SOPHOS
Cybersecurity made simple.

I 5 motivi per cui l'EDR è indispensabile

Gli strumenti di Rilevamento e risposta alle minacce endpoint (Endpoint Detection and Response, EDR) sono opzioni integrate nei sistemi che completano le attività di protezione degli endpoint, in quanto ottimizzano le capacità di rilevamento, indagine e risposta. Tuttavia, il clamore generato dagli strumenti di EDR distoglie l'attenzione dal loro vero scopo e dal perché sono indispensabili. Ad aggravare la situazione vi è il fatto che le moderne soluzioni di EDR non sono in grado di offrire un buon rapporto qualità-prezzo per molte organizzazioni; inoltre, sono spesso molto complicate, presentano diverse lacune di protezione e hanno un impatto eccessivo sulle risorse.

Sophos Intercept X Advanced with EDR integra un sistema intelligente di EDR alla nostra protezione endpoint, tutto in un'unica soluzione, garantendo alle organizzazioni il modo più semplice per offrire una risposta a qualsiasi domanda sugli incidenti di sicurezza, anche quelle più problematiche. Quelli che seguono sono solo alcuni dei motivi per cui consigliamo di prendere in considerazione una soluzione di EDR.

Analisi affidabile dello stato di sicurezza dei sistemi in qualsiasi momento

Spesso la principale motivazione per i team di sicurezza e il reparto informatico sono le statistiche relative ai livelli di protezione dei sistemi. Eppure, la domanda a cui la maggior parte del personale tecnico fa più fatica a rispondere è: "Siamo al sicuro in questo momento?". Ciò avviene perché la maggior parte delle reti presenta punti ciechi di dimensioni non indifferenti, che impediscono ai responsabili di sicurezza informatica e al personale tecnico di avere una visione completa di cosa accade nei propri ambienti.

La mancanza di visibilità è il motivo principale per cui le organizzazioni fanno fatica a capire l'estensione e l'impatto degli attacchi. Questo è evidente quando avviene un incidente e il personale tecnico dà per scontato di essere al sicuro per il semplice fatto che l'incidente è stato rilevato. Intercept X Advanced with EDR offre analisi più dettagliate, in grado di stabilire se sono stati colpiti anche altri computer. Se, ad esempio, viene individuato un file eseguibile sospetto nella rete, le soluzioni di sicurezza provvedono a rimuoverlo. Tuttavia, gli analisti potrebbero non sapere se tale file sia presente in altre parti della struttura informatica. Con Intercept X Advanced with EDR, questa informazione è disponibile pressochè in tempo reale. La capacità di visualizzare qualsiasi area in cui siano state individuate minacce, consente ai responsabili di sicurezza di attribuire una priorità agli incidenti, per permetterne un'ulteriore indagine ed eventuali attività di correzione.

La generazione di un quadro nitido sullo stato di sicurezza dell'azienda offre anche il vantaggio di poter compilare report sulla conformità. Queste informazioni aiutano a identificare le aree del sistema che potrebbero essere vulnerabili agli attacchi e permettono agli amministratori di stabilire se l'estensione di un attacco abbia avuto ripercussioni su aree contenenti dati di natura sensibile. Se ad esempio dovesse essere rilevato nei sistemi un malware che è riuscito a estrapolare dati dalla rete, un analista dovrà essere in grado di stabilire se questo incidente abbia coinvolto anche i computer contenenti informazioni mediche regolamentate dalla normativa statunitense HIPAA (Health Insurance Portability and Accountability Act). Con Intercept X Advanced with EDR questo processo sarebbe molto più semplice. Inoltre, come vantaggio aggiuntivo per il rispetto della conformità, renderebbe anche molto più semplice dimostrare che le informazioni dei pazienti sono al sicuro, grazie alla maggiore visibilità sugli endpoint.

