SOPHOS
Cybersecurity made simple.

您需要 EDR 的五大原因

Endpoint Detection and Response (EDR) 工具專為提升偵測、調查與回應能力，進而補強端點安全而設計。但是，過度吹捧 EDR 工具，反而讓我們難以理解其確切使用方式以及需要這些工具的原因。更糟的是，許多組織內現有的 EDR 解決方案往往無法提供價值，因為這些解決方案難以使用、缺乏足夠的保護能力，而且佔用非常多資源。

現在Sophos Intercept X Advanced with EDR 將智慧型 EDR 與業界頂級的端點保護整合在單一解決方案中，使其成為組織解決安全事件難題最簡單的方式。以下是考量 EDR 解決方案時的一些其他原因。

在任何特定時刻都能自信地回應安全狀況

IT 和安全團隊通常仰賴攻擊和防禦指標，但大多數團隊最難回答的問題是「我們現在安全嗎？」這是因為大多數網路都有相當大的盲點，導致 IT 和安全團隊很難看清環境中發生的狀況。

缺乏可見度是組織無法掌握攻擊範圍和影響的主要原因。當事件發生，團隊因為偵測到該事件就假設自己安全無虞時，往往就會陷入此一盲點。Intercept X Advanced with EDR 可提供確認其他電腦是否受到影響的其他深入資訊。例如，如果網路上發現了一個可疑的可執行檔，就會加以修復。但是，分析人員不見得知道環境中其他位置是否還有該可執行檔。有了 Intercept X Advanced with EDR，則可立即獲得這項資訊。能夠檢視存在於其他位置的威脅，讓安全團隊可排定事件的優先順序，以進行其他調查和可能的修復。

清楚地檢視組織的安全狀況，還可以提供有能力回報合規性狀態的優勢。這項資訊將有助於找出容易受到攻擊的區域。該資訊也可讓系統管理員判斷攻擊範圍是否已經影響敏感資料所在的區域。例如，如果偵測到從網路竊取資料的惡意軟體，分析人員必須判斷受影響的電腦是否包含受 HIPAA (美國健康保險流通與責任法案) 約束的醫療資訊。使用 Intercept X Advanced with EDR，能更容易地達成這個目的。此外，由於端點能見度提高，也可以更容易地證明患者資訊受到保護，獲得額外的合規性優勢。

