Panoramica sulla soluzione

La messa in opera delle informazioni sulle minacce

Dietro ogni allarme autentico ricevuto dal tuo reparto di sicurezza informatica si cela un avversario che utilizza varie tecniche di attacco per penetrare nella tua infrastruttura e comprometterne sistemi vitali o risorse dati. Gli attacchi mirati multifase consistono di una serie di passaggi che vanno a costituire la catena dell'attacco informatico: ricognizione, scansione alla ricerca delle vulnerabilità, loro sfruttamento e trafugamento di preziosi dati aziendali.

Gli analisti della sicurezza conoscono bene tali tecniche e dipendono dalle informazioni sulle minacce per approfondire i metodi e le motivazioni degli attacchi. Possono così rilevare e bloccare le minacce avanzate, applicare la remediation adeguata e prepararsi meglio la prossima volta che scatta un allarme di sicurezza. Tuttavia, troppo spesso non dispongono della visibilità su determinati sistemi oppure vengono inondati da troppi dati e troppo poche informazioni. Secondo lo studio *Who's Using Cyberthreat Intelligence and How? (Chi usa le informazioni sulle cyber minacce e in che modo?)* dell'Istituto SANS, "... solo l'11,9% degli intervistati ha raggiunto la capacità di aggregare le informazioni sulle minacce virtualmente da ogni fonte, mentre solo l'8,8% ha un quadro completo in grado di combinare gli eventi con gli indicatori di compromissione[1]".

In un recente rapporto, Forrester sottolinea che, nelle grandi imprese europee e nordamericane, il 77% dei decisori in materia di sicurezza indica come una priorità il miglioramento delle capacità in termini di informazioni sulle minacce informatiche[2]. Le informazioni di intelligence sulle minacce informatiche avvisano preventivamente gli addetti alla sicurezza del fatto che dei criminali informatici hanno preso di mira la loro regione, settore o anche specifiche aziende, così hanno il tempo di adottare delle contromisure. Tuttavia la sicurezza informatica presenta ancora notevoli problemi:

- Come correlare le informazioni sulle minacce provenienti dalle fonti esterne e interne?
- Come correlare i dati e ordinare per priorità i rischi?
- Come distribuire l'intelligence proveniente dai controlli di sicurezza di diversi fornitori, in tutta l'impresa?
- Come ottenere una maggiore visibilità nell'ambiente informatico, al fine di agire in modo rapido e appropriato?

Le imprese moderne hanno bisogno di un'architettura aperta e integrata che faciliti l'adozione dell'intelligence sulle minacce cogliendone i vantaggi, dalla raccolta delle informazioni basilari sulle minacce all'arricchimento delle analitiche SIEM. In altre parole gli utenti devono poter mettere all'opera le informazioni sulle minacce tramite dei processi automatizzati che ne agevolino analisi, elaborazione e gestione.

intel Security

Minacce nuove richiedono un nuovo approccio alle informazioni

Dato che complessità, precisione e volume degli attacchi continuano ad aumentare, l'approccio adottato finora alle informazioni sulle minacce non è più adeguato. Analizzare gli attacchi mirati non è un'impresa facile. Il comportamento dinamico degli aggressori, la maggiore varietà e disponibilità delle fonti locali e globali di informazioni sulle minacce e la diversità dei loro formati possono rendere l'aggregazione ed elaborazione delle informazioni nei centri operazioni di sicurezza (SOC) difficili come mai prima d'ora.

Un ambiente plurifornitore, tipico della maggior parte delle imprese, complica ulteriormente la condivisione dei dati degli eventi e la promozione della visibilità nell'organizzazione. Come sottolinea Gartner nel suo report *Technology Overview for Threat Intelligence Platforms* (*Panoramica della tecnologia per le piattaforme di informazioni sulle minacce)*, "L'incapacità di un'organizzazione di condividere le informazioni costituisce un vantaggio per gli autori delle minacce informatiche. La condivisione è un moltiplicatore di forza e sta diventando un elemento chiave per stare al passo del crescente numero di attori delle minacce e degli attacchi che usano[3]".