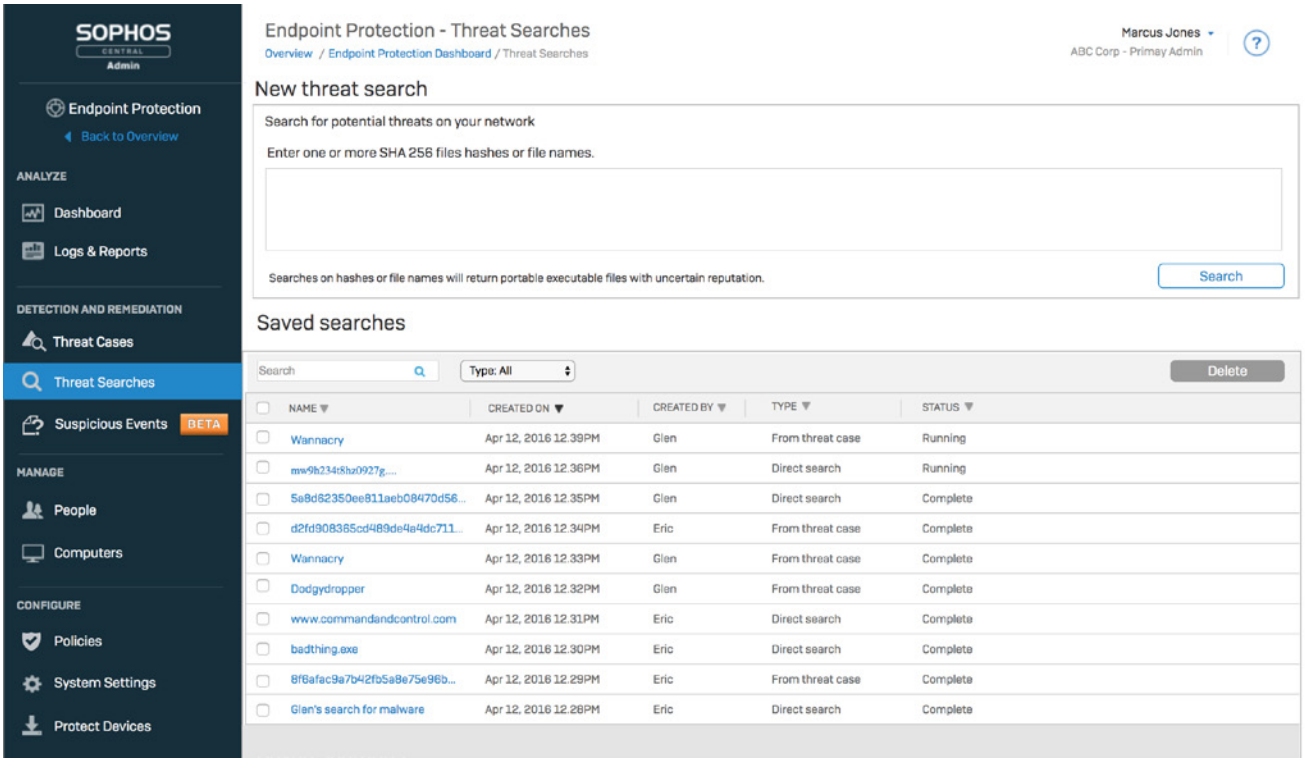

Figura 1: Sophos Intercept X Advanced with EDR mostra tutte le aree in cui è stata individuata una minaccia

Rilevamento degli attacchi che sono passati inosservati

Nell'ambito della cybersecurity, anche gli strumenti più all'avanguardia possono essere sconfitti, se gli autori degli attacchi hanno a disposizione tempo e risorse sufficienti. Di conseguenza, è difficile capire quale sia momento esatto in cui si verificano gli attacchi. Spesso le organizzazioni basano il proprio sistema di difesa solamente sulla prevenzione. Sebbene la prevenzione sia essenziale, l'EDR offre un ulteriore livello di rilevamento, con funzionalità potenzialmente in grado di individuare gli incidenti che sono passati inosservati.