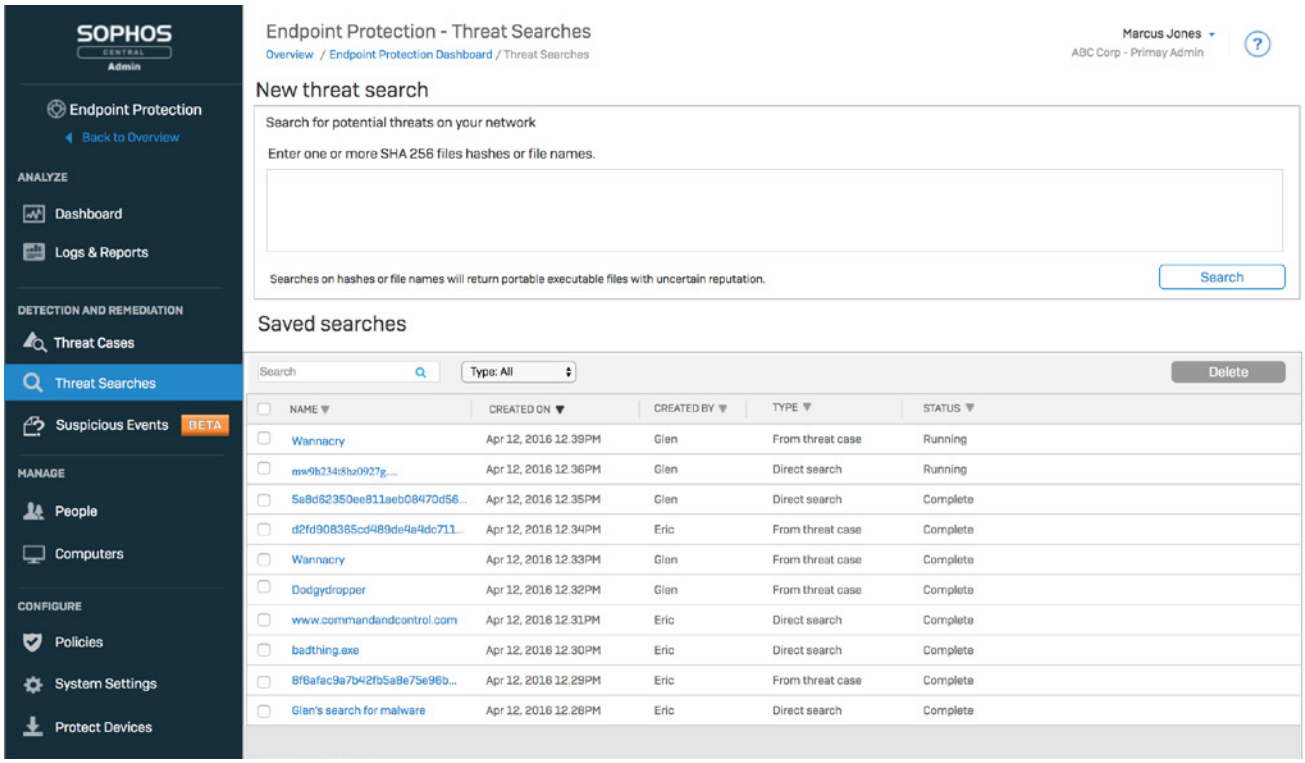

圖 1：Sophos Intercept X Advanced with EDR 會顯示威脅存在的所有其他位置

偵測被忽視的攻擊

在網路安全領域，即使是最先進的工具也可能在時間和資源充足的情況下被擊敗，因此很難真正了解攻擊發生的時間。組織通常僅依靠預防來保護，但雖然預防至關重要，EDR 可提供另一層偵測功能，可能會發現過去沒有發現的事件。

組織可以利用 EDR 搜尋遭駭指標 (IOC)，藉此偵測攻擊。這是尋找可能錯過的攻擊快速而直接的方法。威脅搜尋通常會在收到第三方威脅情報通知後啟動：例如政府機構 (如 US-CERT、CERT-UK 或 CERT Australia) 可能會通知組織其網路中存在可疑活動。此通知可能會隨附 IOC 清單，可以當成判斷發生什麼事件的依據。

Sophos Intercept X Advanced with EDR 會提供一份常見的可疑事件清單，因此分析人員能夠確切知道他們應該調查的內容 (將於 2019 年推出)。透過 SophosLabs 機器學習功能，可以顯示常見的可疑事件清單，並根據其威脅評分進行排名。藉此分析人員可以輕鬆排定工作負載的優先順序，並專注在最重要的事件。

發現可疑事件時，還會突出一個通用場景，讓分析人員確定內容是否真正是惡意的。這個動作適用於沒有足夠的惡意行為可以自動定罪，但仍需深入了解的活動。被判定為「灰色地帶」的事件，需要進行額外分析才能確認其為惡意、良性還是不需要的。

