SOPHOS

5 Motivi Per Cui Non Puoi Fare A Meno dell'EDR

Gli strumenti di 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. Sono spesso molto complicate, e presentano diverse lacune di protezione e hanno un impatto eccessivo sulle risorse.

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

Garanzia di integrità delle IT security operation e individuazione proattiva delle minacce più elusive

A seconda dell'organizzazione, IT operation e IT security possono essere gestite dallo stesso team, da dipendenti che appartengono a team diversi o persino da un'unica persona. Indipendentemente da come vengano gestiti, prevedono casi di utilizzo diversi per uno strumento EDR. Tale strumento deve pertanto essere in grado di svolgere le operazioni richieste da questi due ambiti dell'IT e rimanere accessibile senza incidere sulla potenza di elaborazione.

Per gli amministratori delle IT operation, garantire l'integrità della struttura informatica della propria organizzazione è essenziale. Devono, ad esempio, individuare i computer che segnalano problemi di performance quali spazio limitato su disco o utilizzo elevato della memoria, o identificare i dispositivi che eseguono programmi vulnerabili e che richiedono patch. Oppure determinare se sono presenti endpoint e server con RDP, senza che sia indispensabile per lo svolgimento delle mansioni lavorative, o su cui sono abilitati account guest. Sophos EDR offre agli amministratori gli strumenti necessari per formulare queste domande e molte altre ancora. Inoltre, garantisce accesso remoto ai dispositivi, permettendo così di risolvere eventuali lacune di sicurezza, grazie alle opzioni di indagine sulla performance, alla possibilità di installare patch e alla capacità di disattivare RDP e account guest.

Gli specialisti della cybersecurity devono essere in grado di individuare proattivamente anche le minacce più velate ed elusive, che non vengono automaticamente bloccate dal sistema di protezione endpoint. Lo strumento EDR di cui hanno bisogno deve essere efficace nell'identificare indicatori di compromissione (Indicator of Compromise, IoC) quali: processi che effettuano tentativi di connessione a porte non standard, processi che hanno modificato file o chiavi di registro, oppure processi che si camuffano da elementi diversi. Inoltre, lo strumento deve essere in grado di risalire ai dipendenti che hanno cliccato su un link malevolo in un'e-mail di phishing. Sophos EDR rende ancora più facile e rapido lo svolgimento di questi tipi di indagine all'interno della struttura informatica di un'organizzazione. Una volta terminate le indagini, permette poi con altrettanta semplicità di accedere da remoto al dispositivo interessato per effettuare ulteriori approfondimenti, per implementare strumenti di analisi dettagliata e per interrompere eventuali processi sospetti.