Ma da sola la condivisione delle informazioni sulle minacce non necessariamente produce una serie di azioni correttive e misure di prevenzione sostenibili. Gli analisti della sicurezza possono essere rapidamente sommersi da troppe informazioni. La maggior parte dei team di sicurezza è impegnata in estenuanti procedure manuali (vedere la Figura 1) per l'analisi di milioni di eventi di sicurezza e di file sospetti, nel tentativo di correlare una montagna di dati e ricostruire l'attacco mirato. In ultima analisi ciò compromette la completezza e la velocità del processo di risposta. A causa della comprensione incompleta delle minacce, i team di sicurezza stentano a contenere tempestivamente gli attacchi. Nel recente studio di Intel Security: *Quando i minuti sono fondamentali, 2014*, meno del 25% degli interpellati ha affermato di poter rilevare un attacco in pochi minuti[4].

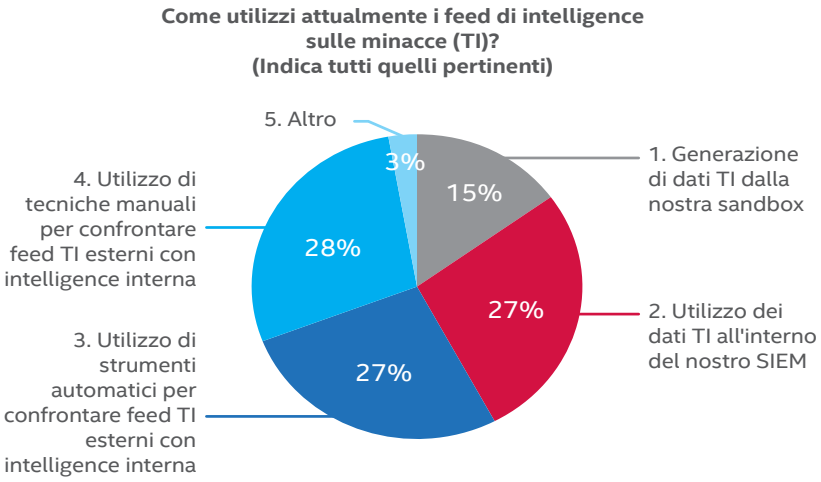

Figura 1. Secondo il sondaggio di Intel Security svolto durante BlackHat 2015, un gran numero di utenti impiega ancora delle tecniche manuali per confrontare i flussi esterni di informazioni sulle minacce con quelli interni.

"Per la nostra infrastruttura di sicurezza avevamo necessità di molto più di un semplice fornitore di tecnologia. Era assolutamente essenziale avviare una collaborazione con un partner che potesse aiutarci a gestire i diversi requisiti della clientela e le minacce in costante evoluzione. McAfee offre tale collaborazione e le informazioni di sicurezza che riceviamo continuamente dalle soluzioni McAfee sono cruciali per poter mantenere efficienti le nostre attività".

– Anurana Saluja
CISO e Vice President
Information Security
Sutherland Global Services

Mettere in opera le informazioni sulle minacce

Il rilevamento e la neutralizzazione delle minacce in base alle informazioni richiedono ben più che la sola importazione manuale nell'elenco di sorveglianza SIEM una volta alla settimana degli indirizzi IP ostili pubblicati su un sito web aperto. È invece necessaria l'inserimento delle informazioni sulle minacce in tempo reale e della correlazione di tutte le sfaccettature di un attacco, compresi i metodi e le campagne globali. In tal modo le imprese possono prevenire anche le minacce più furtive e in più rapido adattamento. I SOC aziendali necessitano di un modo per "mettere all'opera le informazioni sulle minacce" al fine di ottenere il quadro completo degli attacchi che colpiscono i loro ambienti. Hanno poi bisogno di un modo per setacciare la massiccia quantità di dati al fine di analizzare, correlare e ordinare per priorità le informazioni e determinare quelle rilevanti per il loro settore,

la loro area geografica e la loro azienda. Infine devono poter approfondire gli specifici attacchi che si possono verificare nel presente, oltre alle tendenze, in base ai dati storici degli eventi di sicurezza. Come sottolinea Forrester, è fondamentale mettere all'opera le informazioni sulle minacce, dato che il 75% degli attacchi si diffonde da una vittima all'altra nel giro di 24 ore. Le grandi imprese devono colmare la lacuna tra "la velocità della condivisione e la velocità dell'attacco[5]".