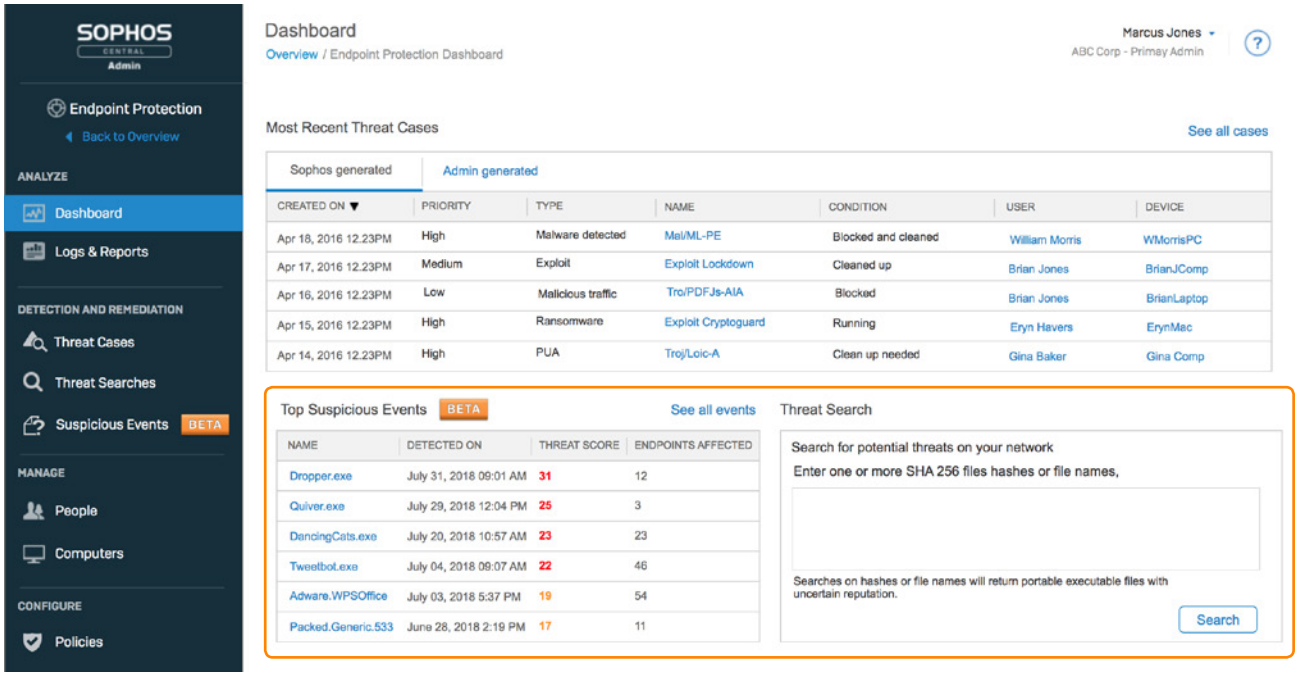

圖 2：Sophos Intercept X Advanced with EDR 能夠搜尋網路上的遭駭指標。它還會利用機器學習來判斷應該調查的主要可疑事件 (可疑事件功能即將在 2019 年推出)

對於潛在事件的回應更快

一旦偵測到事件之後，IT 和安全團隊通常會競相進行修復，以盡快降低攻擊擴散的風險，並控制任何潛在的損害。當然，最重要的問題是如何擺脫每個自身面對的威脅。平均而言，安全和 IT 團隊花費超過三個小時來嘗試修復每個事件。EDR 可以顯著加快速度。

分析人員在回應事件時，可能採取的第一個步驟是阻止攻擊擴散。Intercept X Advanced with EDR 可根據需要隔離端點，這是阻止威脅在整個環境中擴散的關鍵步驟。分析人員通常會在調查之前就完成這個步驟，以便在確定最佳行動方案的同時爭取時間。

調查可能是一個緩慢而痛苦的過程。當然這是假設一直在進行調查。過去，事件回應非常需要依賴技術高超的分析人員。大多數的 EDR 工具也非常仰賴分析人員來了解要詢問的問題以及如何解譯答案。但是，利用 Intercept X Advanced with EDR，所有技術等級的安全團隊都可以經由後續步驟建議、一目瞭然的視覺攻擊表示，以及內建專業知識的引導式調查，快速回應安全事件。