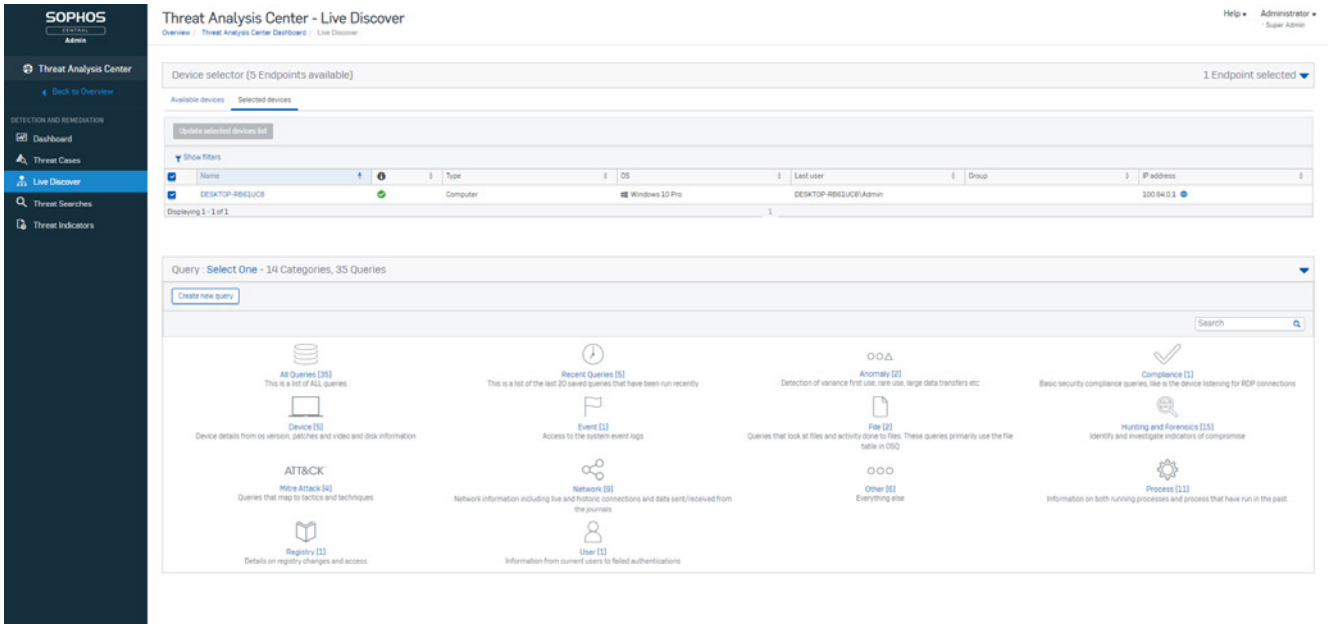

Figura 1: Sophos Intercept X with EDR permette agli utenti di formulare domande dettagliate sull'intera struttura informatica

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 il 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 cyberminacce vengono attivate in seguito a una notifica di intelligence su un possibile attacco 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 un'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.

La funzionalità "The Threat Indicators" in Intercept X offre un elenco dei principali eventi sospetti, fornendo agli analisti un'indicazione specifica sul tipo di analisi da condurre. 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.

Avendo un punto di partenza specifico, gli analisti possono quindi identificare tutte le istanze di un elemento sospetto presenti nell'intera struttura informatica, per poi intraprendere rapidamente azioni correttive volte alla rimozione degli elementi pericolosi. Inoltre, possono anche usufruire delle potenti query SQL per rintracciare altri indicatori di compromissione, quali ad esempio processi che modificano le chiavi di registro e processi che effettuano tentativi di connessione su porte non standard.