Le organizzazioni possono utilizzare l'EDR per il rilevamento degli attacchi, cercando indicatori di compromissione (Indicator of Compromise, IoC). Si tratta di un metodo pratico e veloce per individuare gli attacchi che potrebbero essere passati inosservati. Di solito, le ricerche sulle minacce vengono attivate in seguito a una notifica di intelligence sulle minacce proveniente da una terza parte: può, ad esempio, capitare che un ente governativo (come ad es. US-CERT, CERT-UK o CERT Australia) comunichi a un'azienda di aver rilevato attività sospetta all'interno della sua rete. La notifica potrebbe essere accompagnata da un elenco di IoC, che possono essere utilizzati come punto di partenza per indagare sull'accaduto.

Sophos Intercept X Advanced with EDR offre un elenco dei principali eventi sospetti, per cui gli analisti possono avere un'indicazione specifica sul tipo di analisi da condurre (disponibile nel 2019). Grazie alle capacità di analisi dei SophosLabs, che sfruttano le tecniche di Machine Learning, la nostra soluzione può presentare un elenco dei principali eventi sospetti, classificati in base al relativo punteggio assegnato alle minacce. Tutto ciò semplifica l'attività degli analisti, che possono attribuire priorità diverse in modo da evidenziare prima gli eventi più importanti.

Gli eventi sospetti mettono anche in evidenza le situazioni più comuni in cui gli analisti sono tenuti a determinare se un elemento sia o meno malevolo. Questa opzione riguarda le attività che non presentano un aspetto abbastanza malevolo da determinarne la rimozione automatica, ma che sembrano pur sempre sospette e richiedono quindi un'analisi più approfondita. Tali attività rientrano in una "zona grigia", che richiede ulteriori analisi per confermare se gli elementi in questione siano malevoli, innocui o indesiderati.

