McAfee Investigator

Trasforma gli analisti in ricercatori esperti

McAfee® Investigator aiuta gli analisti a risolvere un maggior numero di casi più rapidamente con maggior certezza di aver stabilito la causa principale. Gli allarmi prioritizzati innescano un'esplorazione guidata da esperti che raccoglie i dati di supporto, interpreta le prove e presenta gli approfondimenti necessari per convalidare pienamente e rapidamente le minacce e quindi rispondere.

Problematiche delle divisioni dedicate alla sicurezza

Enormi volumi di eventi e problemi relativi al periodo di conservazione dei dati rendono difficile valutare con precisione l'importanza e l'entità di un avviso. Gli analisti spesso ignorano gli allarmi perché non dispongono del contesto o della conoscenza per decidere se debbano essere trattati come un incidente formale.

Le indagini di eventuali incidenti selezionati possono quindi richiedere molto tempo e una notevole esperienza sui vettori delle minacce per indagare fino al cuore del problema. Tali trend indicano che la necessità di analisti esperti nelle divisioni dedicate alla sicurezza è in crescita, mentre il gruppo di talenti disponibili non lo è.

Nuove analisi investigative

Per affrontare tale problema, i team della divisione sicurezza devono ottimizzare e velocizzare l'assegnazione di priorità agli allarmi e le indagini per consentire allo staff esistente e agli analisti junior di fare di più.

McAfee Investigator inserisce indagini guidate che includono valutazione, raccolta completa dei dati e analisi avanzate alla portata di ogni team della divisione sicurezza. Poiché è un'offerta SaaS, sistemi esperti e strumenti di acquisizione endpoint si integrano con le fonti di dati e i sistemi di gestione della sicurezza esistenti per conseguire rapidamente un valore con uno sforzo minimo.

Queste analisi interattive forniscono indicazioni costantemente aggiornate per consentire agli incaricati di rispondere agli incidenti di analizzare in modo completo malware, minacce alla rete e IoC (Indicator of Compromise) in minor tempo e con una maggior precisione.

Dati approfonditi alla velocità della macchina

La soluzione McAfee Investigator migliora immediatamente il processo di classificazione consentendo alle operazioni di sicurezza di automatizzare la definizione delle priorità di determinate situazioni per un'attenzione immediata.

Vantaggi principali

- **Riduzione del tempo di attesa:** un'accurata analisi dei dati relativi al caso migliora il rilevamento della causa principale piuttosto che porre rimedio ad un sintomo.
- **Dagli allarmi ai casi:** diminuzione del tempo dedicato ad indagini manuali e a bassa priorità.
- **Focalizzazione su ciò che è sconosciuto:** focalizzazione su reperti e dettagli che necessitano di interpretazione e decisioni umane.
- **Miglioramento del processo di triage:** elaborazione di un maggior numero di casi più rapidamente con una maggior qualità.
- **Riduzione della pressione sugli analisti:** miglior impiego di tempo limitato, energia e capacità cognitiva.
- **Sviluppa le abilità degli analisti:** guide e approfondimenti pertinenti istruiscono gli analisti sulle giuste domande da porre e ipotesi all'interno del flusso di lavoro.
- **Incremento del valore dei sistemi attuali:** le fonti dati esistenti e le analisi vengono migliorate per incrementare il focus e la precisione.

Per questi allarmi, e per altri che un analista desidera prendere in esame, McAfee Investigator acquisisce, organizza, riassume e visualizza gli allarmi, l'attività, la prova e le informazioni raccolte su un attacco sospetto.

I dati pertinenti vengono acquisiti in background e includono solo gli approfondimenti importanti per un'analisi su una specifica minaccia che porterà a prendere una decisione. I dati provenienti dalle soluzioni per la gestione delle informazioni e degli eventi di sicurezza (SIEM) possono essere arricchiti con i dati degli endpoint, senza richiedere la presenza di agent EDR (Endpoint Detection e Response) su ogni nodo. Questo modello sostituisce i silos con visibilità contestuale su IoC, tattiche, tecniche, procedure e relazioni.

Un motore di analisi dei dati e di apprendimento automatico confronta i dati delle prove con le linee di riferimento conosciute e le fonti di intelligence delle minacce. Analizza gli elementi ed arricchisce le principali informazioni ambigue.

Acquisendo e assegnando le priorità ai dati giusti in modo automatico, McAfee Investigator riduce l'impegno e aumenta la velocità con cui gli analisti possono determinare il rischio e l'urgenza dell'incidente. Gli analisti possono prendere decisioni di triage accurate più velocemente e concentrarsi sulle minacce più significative.