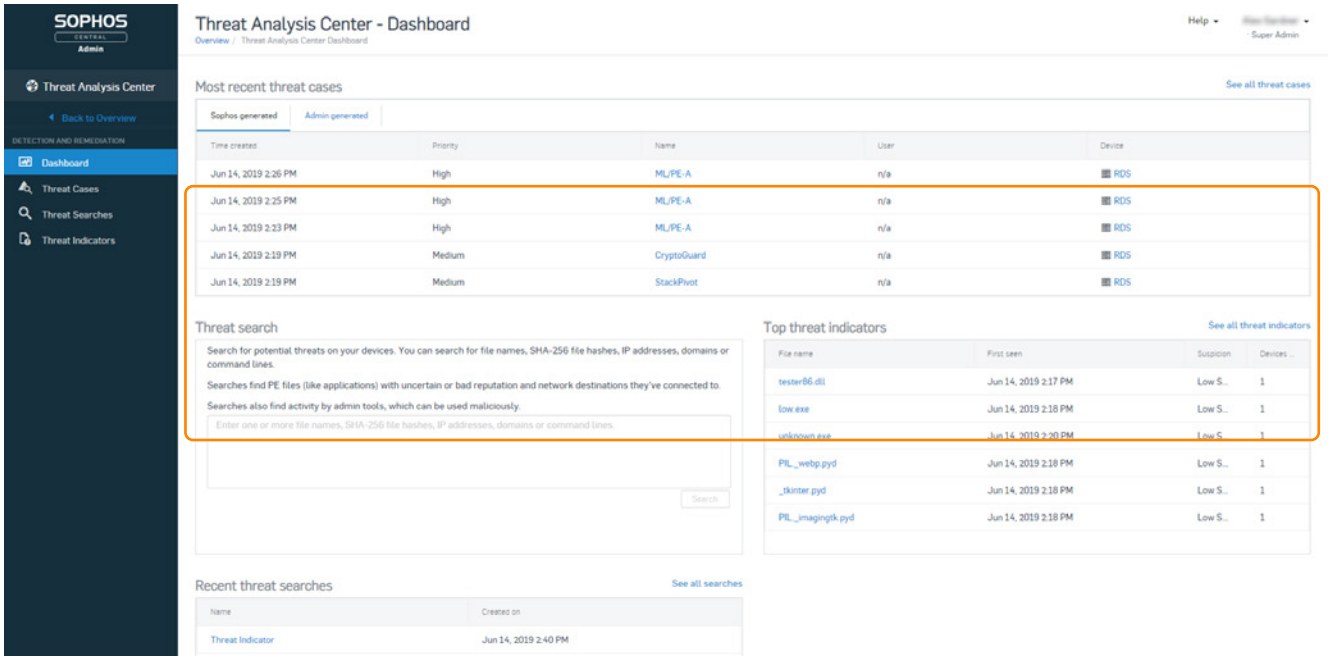

Figura 2: Sophos Intercept X with EDR offre la possibilità di cercare indicatori di compromissione all'interno della rete. Inoltre, utilizza il machine learning per determinare i principali eventi sospetti su cui indagare

La potente combinazione tra la formulazione di domande dettagliate e i consigli pratici su dove cominciare le indagini, unita a dati di intelligence sulle minacce gestiti da esperti, risulta utile sotto diversi punti di vista: Sophos EDR è infatti una soluzione semplicissima da usare, che non costringe gli amministratori a scendere a compromessi in termini di potenza di elaborazione o livello di dettaglio.

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 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 vengano effettuate. 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 formulare le giuste domande e di interpretare le risposte in maniera corretta. Ma con Intercept X with EDR, i team di sicurezza, indipendentemente dal livello di preparazione, possono rispondere rapidamente agli incidenti di sicurezza, grazie alle indagini guidate che offrono consigli sulle azioni da intraprendere, con dati integrati e rappresentazioni visive dell'attacco.

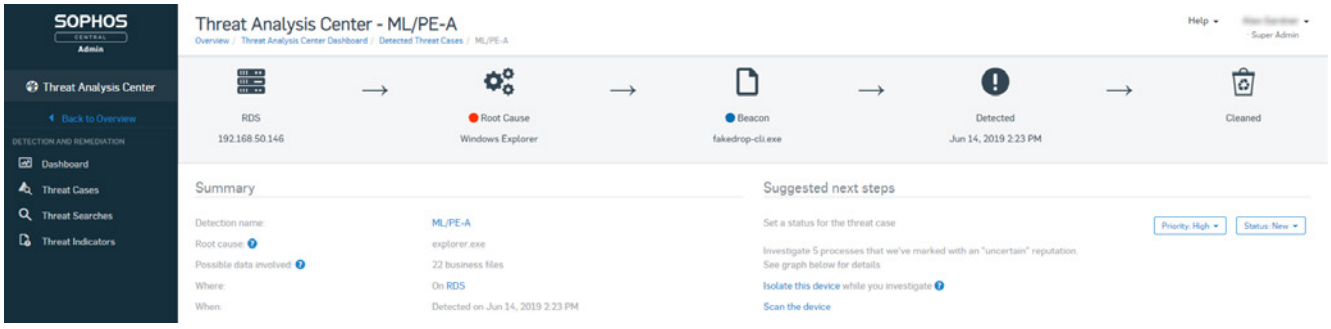

Figura 3: La risposta guidata agli incidenti offre le opzioni "Azioni successive consigliate" e "Isolamento endpoint" su richiesta per la risoluzione rapida e sicura degli incidenti.

Sophos EDR include anche opzioni di accesso remoto ai dispositivi mediante interfaccia della riga di comando. È la soluzione ideale per una risposta rapida, anche quando il dipendente non si trova fisicamente in ufficio. Non appena effettuato l'accesso al dispositivo, gli amministratori possono svolgere ulteriori indagini implementando strumenti di analisi dettagliata, installando o disinstallando software, terminando processi e riavviando il dispositivo.