Sfrutta l'architettura integrata di Intel Security

Intel Security offre una piattaforma di collaborazione unificata, dotata di tutti i componenti necessari per la messa all'opera delle informazioni sulle minacce, comprendenti i feed globali, le fonti locali, la condivisione in tempo reale nell'infrastruttura informatica, la gestione delle informazioni e degli eventi legati alla sicurezza e una protezione adattiva e automatizzata.

Requisiti per le informazioni sulle minacce	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Raccoglie le informazioni sulle minacce provenienti da fonti esterne	STIX, importazione in McAfee Global Threat Intelligence (McAfee GTI) e VirusTotal	Importazione in McAfee GTI	McAfee GTI, importazione in TAXII/STIX e feed sulle minacce HTTP tramite il gestore delle minacce informatiche di McAfee Enterprise Security Manager	McAfee GTI aggrega le informazioni sulle minacce provenienti dai vari partner della Cyber Threat Alliance e da fonti pubbliche. McAfee GTI estrae le informazioni sulle minacce provenienti dai milioni di sensori dei prodotti Intel Security usati dalla clientela e relativi a endpoint, web, posta elettronica, sistemi di prevenzione delle intrusioni (IPS) in rete e dispositivi firewall.
Acquisisce le informazioni interne sulle minacce	Riceve i campioni da McAfee VirusScan®, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense, McAfee Enterprise Security Manager e dai prodotti di terzi, inviando le informazioni tramite McAfee Data Exchange Layer	Esegue in sicurezza i campioni di file ricevuti da McAfee Threat Intelligence Exchange o dalla rete	Tramite STIX/TAXII e McAfee Data Exchange Layer	
Produce informazioni locali sulle minacce	Registra le occorrenze dei file sospetti e crea un database locale che registra il primo contatto e la traiettoria delle minacce	Esamina i file, determina quali sono malware, genera informazioni locali sulle minacce e le distribuisce tramite McAfee Data Exchange Layer o come API formattata con STIX.	A partire dalle informazioni sulle minacce crea elenchi di sorveglianza, report e visualizzazioni in base agli eventi correlati	
Distribuisce le informazioni sulle minacce fra i vari controlli di sicurezza	Tramite McAfee Data Exchange Layer	Tramite McAfee Data Exchange Layer e l'API del prodotto	Tramite McAfee Data Exchange Layer, l'API del prodotto e l'integrazione dello script	McAfee GTI è integrato con numerosi prodotti di Intel Security, come McAfee Web Gateway, McAfee Enterprise Security Manager e le soluzioni endpoint McAfee
Offre visibilità sulle informazioni raccolte	Tramite le dashboard di McAfee Threat Intelligence Exchange	Tramite la reportistica	Tramite le dashboard, le viste e i report forniti nei pacchetti di contenuti oppure generati dal cliente	Tramite McAfee Threat Center e il report trimestrale McAfee sulle minacce

Tabella 1. La piattaforma integrata Intel Security per le informazioni sulle minacce.

Inserimento, analisi e propagazione

McAfee Global Threat Intelligence

Un buon punto di partenza per realizzare la tua piattaforma integrata di informazioni sulle minacce è McAfee Global Threat Intelligence (McAfee GTI), un servizio di reputazione completo, in tempo reale e basato sul cloud, che è pienamente integrato con i prodotti Intel Security, ai quali permette di bloccare meglio le minacce informatiche in tutti i vettori – file, web, messaggi e rete – rapidamente. McAfee GTI assegna un punteggio reputazione a miliardi di file, URL, domini e indirizzi IP, in base ai dati sulle minacce raccolti da svariate fonti: milioni di sensori globali monitorati e analizzati da McAfee Labs, i feed sulle minacce provenienti dai partner di ricerca della Cyber Threat Alliance e i dati multivettore provenienti da web, email e reti. Supportato dai feed rilevanti e di alta qualità sulle minacce, McAfee GTI offre suggerimenti accurati per prendere decisioni informate sulle politiche da adottare e che consentono ai controlli di bloccare, ripulire o consentire, a seconda delle circostanze.