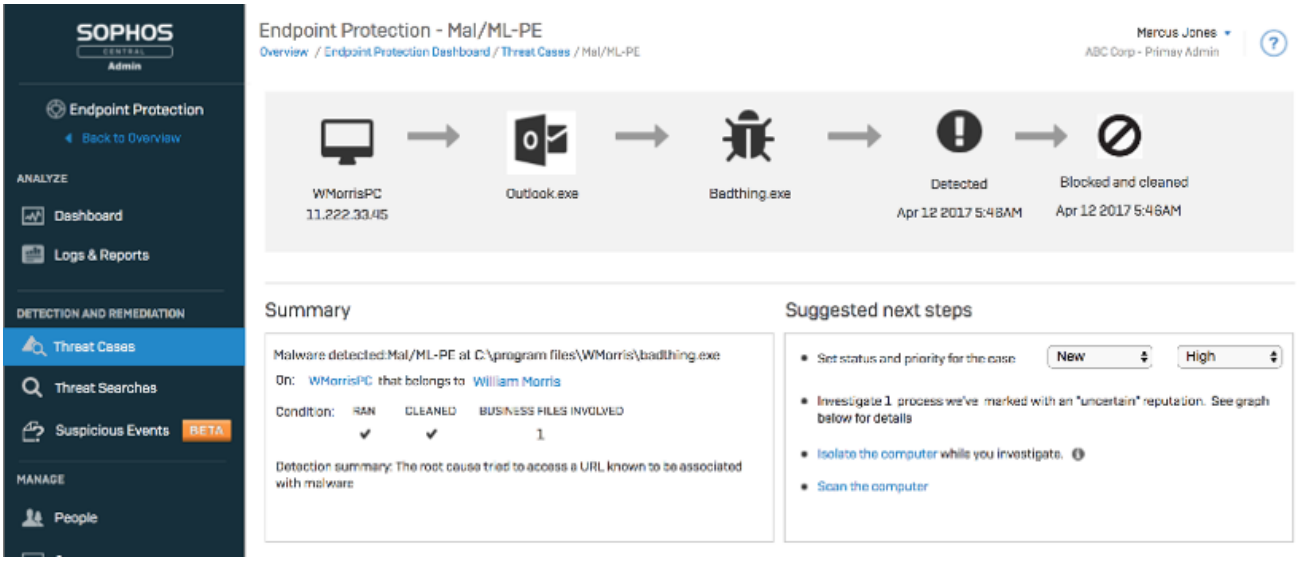

圖 3：引導式事件回應提供建議的後續步驟，並可依需要隔離端點，以快速並安全地解決事件。

調查結束後，分析人員只需要按一下按鈕即可進行回應。快速回應選項包括隔離需要立即修正的端點、清除並阻擋檔案，以及建立鑑識快照。此外，如果檔案被誤擋，也可以輕鬆回復。

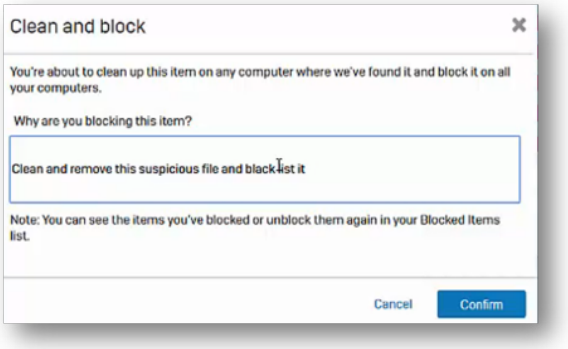

圖 4：Intercept X Advanced with EDR 中有許多動作按鈕，可提供多個修復選項，包含最常使用的「清除並阻擋」。

增加專業知識，但無須增加員工

組織大多希望增加端點偵測和回應功能，並認為「員工知識」是採用 EDR 的最大障礙。這不令人意外，因為合格網路安全專業人員的人才缺口已經被廣泛討論了好幾年。這種障礙對於較小的組織尤其明顯。