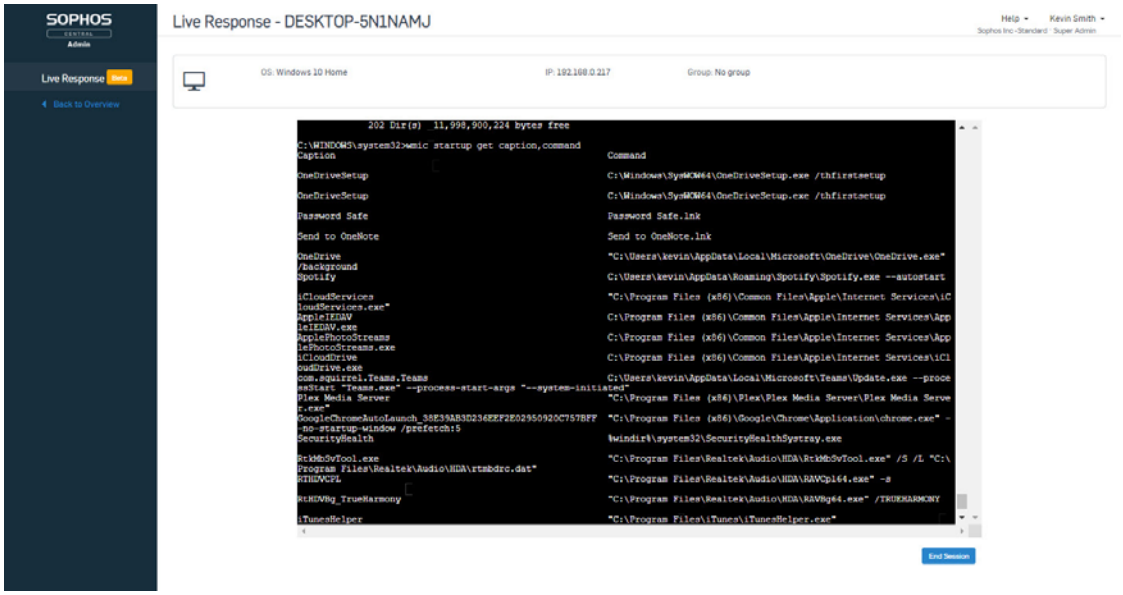

Figura 4: Intercept X with EDR include diversi pulsanti di azione, che offrono moltissime opzioni di correzione rapida, la più comune è chiamata "Clean and Block".

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

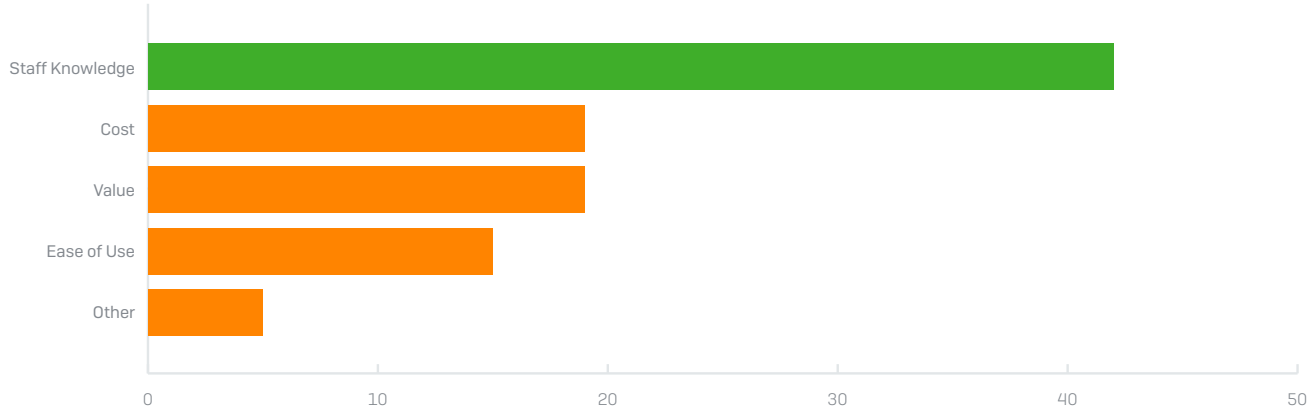

Figura 5: La mancanza di dipendenti con adeguate competenze tecniche è il motivo maggiormente citato dalle organizzazioni che non hanno adottato una soluzione di rilevamento e risposta alle minacce endpoint (Endpoint Detection and Response, EDR). (Fonte: Studio di Sapio in collaborazione con Sophos,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