A livello organizzativo, i vantaggi si moltiplicano. Aumentando il triage dalle revisioni degli avvisi ai casi contestuali, ciascun analista può essere più efficiente, gli analisti di livello 1 possono sistemare più casi e il tempo degli analisti viene dedicato alle attività di valore più elevato.

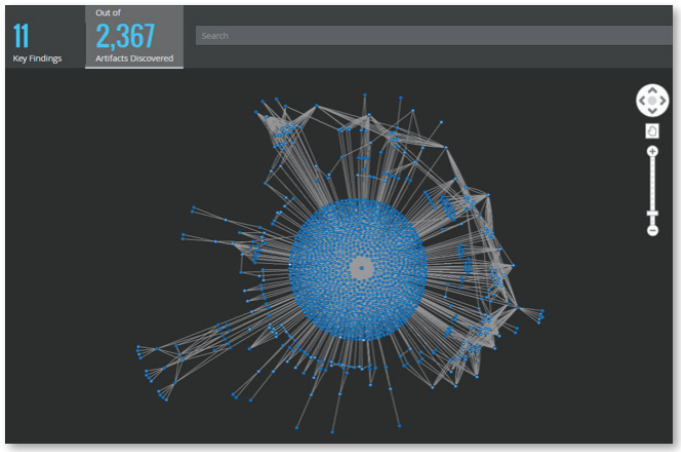

Figura 1. McAfee Investigator acquisisce migliaia di elementi di prova.

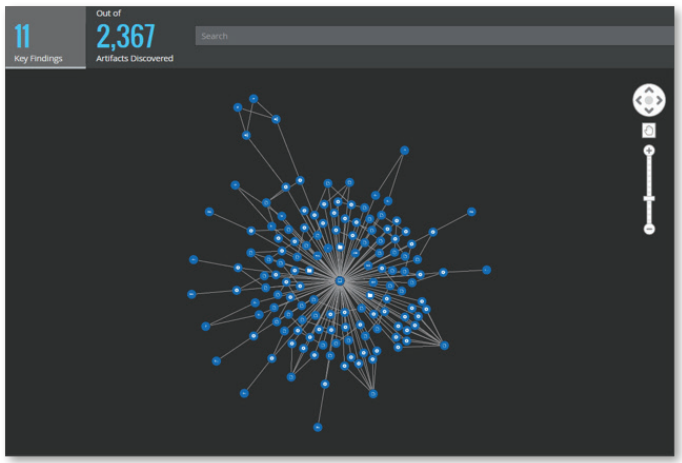

Figura 2. McAfee Investigator quindi applica analisi e indicazioni avanzate per presentare i risultati che contano.

Funzionalità principali

- Acquisizione precisa di dati on demand
- Agent temporaneo di acquisizione endpoint
- Interpretazione dei dati acquisiti sulla base di una guida esperta e intelligenza artificiale
- Visualizzazioni interattive
- Ipotesi multi-vettore per esaminare dati plausibili
- Linee guida per l'intelligence istituzionale
- La gestione dei casi guida lo staff e consente la condivisione delle informazioni durante le indagini