組織尚未實作 EDR 的常見原因

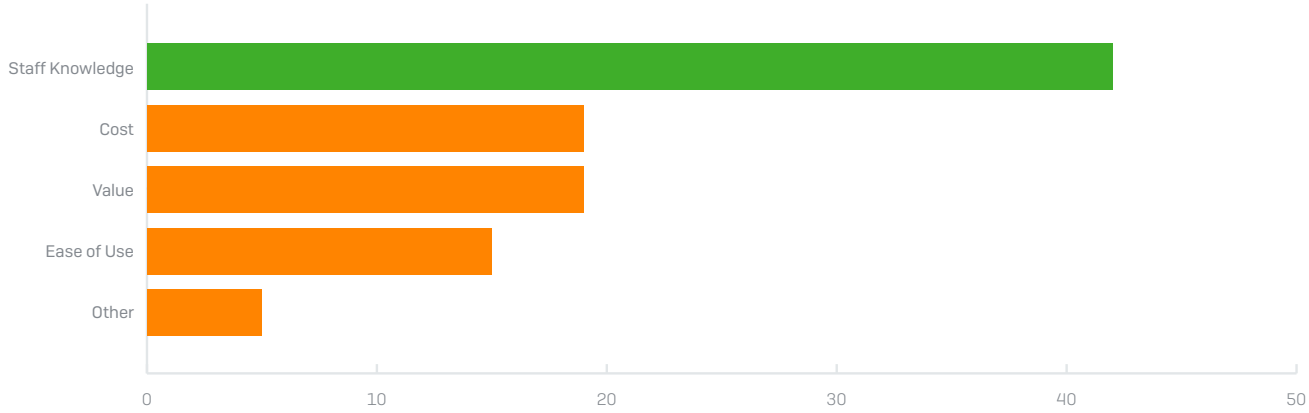

圖 5：「員工知識」被列為組織尚未採用 Endpoint Detection and Response (EDR) 解決方案的常見原因 (資料來源：Sapio 和 Sophos 共同進行的研究，2018 年 10 月)

為解決員工知識差距，Intercept X Advanced with EDR 提供了與專精分析人員同等的功能。它利用機器學習來整合深度安全洞察力，並透過精選的 SophosLabs 威脅情報加以強化，因此您無需增加員工即可增加專業知識。智慧型 EDR 功能有助於彌補缺乏員工知識而導致的差距，提供了數種分析人員的功能：

- **安全分析人員**：這一線的分析人員，負責對事件進行分類並確定需要立即處理的警示。理想情況下，他們還能夠主動尋找並偵測可能未被注意到的任何攻擊。Intercept X Advanced with EDR 會自動偵測潛在威脅並排定其優先順序 (即將在 2019 年推出)。使用機器學習可以識別可疑事件並為威脅評分。評分最高的事件是最重要的事件。分析人員可以很快看到需要注意之處，並開始調查。
- **惡意軟體分析人員**：組織可能會透過專門針對可疑檔案進行反向工程的惡意軟體專家來進行分析。這種方法不僅耗時且難以實現，還假設大多數組織的網路安全不複雜。您需要惡意軟體分析人員來確定未受阻擋的檔案實際上是否是惡意的。他們也會檢視遭到判定有問題但實際上可能是誤報的檔案。而Intercept X Advanced with EDR 利用機器學習能提供更好的惡意軟體分析方法。其使用業界最佳的端點惡意軟體偵測引擎，能自動詳細分析惡意軟體、分解檔案屬性和程式碼元件，並將其與數百萬個其他檔案進行比較。分析人員可以輕鬆察看與「已知良好」和「已知不良」檔案類似的屬性與程式碼區段，以判斷應該阻擋還是加以放行。