Per sopperire alla mancanza di competenze adeguate, Intercept X 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 with EDR rileva automaticamente le potenziali minacce, attribuendo priorità a ciascuna di esse. 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.
- Analisti di malware: a volte le aziende si affidano a esperti di malware specializzati nel reverse engineering 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 molto sofisticati, 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 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 terze parti, 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 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 e gestiti dai SophosLabs. Per garantire visibilità completa sul panorama delle minacce, ogni giorno i SophosLabs rintracciano e analizzano 400.000 attacchi di malware diversi e mai visti prima, 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.

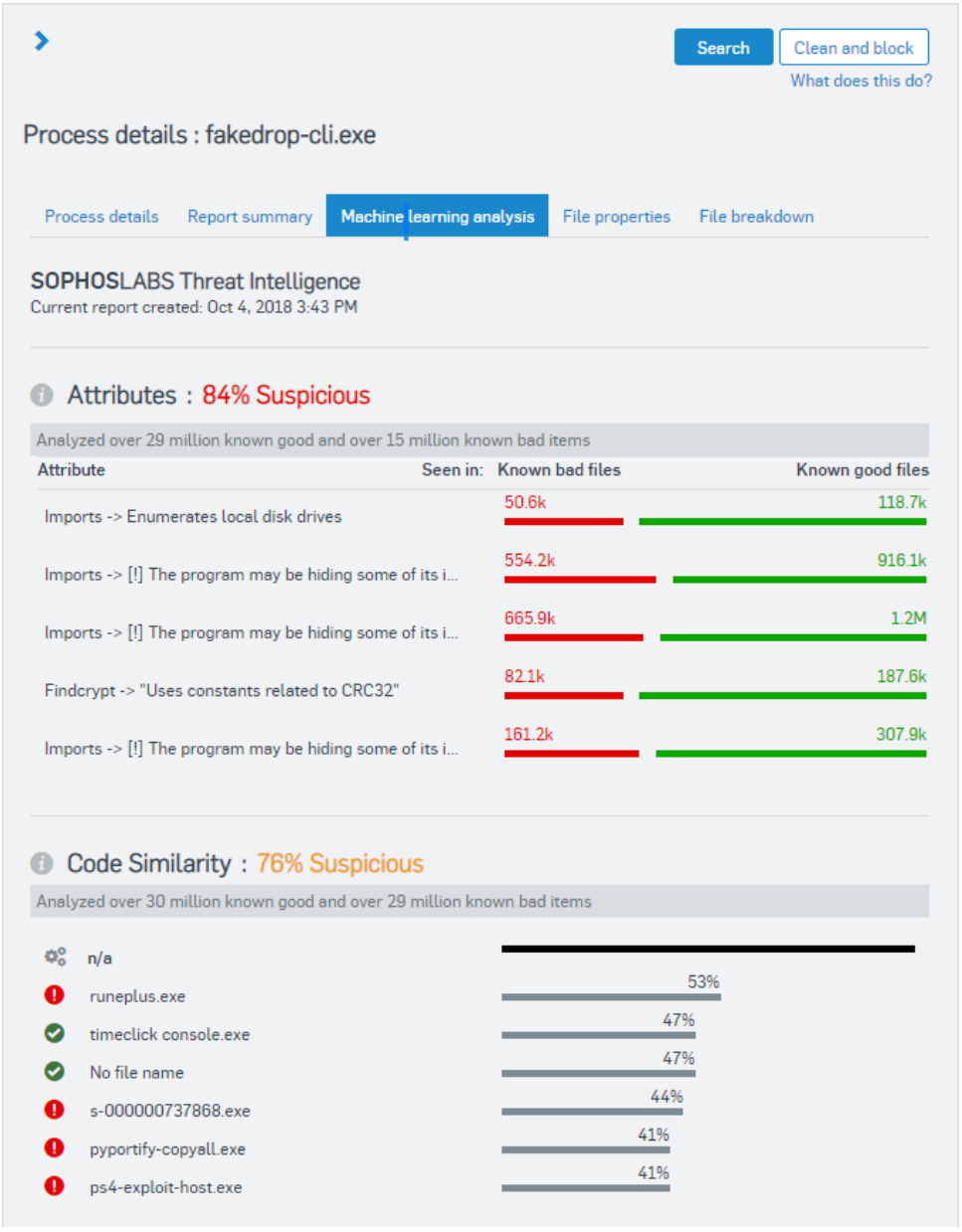

Figura 6: Il Machine Learning consente di visualizzare gli attributi, le somiglianze del codice e i dati sul percorso del file, per un'analisi potente ma semplice da svolgere.

Managed Threat Response (MTR)

Avete bisogno di aiuto per gestire l'EDR? Sophos MTR è un servizio che unisce le nostre tecnologie alle analisi a cura di esperti, per ottimizzare le attività di threat hunting, per indagare con maggiore profondità sugli avvisi e per intraprendere azioni mirate in risposta alle minacce.

