamente rilevate.

McAfee Threat Intelligence Exchange permette agli amministratori di personalizzare facilmente le informazioni sulle minacce. Gli amministratori della sicurezza possono assemblare, sovrascrivere, incrementare e ottimizzare le informazioni complete di intelligence per personalizzare la protezione per il loro ambiente e la loro azienda. Queste informazioni sulle minacce prioritizzate e ottimizzate a livello locale forniscono una risposta immediata a qualsiasi rilevamento futuro.

I punti di applicazione migliorano la protezione

Soluzioni integrate in tutta la rete - dall'endpoint al perimetro della rete - applicano le policy sulla base di reputazione e metadati disponibili o una combinazione di punti dati. McAfee Endpoint Security, una soluzione perfettamente integrata, sfrutta le informazioni combinate locali (metadati dei file, come la prevalenza all'interno dell'azienda e l'età, unitamente alla reputazione locale fornita da altri componenti della sicurezza) e le informazioni attuali disponibili sulle minacce globali per prendere decisioni accurate. Per esempio, un'applicazione personalizzata senza reputazione globale ma con un'elevata prevalenza organizzativa non genererebbe una reputazione composita dannosa e molto probabilmente ne sarebbe consentita l'esecuzione. D'altro canto, un file non osservato in precedenza all'interno dell'azienda, senza reputazione locale o globale e assemblato in modo sospetto, molto probabilmente genererebbe un basso livello di affidabilità, dando inizio a un possibile blocco o richiedendo ulteriori indagini attraverso motori aggiuntivi McAfee Endpoint Security o sandboxing tramite McAfee Advanced Threat Defense o McAfee Cloud Threat Detection.

Real Protect, la funzionalità di apprendimento automatico di McAfee Endpoint Security, e il contenimento dinamico delle applicazioni migliorano ulteriormente il rilevamento e la protezione degli endpoint. Real Protect esegue ricerche sul cloud delle informazioni sulle minacce più recenti con analisi pre e post esecuzione, mentre il contenimento dinamico delle applicazioni impedisce l'esecuzione di attività dannose sull'endpoint, proteggendo il primo computer esposto a una nuova minaccia, mentre vengono eseguite ulteriori analisi.

Gli attacchi mirati avanzati sono una sfida del mondo reale

Progettati per contrastare il rilevamento e stabilire una presenza duratura all'interno di un'azienda, gli attacchi mirati avanzati continuano ad affliggere le aziende e ad esfiltrare dati di grande valore. Secondo i dati da poco rilasciati come parte del report *Verizon 2015 Data Breach and Investigations Report* (Rapporto investigativo Verizon 2015 sulle Violazioni dei Dati), dal 70% al 90% degli esempi di malware sono unici per una singola organizzazione, indicando che il rilevamento di indicatori unici sulle minacce è la principale problematica odierna[1].

Per maggiori informazioni, visita **www.mcafee.com/it/products/threat-intelligence-exchange.aspx**.

I vantaggi della collaborazione

Analisi delle minacce avanzate

Se sono necessarie maggiori informazioni su un file, è possibile inviarlo automaticamente da McAfee Threat Intelligence Exchange alle soluzioni di analisi avanzata - come McAfee Advanced Threat Defense o McAfee Cloud Threat Detection - per ottenere immediatamente ulteriori informazioni sulle potenziali nuove minacce e determinare la reputazione del file in questione. Tutto ciò è automatizzato, documentato e condiviso collettivamente tramite DXL per proteggere l'intero ecosistema di sicurezza.

Gestione degli eventi di sicurezza

McAfee Enterprise Security Manager permette di indagare più a fondo quando si analizzano gli indicatori di compromissione (IoC) identificati da McAfee Threat Intelligence Exchange. L'accesso alle informazioni di sicurezza storiche e la capacità di creare elenchi di sorveglianza automatizzati aumentano l'efficienza della sicurezza per le organizzazioni.

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee
Together is power.

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