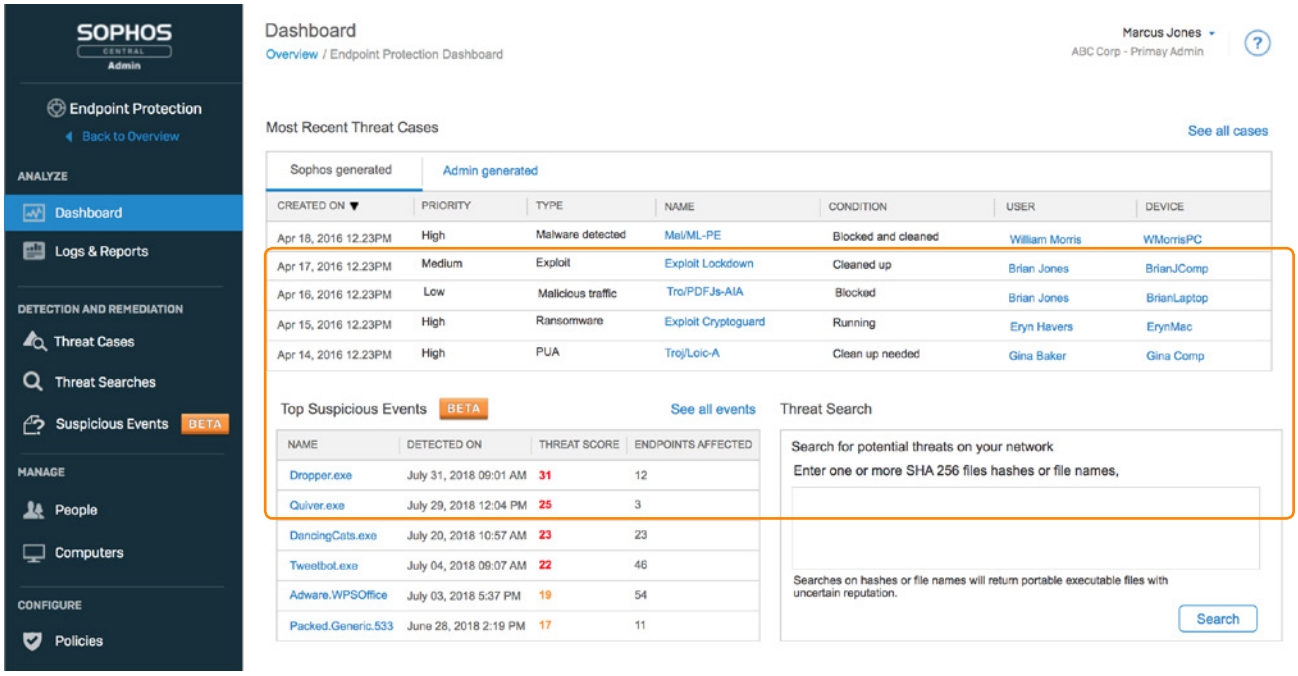

Figura 2: Sophos Intercept X Advanced with EDR offre la possibilità di cercare indicatori di compromissione all'interno della rete. Inoltre, sfrutta i vantaggi del Machine Learning per determinare i principali eventi sospetti su cui indagare (la funzionalità di individuazione degli eventi sospetti sarà disponibile nel 2019)

Risposta più rapida ai potenziali incidenti

Quando vengono rilevati incidenti, i responsabili di sicurezza e il personale tecnico cercano in tutti i modi di correggerli il più rapidamente possibile, per ridurne il rischio di diffusione e per limitare eventuali danni. Ovviamente, la domanda più importante da farsi è come sbarazzarsi individualmente di ciascuna minaccia. In media, a responsabili di sicurezza e personale tecnico occorrono più di tre ore per risolvere un incidente. L'EDR può accelerare il processo.

Per un analista, il primo passo da intraprendere durante il processo di risposta agli incidenti è impedire all'attacco di diffondersi. Intercept X Advanced with EDR isola gli endpoint su richiesta: un'azione fondamentale per arrestare la diffusione di una minaccia all'interno dell'ambiente. Spesso gli analisti isolano i sistemi prima di iniziare le indagini, per guadagnare tempo prezioso mentre determinano qual è la strategia migliore da adottare.

Le indagini possono essere un processo lungo e difficile, sempre che ci sia il tempo per effettuarle. Tradizionalmente, la risposta agli incidenti si basa soprattutto sulle capacità e sull'esperienza di analisti umani. Anche la maggior parte degli strumenti di EDR si affida all'abilità degli analisti di rivolgere le giuste domande e di interpretare le risposte in maniera corretta, ma con Intercept X Advanced with EDR, la risposta rapida agli incidenti è alla portata di chiunque si occupi della sicurezza (indipendentemente dal livello di competenze tecniche), grazie alle indagini guidate che offrono consigli sulle azioni successive da intraprendere, rappresentazioni visive nitide dell'attacco e dati integrati.