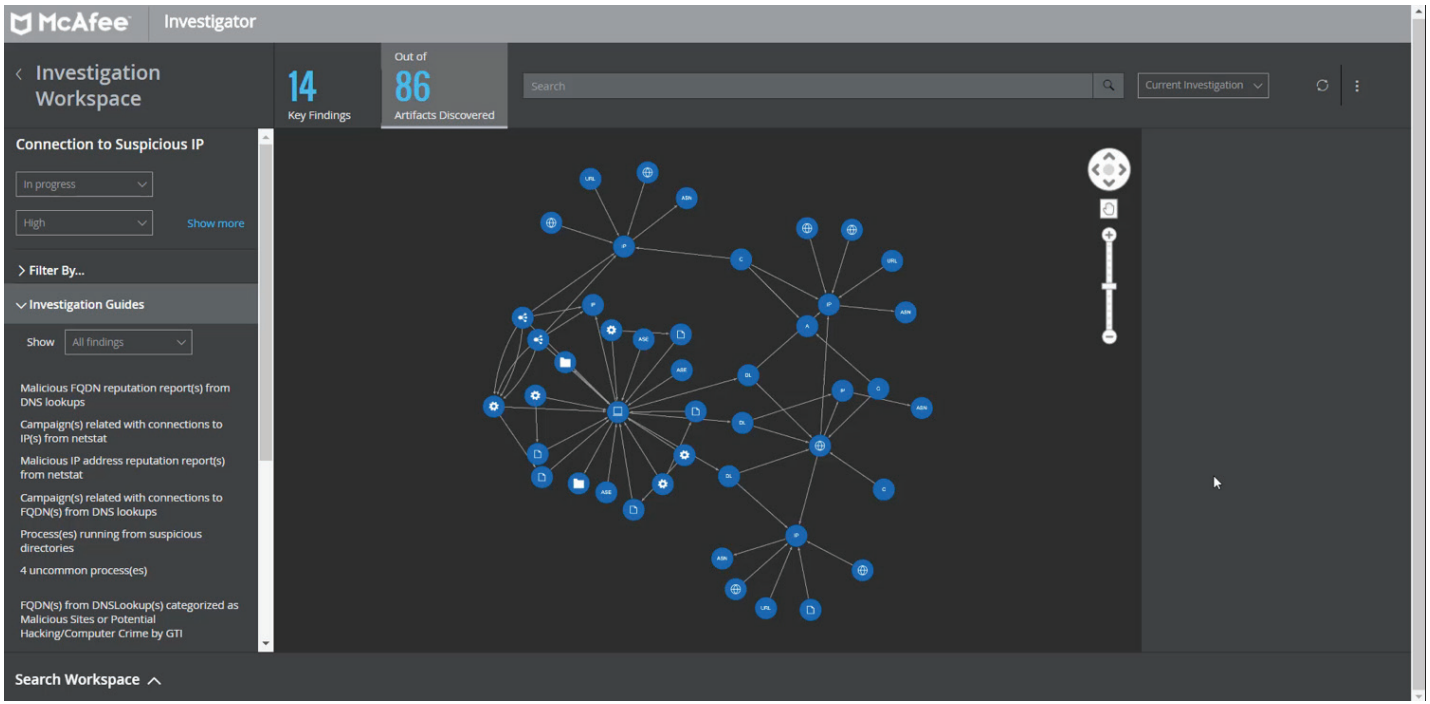

Figura 3. Lo spazio di lavoro rende i risultati principali ovvi e facili da esplorare.

Guida le indagini con competenze specialistiche

Quando viene scelto un incidente per un'indagine dettagliata, gli analisti si avvalgono di guide interattive che permettono loro di concentrarsi su ciò che è importante. Le guide investigative non sono basate su script o statiche. Il sistema imita il processo mentale umano, esplorando diverse ipotesi in parallelo per la massima velocità e precisione.

Le guide leggibili dall'uomo sono state create combinando l'esperienza dei ricercatori Foundstone® con l'intelligenza artificiale. Questo è un modo in cui McAfee Investigator incarna la collaborazione uomo-macchina.

Lo spazio di lavoro organizza le informazioni dettagliate e i risultati per aiutare gli analisti a porre le domande giuste. Questa esplorazione mirata e multi-vettore porta ad una chiusura dei casi efficiente ed accurata con maggior certezza di aver stabilito la causa principale da parte degli analisti.

Esperienza e capacità scalabili

Lo spazio di lavoro interattivo di McAfee Investigator presenta i flussi di lavoro e la navigazione attraverso i dati all'interno di un singolo ambiente cognitivo. Questo modello migliora l'efficienza e riduce la varietà di informazioni generata dalla moltitudine di tipi di allarmi ed elimina la necessità di controllare più schermi.

Lo spazio di lavoro istruisce i neofiti e gli analisti di livello intermedio per implementare i processi mentali di analisti esperti, creando competenze senza necessità di formazione separata.

Sfrutta strumenti e dati esistenti

McAfee Investigator opera con un sistema SIEM e il software McAfee® ePolicy Orchestrator® per arricchire fonti dati, linee guida, correlazioni e allarmi esistenti con analisi avanzate. Un agent temporaneo acquisisce nuovi dati endpoint che sono particolarmente determinanti per l'interpretazione precisa di prove tenui. L'integrazione tra McAfee Investigator e McAfee Active Response consente agli analisti di valutare l'impatto di una minaccia sui loro endpoint in tempo reale. Un feed attività condivide i dati con strumenti di terze parti per collegarsi ai flussi di lavoro correnti, snellire i processi e migliorare la collaborazione. I servizi professionali velocizzano il processo di onboarding e l'attivazione.

Ulteriori informazioni

Con McAfee Investigator, una volta che si ha un sospetto, non è necessario passare ore a raccogliere dati e ancora più tempo a interpretarli. Il motore di analisi avanzata alla base di McAfee Investigator analizza e classifica in ordine di priorità gli avvisi di minaccia all'interno di un'interfaccia basata sul contesto per scalare le operazioni di sicurezza. McAfee Investigator automatizza l'utilizzo di conoscenza esperta all'interno delle indagini a livello di SOC, consentendo agli analisti di lavorare in modo più intelligente, rapido e con maggior precisione.

Questa si definisce collaborazione uomo-macchina.

Visita **www.mcafee.com/it/products/investigator.aspx** per maggiori informazioni.

McAfee
Together is power.

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