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (SIEM) porta l'inserimento e l'analisi delle informazioni sulle minacce a un livello superiore, fornendo un hub per riunire e analizzare ogni tipo di informazione e agire di conseguenza. Questa visuale a 360° fornisce la visibilità completa e la consapevolezza della situazione, al fine di velocizzare il rilevamento e la risposta agli attacchi mirati. Il suo sistema di gestione avanzata dei dati è appositamente studiato per memorizzare e assimilare volumi elevati di dati contestuali in tempo reale.

McAfee Enterprise Security Manager raccoglie i dati di attività ed eventi provenienti da tutti i tuoi sistemi, database, reti e applicazioni. Importa inoltre i feed globali sulle minacce e utilizza le informazioni in formati e vettori standard, come il linguaggio Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) e Cybox, generalmente pubblicati da comunità o gruppi del settore, come Financial Services Information Sharing e Analysis Center (FS-ISAC). Tramite funzioni avanzate di analisi, traduce le informazioni raccolte in intelligence sulla sicurezza comprensibile e fruibile. Cosa ancora più significativa, offre una visibilità più approfondita sulle minacce emergenti tramite le viste in tempo reale e l'accesso alle informazioni storiche. Ciò consente di indagare a ritroso nel tempo per comprendere la prevalenza e le modalità di un attacco, oltre a creare automaticamente degli elenchi di osservazione per rilevare l'occorrenza o ri-occorrenza degli eventi nel futuro. Potenziando la sensibilità del tuo sistema agli eventi notoriamente dannosi, aumenti la tua capacità di rilevamento delle attività sospette e delle loro modalità nelle varie fasi della catena di attacco, per dare priorità alla risposta.

Che cos'è la Cyber Threat Alliance?

La **Cyber Threat Alliance** è un gruppo di professionisti della sicurezza provenienti da aziende che collaborano per condividere informazioni al fine di difendere meglio se stesse e i rispettivi clienti dai malintenzionati. Intel Security, una delle aziende fondatrici, ha dedicato le proprie risorse per determinare i modi più efficienti per condividere le informazioni sulle minacce, incoraggiare la collaborazione fra i membri del gruppo e lotta contro i più sofisticati criminali informatici.

Figura 2. Vista di McAfee GTI

McAfee GTI for McAfee Enterprise Security Manager porta la potenza delle capacità di ricerca di McAfee al monitoraggio della sicurezza aziendale. Il ricco feed di McAfee GTI, costantemente aggiornato, aumenta la percezione della situazione permettendo la rapida scoperta degli eventi, che includono le comunicazioni con gli IP sospetti o malevoli. Consente inoltre agli amministratori della sicurezza di determinare quali host aziendali hanno comunicato o stanno attualmente comunicando con i malintenzionati noti.

McAfee Threat Intelligence Exchange

Il terzo componente che puoi aggiungere durante lo sviluppo dell'ecosistema integrato di informazioni sulle minacce è McAfee Threat Intelligence Exchange, che aggrega e condivide le reputazioni dei file nell'intera infrastruttura di sicurezza. McAfee Threat Intelligence Exchange riceve le informazioni sulle minacce da McAfee GTI, dalle importazioni dei file in STIX, dai feed di McAfee Enterprise Security Manager, oltre che da endpoint, controllo delle applicazioni, dispositivi mobili, gateway, centri dati e tecnologie di sandbox, sia delle soluzioni di Intel Security che di altri fornitori. La raccolta dei dati da tutti i punti della tua infrastruttura fornisce informazioni su minacce che potrebbero essere presenti solo nel tuo ambiente, come molti attacchi mirati tendono a essere. Le informazioni sulla reputazione dei file vengono poi istantaneamente condivise attraverso l'intero ecosistema a tutti i prodotti e le soluzioni connessi a McAfee Threat Intelligence Exchange tramite McAfee Data Exchange Layer. Per esempio, se McAfee Threat Intelligence Exchange invia informazioni su un file eseguibile malevolo, McAfee Data Loss Prevention le riceve tramite McAfee Data Exchange Layer e quindi inizia a monitorare l'eseguibile nel caso acceda a dei dati sensibili.