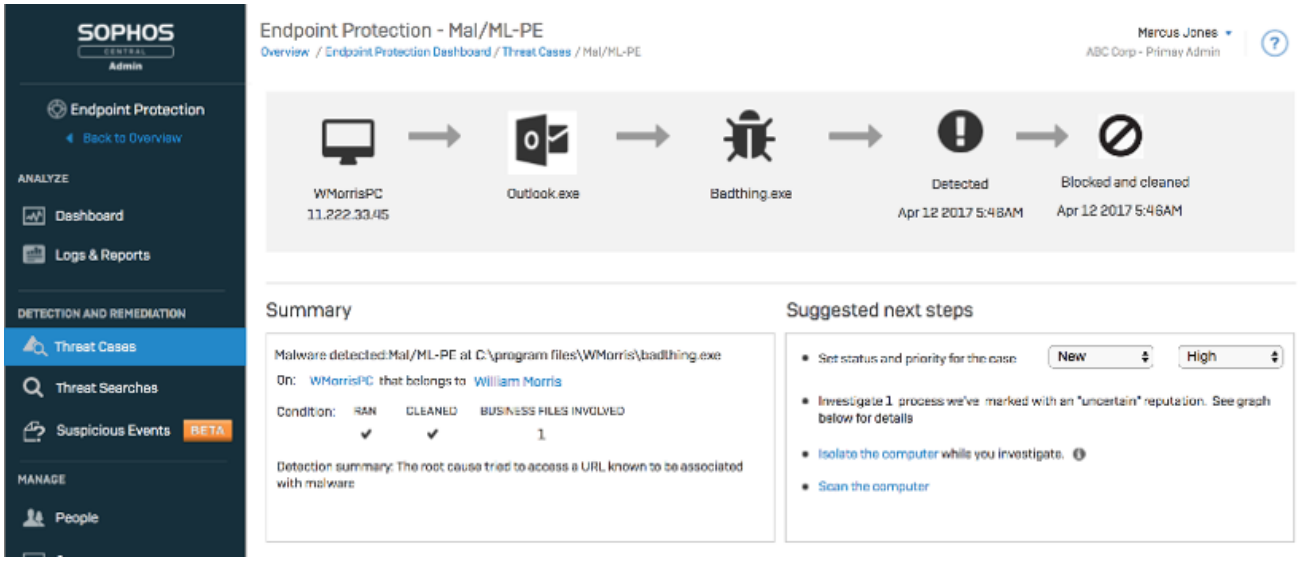

Figura 3: La risposta guidata agli incidenti offre le opzioni "Azioni successive consigliate" e "Isolamento endpoint" su richiesta per la risoluzione rapida e sicura degli incidenti.

Ottenuti i risultati dopo l'analisi effettuata, gli amministratori IT possono compiere la scelta migliore attraverso semplici passaggi. Tra le opzioni disponibili, è possibile isolare gli endpoint per attuare azioni di correzione immediate, a scopo di disinfezione e blocco dei file e per acquisire dati di analisi approfonditi. E se un file dovesse essere stato bloccato per errore, sarà possibile invertire il processo.

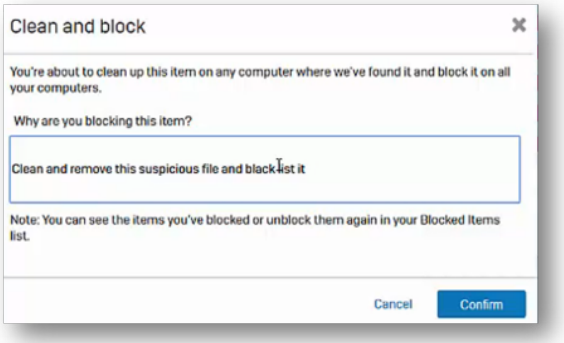

Figura 4: Intercept X Advanced with EDR include diversi pulsanti di azione, che offrono moltissime opzioni di correzione rapida, la più comune delle quali è "Disinfezione e blocco".

L'importanza di aggiungere competenze, non dipendenti

Le statistiche mostrano che le organizzazioni che desiderano aggiungere funzionalità di rilevamento e risposta alle minacce citano la "mancanza di dipendenti con adeguate competenze tecniche" come primo ostacolo all'adozione di un sistema di EDR. Questo dato non sorprende, in quanto sono diversi anni che si discute della mancanza di professionisti qualificati e dotati di competenze avanzate di cybersecurity. Questo ostacolo è ancora più insormontabile per le aziende di piccole dimensioni.