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, cioè un dirigente che urla "come è possibile che sia accaduto questo!?" e non possono reagire in nessun 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 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.

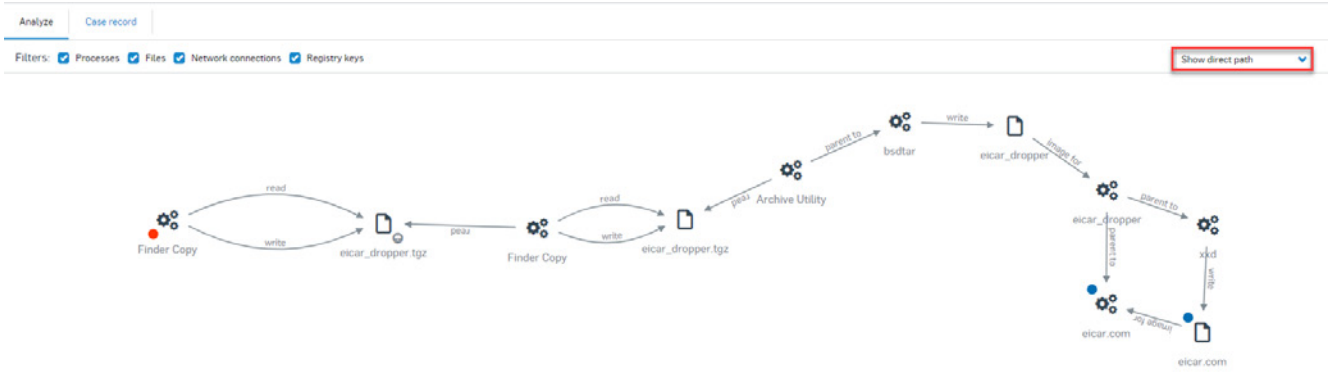

Figura 7: Rappresentazione grafica interattiva della catena di attacco.

Visibilità sull'intero ambiente di cybersecurity

Sophos offre sia EDR che XDR (Extended Detection and Response, rilevamento e risposta estesi), per una visibilità che non ha eguali su endpoint e server, nonché sui dati relativi alla rete e alla posta elettronica. Queste funzionalità permettono di passare rapidamente da una prospettiva olistica (ovvero un quadro completo) dell'ambiente ai dettagli granulari in ambiti di interesse specifici. Ma non è tutto: si vanno a sommare alla nostra protezione leader di settore, in grado di bloccare le minacce più recenti, come ad esempio il ransomware, le tecniche di exploit e gli hacker.

Per saperne di più e per iniziare una prova gratuita, visitare: sophos.it/intercept-x

Effettuate subito una prova gratuita

Registratevi per ricevere una prova gratuita di 30 giorni su: sophos.it/intercept-x

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

19/04/2021 (MP)

SOPHOS