I dati sulle minacce condivisi tramite McAfee Data Exchange Layer includono le reputazioni dei file, le classificazioni dei dati, l'integrità delle applicazioni e i dati contestuali degli utenti. Il tutto viene condiviso con e fra i prodotti integrati nel tessuto di McAfee Data Exchange Layer. Qualsiasi prodotto o soluzione può essere integrata in McAfee Data Exchange Layer e poi configurata per determinare le informazioni da pubblicare nel sistema e quelle da seguire e a cui abbonarsi.

McAfee Threat Intelligence Exchange funziona strettamente con McAfee Advanced Threat Defense, l'avanzata soluzione di sandboxing di Intel Security, che invia i dati delle analisi antimalware a McAfee Threat Intelligence Exchange. Se un file viene riscontrato come malevolo, McAfee Threat Intelligence invia, tramite McAfee Data Exchange Layer, un aggiornamento della reputazione del file stesso a tutti i sistemi connessi. Lo stesso meccanismo funziona anche in senso inverso. Quando gli endpoint abilitati da McAfee Threat Intelligence Exchange intercettano dei file dalla reputazione ignota, i file stessi possono essere inviati a McAfee Advanced Threat Defense per determinare se sono nocivi, eliminando così le zone d'ombra dalla consegna dei payload fuori banda. Questi due prodotti collaborano per creare una protezione automatizzata e adattiva contro le minacce emergenti. Le informazioni sugli attacchi scoperti vengono comunicate nel tuo ambiente per bloccare la catena dell'attacco informatico prima che possa causare altri danni.

Figura 3. La dashboard di McAfee Threat Intelligence Exchange

McAfee Threat Intelligence Exchange consente il rilevamento e la risposta adattivi, tramite la messa in opera delle informazioni fra le soluzioni di sicurezza per endpoint, gateway, rete e centri dati, in tempo reale. La combinazione delle informazioni globali importate con quelle raccolte a livello locale e la loro condivisione istantanea consentono alle tue soluzioni di sicurezza di funzionare come una sola, scambiando le informazioni condivise e agendo in base a esse.

Interruzione della catena dell'attacco informatico
Indipendentemente dalla posizione del primo punto di contatto di un file di malware sconosciuto, dopo che quest'ultimo è stato identificato come dannoso l'ambiente viene aggiornato immediatamente. Quando un file viene giudicato dannoso da McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange lo rende noto inviando un aggiornamento della reputazione, disseminata tramite McAfee Data Exchange Layer, a tutti i controlli di sicurezza integrati nell'organizzazione. I gateway abilitati da McAfee Threat Intelligence Exchange impediscono al file di penetrare nell'infrastruttura. Tramite la condivisione coordinata delle informazioni sulle minacce fra tutti i controlli di sicurezza, diventa più facile spezzare la catena dell'attacco e prevenire ulteriori danni senza la necessità di interventi manuali.

Elaborazione e applicazione: un rilevamento accurato per prendere decisioni migliori

Dopo aver utilizzato i dati sulle minacce, McAfee Enterprise Security Manager funge da punto centrale di visibilità, correlando i feed di McAfee GTI e McAfee Threat Intelligence Exchange e gli indicatori di compromissione (IoC) formattati secondo STIX/TAXII con i dati degli eventi, rilevati in tempo reale oppure storici, quando i nodi della tua rete stanno comunicando con noti malintenzionati o con domini sospetti. La dashboard di gestione delle minacce offre agli analisti una singola vista esaustiva di indicatori delle minacce raccolti, feed delle fonti, tasso di corrispondenza rispetto agli indicatori e dettagli intelligibili più significativi.