- **威脅情報分析人員**：進行調查時，可能需要仰賴第三方威脅情報 (通常需要額外付費) 來取得額外的威脅深入資訊和背景。分析人員必須解釋並整合這項資料，才能確保它可以帶來效益。威脅情報可以當做調查的起點、向安全社群詢問對可疑檔案看法的方式，或是確定攻擊是否針對組織的參考。Intercept X Advanced with EDR 可以讓 IT 和安全管理員存取 SophosLabs 精選的隨需威脅情報，使他們能夠搜尋更多資訊。為了保持對威脅狀況的全面了解，SophosLabs 每天追蹤、解構並分析 400,000 個獨特且以前從未見過的惡意軟體攻擊，藉此不斷搜尋最新和最強大的攻擊技術。這項威脅情報經過收集、彙整並加以總結，可以輕鬆地進行分析，因此即使是缺少專屬威脅情報分析人員，或是使用昂貴且難以理解的威脅摘要的團隊，均可以從這個全球頂尖的網路安全研究和資料科學團隊受益。

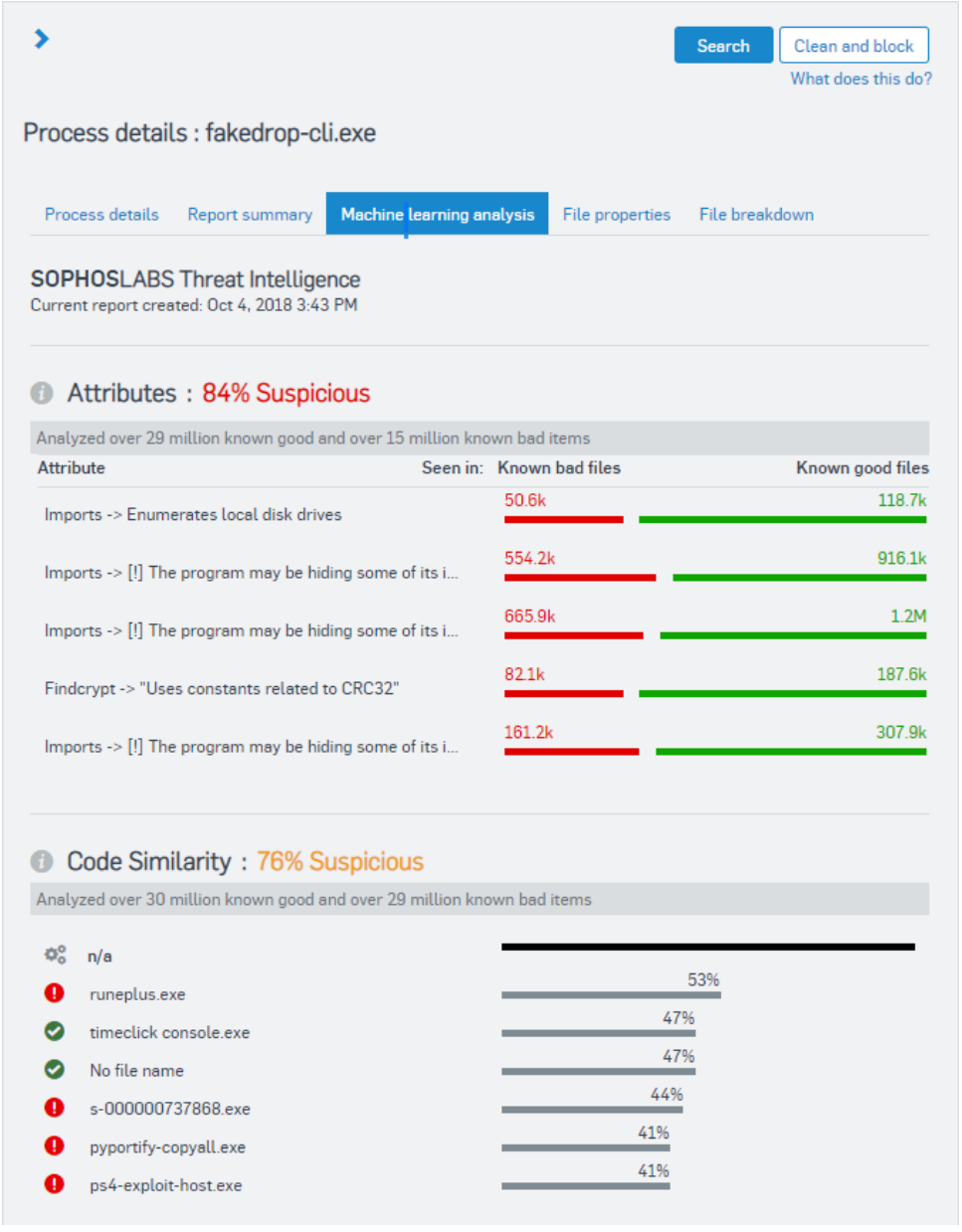

圖 6：機器學習分析會顯示屬性、程式碼相似性以及檔案路徑分析，以進行強大而簡單的分析。

了解攻擊發生的方式，以及如何阻止攻擊再次發生

