McAfee Active Response

Rilevamento completo degli endpoint e risposta

Le aziende attente alla sicurezza oggi devono affrontare un panorama delle minacce in rapida evoluzione. Gli attacchi vengono creati e diffusi a ritmi sempre più veloci. Gli attacchi definiti "designer" prendono di mira singole aziende utilizzando conoscenza mirata per migliorare la loro efficacia e ridurre l'eventualità di essere rilevati. Gli aggressori violano sempre più frequentemente le tecnologie di prevenzione. Le aziende che guardano al futuro perciò richiedono strumenti integrati semplici da utilizzare che aiutano a rilevare meglio la presenza degli aggressori e quindi permettono rapide attività di analisi e remediation. Le migliori soluzioni per il rilevamento e la risposta aumentano l'efficienza della sicurezza anche quando acquisiscono maggiori informazioni da un numero crescente di sistemi. Fornendo funzionalità predefinite di livello superiore, l'interazione automatica con le soluzioni esistenti per la gestione della sicurezza e la personalizzazione da parte dell'utente, McAfee® Active Response restringe notevolmente la finestra di opportunità a disposizione degli aggressori per danneggiare le risorse elaborazione e il brand dell'azienda.

Vantaggi principali

- **Automatizzato:** acquisizione e controllo del contesto e dello stato dei sistemi alla ricerca di modifiche come gli indicatori di attacco, oltre a individuazione di componenti di attacco dormienti e invio di informazioni ai gruppi di analisi, operazioni e forensi.
- **Adattabile:** una volta allertato, puoi adeguarti ai cambiamenti nelle metodologie di attacco, automatizzare la raccolta dei dati, gli allarmi e le risposte agli elementi di interesse, nonché personalizzare la configurazione ai flussi di lavoro dei clienti.
- **Costante:** strumenti di raccolta tenaci attivano elementi per il rilevamento degli attacchi, avvisando te e i tuoi sistemi dell'attività d'attacco che hai osservato.

Il panorama in evoluzione delle minacce

Le aziende si sono rese conto che potrebbero essere violate da un aggressore in qualsiasi momento e che devono essere preparate per affrontare in modo efficace tali violazioni tramite rilevamento precoce di un attacco, dell'attività in corso o la scoperta di indicatori di attacco. Oltre a ciò le aziende comprendono anche che sono necessarie nuove tecnologie per risolvere le attuali falle in termini di visibilità, scoperta, rilevamento e risposta.

Limitazioni degli attuali approcci per la risposta agli eventi

Quando viene loro chiesto di analizzare un evento sospetto o conosciuto all'interno dell'intera azienda, i responsabili della risposta agli eventi e gli amministratori della sicurezza sono limitati tipicamente da tue fattori fondamentali: tempo e portata. Sebbene numerose informazioni dettagliate vengano acquisite dai sistemi o strumenti esistenti, è necessario davvero molto tempo per raccogliere e analizzare tali informazioni. Poiché la velocità è un requisito critico per la raccolta dei dati, vengono accettati compromessi significativi in termini di natura dei dati raccolti, oltre al numero di sistemi da cui vengono acquisiti. Inoltre, l'elaborazione dell'enorme quantità di dati raccolti che deve essere ordinata per identificare le informazioni principali sta diventando sempre più difficile.

Gli strumenti più comunemente utilizzati per la risposta agli eventi sono gli script scritti da coloro che rispondo agli eventi. Tali strumenti forniscono la base di raccolta di dati da utilizzare per un'analisi più ampia. Questo insieme di conoscenze, insieme agli strumenti associati, è abbastanza maturo, ma la capacità di sfruttarli

Piattaforme supportate

- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2; Windows 7, 8, 8.1, 10
- Linux (Red Hat, CentOS, SUSE, Ubuntu)

su larga scala e con velocità è limitata. Questa mancanza di capacità di eseguire un'analisi live su indicatori di attacco specifici per l'intera azienda spesso porta coloro che rispondono alle minacce ad avere una visione miope nelle loro attività di scoperta e risposta. Tipicamente, queste attività vengono limitate artificialmente per soddisfare i requisiti temporali e ciò può contribuire a carenze significative nel processo di risposta agli eventi. Questo mette seriamente in svantaggio coloro che rispondono agli eventi, poiché i loro sforzi vengono limitati artificialmente dai vincoli degli strumenti attuali.