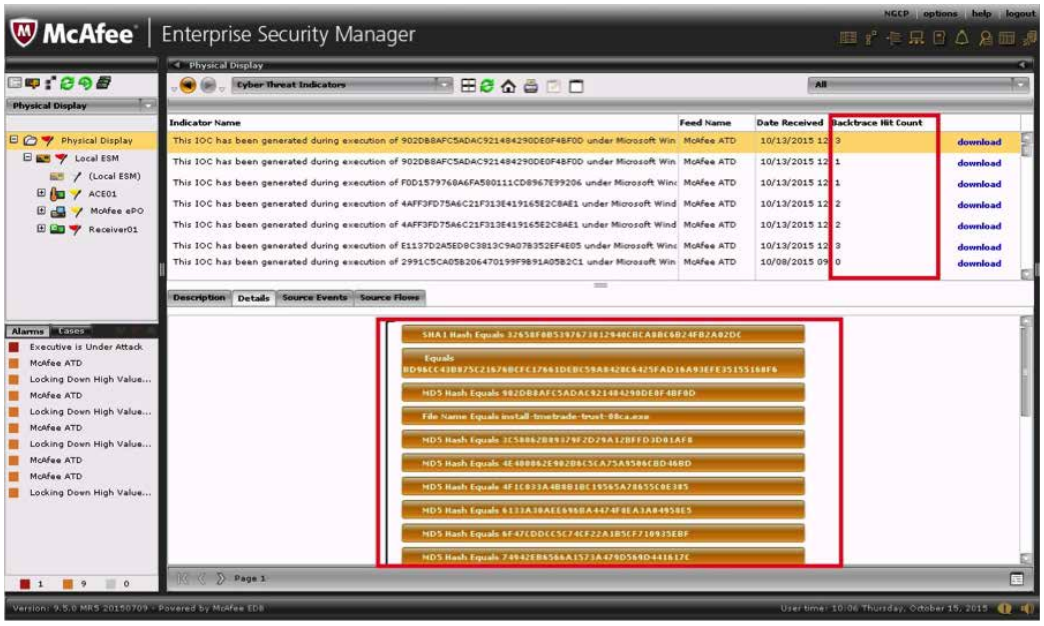

Figura 4. Indicatori delle minacce informatiche, conteggio corrispondenze di backtrace e dettagli degli IoC in McAfee Enterprise Security Manager

Usando il sistema Intel Security SIEM insieme ad altri strumenti collaborativi di informazioni sulle minacce si riducono i costi operativi associati con la configurazione delle regole di correlazione, che costituisce di solito un gravoso processo manuale. Per esempio, gli analisti della sicurezza possono leggere le informazioni appena ricevute in un formato intelligibile, che facilita la comprensione delle nuove minacce rilevate. Cosa ancora più importante è che le informazioni ricevute sulle minacce possono essere adottate dalle regole di correlazione in tempo reale o storiche, pertanto riducendo il tempo necessario per rilevare le attività ostili nuove o continuate. Gli utenti possono inoltre seguire l'avanzamento delle minacce segnalate in tutto il tuo ambiente informatico, oltre che tramite le informazioni contestuali delle viste degli allarmi, potendo così prendere decisioni migliori e più informate. Tutte le informazioni raccolte migliorano e velocizzano il rilevamento e l'indagine degli attacchi mirati.

Dato che le minacce cancellano rapidamente i segni del loro passaggio nell'infrastruttura informatica, McAfee Enterprise Security Manager aggiorna periodicamente tutte le informazioni acquisite, eliminando i dati obsoleti e meno rilevanti. Per esempio, i server di comando e controllo smantellati o i siti web ripuliti con un basso punteggio di reputazione pericolosa, vengono automaticamente rimossi per eliminare i falsi positivi che possono distogliere gli addetti alla sicurezza dalla caccia alle vere minacce.

I seguenti prodotti di Intel Security supportano le informazioni sulle minacce formattate in STIX:

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

Riepilogo

Le informazioni sulle minacce integrate da Intel Security mettono all'opera l'inserimento, elaborazione e gestione delle informazioni sulle minacce, permettendoti di aumentare l'accuratezza del rilevamento, eliminare le attività manuali e impedire ai malintenzionati di danneggiare il tuo business. Grazie alla maggiore visibilità e ai migliori approfondimenti sull'attività ostile nell'intero ecosistema di sicurezza, sei meglio preparato a identificare e prevenire gli attacchi mirati oggi, per impedirli in futuro.

Per saperne di più

Per maggiori informazioni sui fondamenti della piattaforma Intel Security di informazioni integrate sulle minacce, visita:

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **How to Use a TAXII Feed with McAfee Enterprise Security Manager (Come usare un feed TAXII con McAfee Enterprise Security Manager)**

1. **https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767**
2. **https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011**
3. **https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms**
4. **http://www.mcafee.com/it/resources/reports/rp-when-minutes-count.pdf**
5. **https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf**

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