I motivi principali per cui le organizzazioni non implementano l'EDR

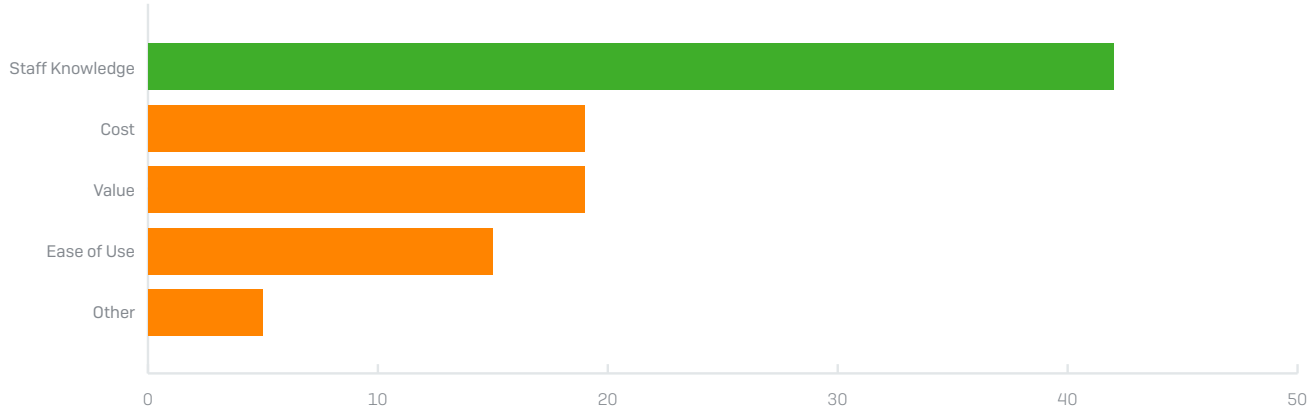

Figura 5: La mancanza di dipendenti con adeguate competenze tecniche è il motivo maggiormente citato dalle organizzazioni che non hanno adottato una soluzione di rilevamento e risposta alle minacce endpoint (Endpoint Detection and Response, EDR). (Fonte: Studio di Sapio in collaborazione con Sophos, ottobre 2018)

Per sopperire alla mancanza di competenze adeguate, Intercept X Advanced with EDR replica le capacità solitamente associate a questi analisti esperti, che sono figure professionali praticamente introvabili. La nostra soluzione sfrutta il Machine Learning per includere analisi approfondite di sicurezza ed è ottimizzata con i dati di intelligence sulle minacce gestiti dai SophosLabs. Ciò permette di aggiungere competenze senza dover assumere altri dipendenti. Le funzionalità intelligenti dell'EDR aiutano a colmare la mancanza di dipendenti dotati di competenze tecniche adeguate, riproducendo le funzioni di diversi tipi di esperti:

- Esperti di sicurezza: sono gli analisti che operano in prima linea, quelli con l'incarico di attribuire la giusta priorità agli incidenti e stabilire quali siano gli avvisi che richiedono azione immediata. In una situazione ideale, sono anche in grado di individuare proattivamente eventuali attacchi passati inosservati. Intercept X Advanced with EDR rileva automaticamente le potenziali minacce, attribuendo priorità a ciascuna di esse (opzione disponibile nel 2019). Il Machine Learning aiuta a identificare gli eventi sospetti e ad attribuire loro un punteggio minacce. Gli eventi con i punteggi più elevati vengono automaticamente classificati come eventi di importanza prioritaria. Gli analisti possono così vedere subito quali sono i problemi più impellenti e utilizzare queste informazioni per avviare le indagini.
- Studiosi di malware: a volte le aziende si affidano a esperti di malware specializzati nella decompilazione dei file a scopo di analisi. Questo approccio comporta un inutile dispendio di tempo ed è di dubbia efficacia; inoltre, si basa sul presupposto che siano disponibili livelli di cybersecurity di una sofisticatezza fuori dalla portata della maggior parte delle organizzazioni. Gli studiosi di malware vengono interpellati per capire se un file che non è stato bloccato sia in realtà malevolo. Potrebbero anche analizzare i file identificati come malevoli che risultano essere invece falsi positivi. Intercept X Advanced with EDR offre un approccio migliore all'analisi del malware, grazie all'utilizzo del Machine Learning. Utilizzando il miglior motore di rilevamento antimalware per endpoint disponibile nel settore, la nostra soluzione analizza automaticamente il malware nei minimi dettagli, scomponendo il file per estrarne attributi e codice, e mettendo questi ultimi a confronto con milioni di altri file. Attraverso questa analisi, è possibile vedere immediatamente quali attributi e segmenti di codice del file analizzato sono simili a file "noti per essere innocui" o "noti per essere malevoli" e stabilire se bloccare o autorizzare un file specifico.