遭受攻擊後，安全分析人員最常遇到的惡夢就是：一位高級主管高喊：「這是怎麼發生的？！」，而他們所能做的就是聳聳肩。找出並移除惡意檔案可以解決當前的問題，但是並無法了解它是如何在第一時間完成這項工作，或者攻擊者在攻擊結束之前做了什麼。

Intercept X Advanced with EDR 中隨附的威脅案例會鎖定觸發偵測的所有事件，使人易於了解惡意軟體影響哪些檔案、處理程序和登錄機碼，以確定攻擊的影響範圍。它可以透過視覺方式呈現整個攻擊鏈，進而確保攻擊發動方式以及攻擊者動向的可靠報告。更重要的是，了解攻擊的根本原因之後，IT 團隊將更有機會阻止它再次發生。

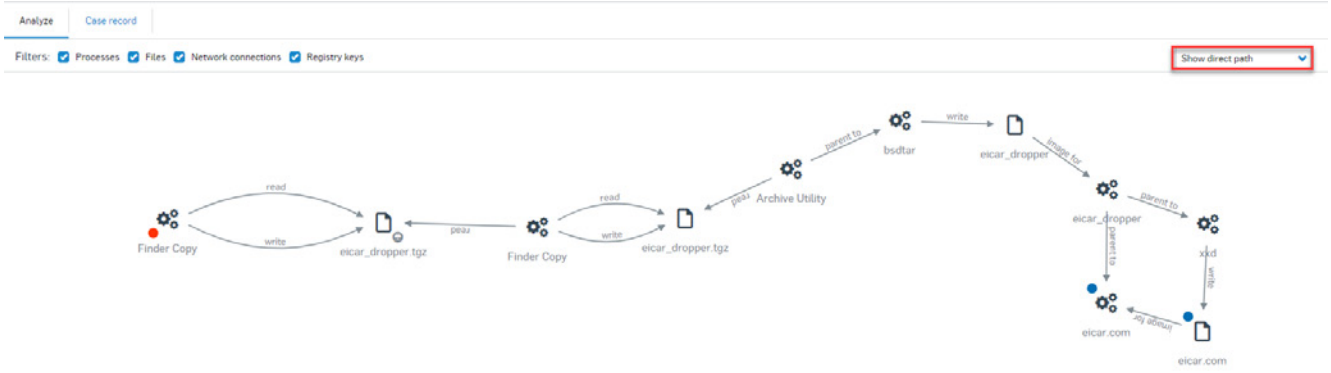

圖 7：威脅案例可以透過視覺和互動的方式呈現攻擊鏈。

立即免費試用

取得 30 天免費試用版本：
www.sophos.com/interceptx

台灣業務窗口
電話：+886 2 7709 1980
電子郵件：Sales.Taiwan@Sophos.com

2018/11/14 (PC)

SOPHOS