Rilevamento completo degli endpoint e risposta

McAfee Active Response consente di rilevare costantemente e rispondere alle minacce avanzate alla sicurezza per aiutare i professionisti della sicurezza a controllare lo stato di sicurezza, migliorare il rilevamento delle minacce e ampliare le funzionalità di risposta agli eventi attraverso attività di rilevamento di minacce future, analisi dettagliata, analisi forense, reportistica completa e allarmi e azioni prioritizzate. Ottimizzato per soddisfare i rigidi criteri per il rilevamento degli endpoint e la risposta, McAfee Active Response utilizza collettori predefiniti e personalizzabili dall'utente per effettuare ricerche approfondite su tutti i sistemi per individuare indicatori d'attacco che non sono solo presenti tramite processi di esecuzione ma potrebbero anche essere dormienti o essere stati cancellati. Inoltre, McAfee Active Response permette agli utenti non solo di ricercare un indicatore d'attacco nel presente, ma anche di allertare e agire in accordo con gli obiettivi di sicurezza tramite attivatori che forniscono istruzioni qualora l'indicatore di attacco si dovesse manifestare in futuro.

McAfee Active Response è una dimostrazione dell'efficacia dell'architettura Security Connected. McAfee Active Response offre visibilità costante e approfondimenti efficaci relativamente agli endpoint per poter identificare le violazioni più rapidamente. Inoltre, mette a disposizione gli strumenti necessari per correggere i problemi più rapidamente e nel modo più adeguato per l'azienda. Tutta questa potenza è gestita tramite il software McAfee® ePolicy Orchestrator® (McAfee ePO™) che sfrutta McAfee Data Exchange Layer, offrendo scalabilità ed estendibilità senza la necessità di personale incrementale per amministrare il prodotto.

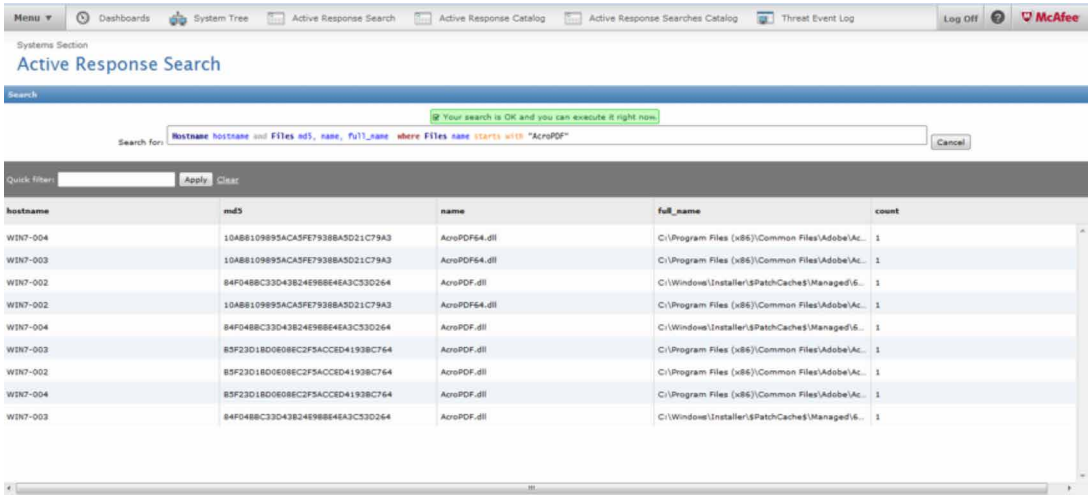

Figura1. Interfaccia utente di ricerca McAfee Active Response.