- **Esperti di intelligence sulle minacce**: le indagini possono anche essere svolte con dati di intelligence sulle minacce provenienti da terzi, per ottenere (spesso a un costo extra) analisi dettagliate e informazioni di contesto per le minacce rilevate. Gli analisti sono coloro che interpretano e integrano questi dati, per assicurarsi che aggiungano informazioni utili. I dati di intelligence sulle minacce possono essere utilizzati come punto di partenza per le indagini, come base per chiedere alla community di sicurezza un parere su un file sospetto, oppure per stabilire se si stia verificando un attacco mirato ai danni della propria organizzazione. Intercept X Advanced with EDR offre ai responsabili di sicurezza e al personale tecnico la possibilità di raccogliere maggiori informazioni, grazie all'accesso a dati di intelligence sulle minacce disponibili su richiesta, a cura dei SophosLabs. Per garantire la visibilità completa sul panorama delle minacce, ogni giorno i SophosLabs rintracciano e analizzano 400.000 attacchi di malware diversi e precedentemente non conosciuti, alla costante ricerca delle tecniche di attacco più recenti e più efficaci. I SophosLabs procedono quindi alla raccolta, all'aggregazione e al riepilogo di questi dati, per permettere alle aziende che non dispongono di personale specializzato e dedicato esclusivamente all'analisi dei dati di intelligence sulle minacce di affidare questo compito a uno dei migliori team di ricercatori di cybersecurity ed esperti di data science al mondo.

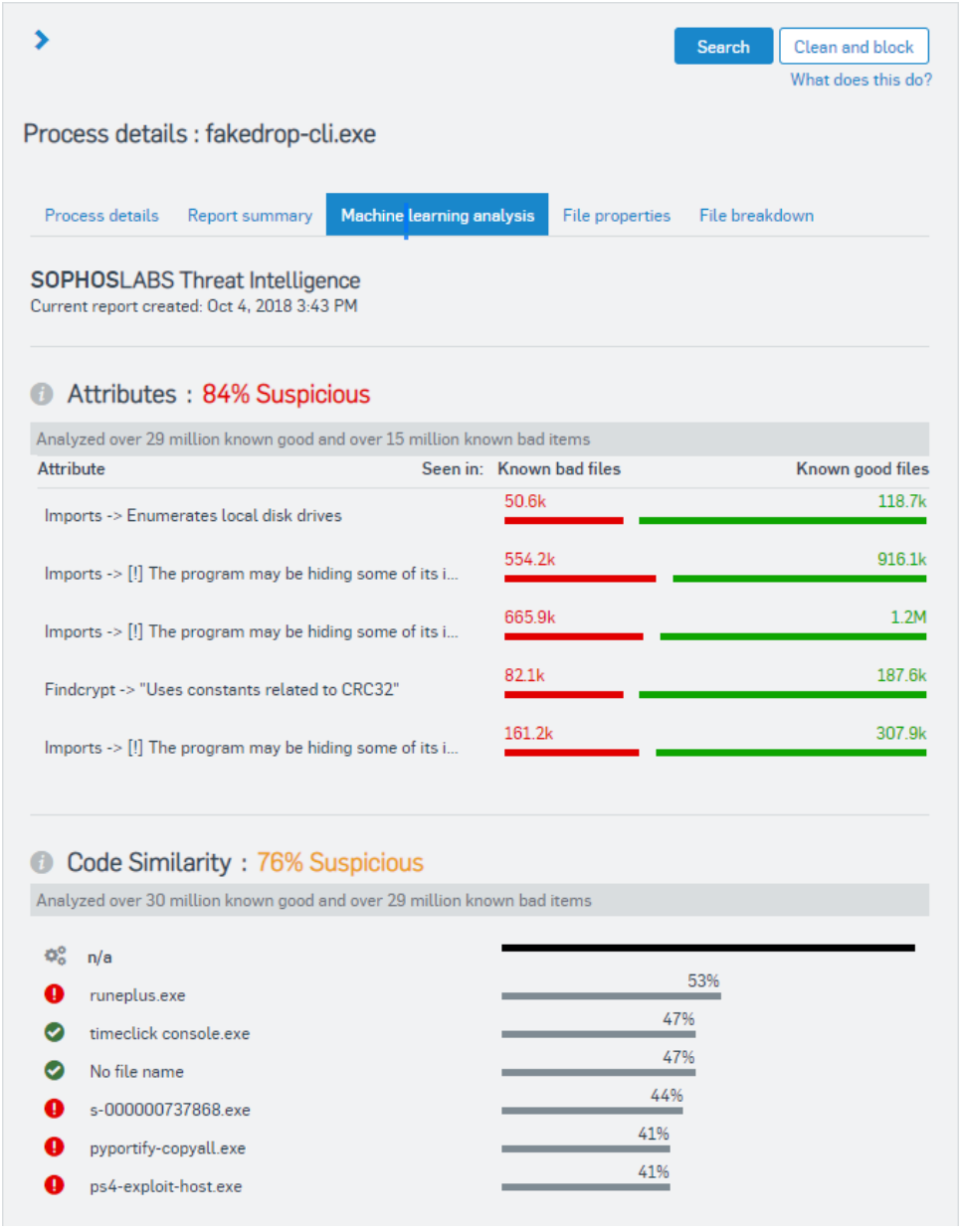

Figura 6: Il Machine Learning consente di visualizzare gli attributi, le somiglianze del codice e i dati sul percorso del file, per un'analisi potente ma semplice da svolgere.

Come scoprire l'origine di un attacco e impedire che si ripeta in futuro

Dopo un attacco, gli esperti di sicurezza hanno un incubo ricorrente: un dirigente che urla "Come è possibile che sia accaduto questo!?" e non poter reagire in altro modo se non facendo spallucce. L'identificazione e la rimozione dei file malevoli risolve il problema più immediato, ma non spiega come questi file siano finiti nei sistemi o cos'altro abbia fatto l'autore dell'attacco prima del rilevamento.

I casi di minacce, un'opzione inclusa in Intercept X Advanced with EDR, mettono in evidenza tutti gli eventi che hanno portato a un rilevamento, semplificando l'identificazione dei file, dei processi e delle chiavi di registro che sono stati colpiti dal malware, per stabilire l'impatto complessivo di un attacco. Offrono una rappresentazione grafica dell'intera catena di attacco, per permettere di compilare report accurati su come abbia avuto origine un attacco e sulle aree colpite dal suo autore. E soprattutto, una volta scoperta la causa originaria di un attacco, i responsabili tecnici hanno maggiori probabilità di impedire che si ripeta.

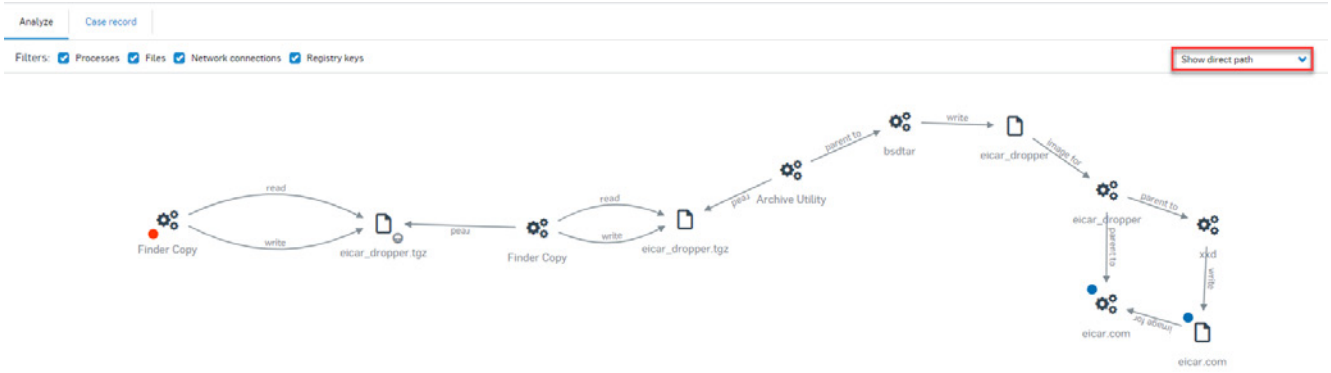

Figura 7: Rappresentazione grafica interattiva della catena di attacco.

Effettuate subito una prova gratuita

Registratevi per ricevere una prova gratuita di 30 giorni su: sophos.it/interceptx

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

14/11/2018 (PC)

SOPHOS