Funzione	Vantaggio	Vantaggi per il cliente	Differenziazione
Strumenti di raccolta	Gli strumenti di raccolta permettono agli utenti di individuare e visualizzare i dati dai loro sistemi.	Gli strumenti di raccolta offrono funzionalità di ricerca per effettuare un'analisi approfondita all'interno dei sistemi. Forniscono visibilità su violazioni critiche o potenziali attacchi per acquisire e visualizzare i dati da tali sistemi. Utilizzando uno dei molti linguaggi comuni di scripting, gli utenti possono personalizzare facilmente i propri strumenti di raccolta e risposta, offrendo configurabilità e adattabilità ottimali.	McAfee Active Response guarda oltre file eseguibili o in esecuzione in codice che potrebbe essere dormiente o anche cancellato nel tentativo di mascherare le tracce dell'aggressore. McAfee Active Response può ricercare file, flussi di rete, registri e mappatura dei processi.
Attivatori	Gli attivatori permettono a un professionista della sicurezza di monitorare costantemente un evento critico o un cambiamento di stato con una serie di istruzioni sia nell'immediato che in futuro.	Le azioni vengono avviate da un attivatore preimpostato, generando un evento o eseguendo le risposte. McAfee Active Response non si limita ad "anteprime" statiche ma utilizza una modalità di risposta costante.	McAfee Active Response può individuare le minacce oggi e attivare azioni per le minacce che possono verificarsi in futuro.
Reazioni	Le reazioni forniscono azioni preconfigurate e personalizzabili quando si verifica la corrispondenza delle condizioni dell'attivatore, consentendo di individuare ed eliminare le minacce.	Le reazioni consentono agli utenti di intraprendere azioni, come ricercare file che sono stati cancellati dal sistema da file hash (MD5 e SHA1), verificare se qualche host è attivamente collegato a un indirizzo IP o è stato collegato a un indirizzo IP in passato, o ricercare un file pericoloso non basato su Windows PE che non è stato consultato o attivato sul sistema (ricerca di un PDF pericoloso su un sistema laddove era stato copiato, ma non aperto, sul file system).	McAfee Active Response è preconfigurato per agire sui risultati delle ricerche e impostare azioni personalizzate stabilite dall'utente per soddisfare un'esigenza specifica definita dall'utente.
Gestione centralizzata tramite il software McAfee ePO	L'ambiente con una console unica offre funzioni complete di gestione e automazione.	Gli amministratori possono sfruttare il software McAfee ePO come parte di Security Connectd per indirizzare risposte automatiche agli attivatori e ricercare, rispondere e mitigare le minacce. La gestibilità tramite un unico riquadro di visualizzazione offre maggior visibilità sulla sicurezza senza oneri amministrativi ulteriori. Semplifica gli aspetti operativi e richiede minor tempo allo staff amministrativo.	La possibilità di gestire e agire con un'unica console è un chiaro elemento di differenziazione. Utilizzando un'unica console, proteggiamo in modo unico una varietà di piattaforme con una potente serie di controlli di sicurezza, tra cui McAfee Active Response.
Security Connected	Sfrutta Data Exchange Layer (DXL) per ottimizzare le comunicazioni con altri prodotti di McAfee, parte di Intel Security.	L'integrazione con Security Connected riduce il rischio e i tempi di risposta nonché i costi di gestione e dello staff operativo grazie ai concetti innovativi, ai processi ottimizzati e ai consigli pratici offerti dalla piattaforma.	

Maggiori informazioni sui vantaggi di McAfee Active Response sono disponibili all'indirizzo **www.mcafee.com/it/about/active-response-technology-preview.aspx**.

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com