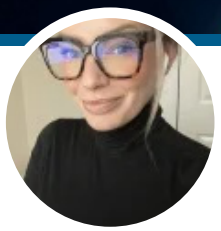
5 大 EDR 使用案例

2024 年 5 月 22 日發布｜產品洞察



阿麗莎·史密斯
博通企業安全部門
產品行銷負責人

當防禦措施失敗時，這五項行動準則可以拯救您

攻擊者行動越來越隱密，他們的攻擊方法不斷演進，甚至可以避開更進階的預防性網路安全防禦。本部落格提供端點偵測與回應 (EDR) 可協助您識別並阻止複雜攻擊的使用範例。

什麼是端點偵測與回應 (EDR) ？

端點偵測與回應 (EDR) 是整合式端點安全解決方案，結合即時持續監控與端點資料收集，和以規則為基礎的自動回應與分析功能。

EDR 在傳統防毒、甚至下一代防毒 (NGAV) 保護之後提供第二道防線，由於攻擊者使用進階技術避開第一道防線，因此越來越需要第二道防線。EDR 可讓安全團隊迅速偵測進階攻擊並作出回應，找出攻擊者滲透環境的方式，並 (與 NGAV 或其他解決方案一起部署時) 設定政策以防止未來發生類似的攻擊。

端點之所以受到攻擊，大部分原因在於『人』的因素，因為使用者很容易受到社交工程、網路釣魚和其他利用忙碌、分心對使用者進行攻擊。(事實上，入侵事件中人為因素統計約 74% 扮演重要角色)。端點本身的漏洞，包括過時的軟體和作業系統，也讓組織更容易受到攻擊。

EDR 可作為安全網來防禦所有這些威脅，幫助您捕捉被端點防護漏過的威脅，並讓您能迅速有效地作出回應。

EDR 實例：安全團隊的進階行動

EDR 解決方案可讓安全團隊進行進階的偵測與回應活動，如果沒有 EDR 的協助，這些活動會變得困難、費時且雜亂無章。EDR 範例以及 EDR 可實現的進階功能包括事件回應、遠端修復、警示分類／可視化、威脅獵捕以及鑑識調查。

事件回應

對偵測到的網路安全事件迅速且有信心地作出回應的功能，結果有可能會對業務造成極小的干擾，也可能會造成災難性的損害。適當的事件回應 (IR) 策略和戰術對於限制攻擊的爆雷影響範圍至關重要。根據《2023 年資料外洩成本報告》(Cost of a Data Breach Report 2023)，要更快地識別和應對資料外洩，最有效的 IR 策略是成立 IR 團隊，並在執行 IR 計畫前進階行測試。根據該報告，這樣做可以將識別資料外洩所需的時間縮短 54 天。

有效的 IR 計劃和程序固然重要，但擁有正確的資訊以採取行動也同樣重要--這意味著您的安全堆疊中要有正確的元件。這就是 EDR 解決方案的用武之地。在比較 EDR 解決方案時，請尋找能夠持續記錄和儲存端點活動資料的解決方案。這將為您的 IR 團隊提供端點活動記錄系統，以追蹤已識別威脅的證據並偵測行為模式。進階 EDR 可提供 IR 團隊有效執行工作所需的能見度與情境--傳統防毒軟體甚至許多端點防護解決方案根本無法提供可行的洞察力。EDR 供應商應透過各種模式提供 EDR 保護，從內部建置到混合環境與管理服務。

遠端修復

我們在前面提到，一旦偵測到威脅，迅速果斷地採取行動是非常重要。在安全和 SOC 團隊成員從多個地點 (包括家庭辦公室) 工作的時代，這可能是一項挑戰。請詢問 EDR 供應商，他們的解決方案是否允許您的團隊從世界上任何地點安全、快速地執行全面調查和修復。

進階的解決方案會利用雲端原生架構，例如：提供管理員一個遠端 shell，讓他們可以直接看到整個企業的每個端點，這是團隊需要儘快對受感染主機作出回應的關鍵能力。

警示分類／可視化

詢問任何 SOC 團隊成員，他們都會證實：警示倦怠是真實存在。對抗警示倦怠最重要的功能之一，就是讓分析師能夠分類警示的可視化功能。有了正確的工具，分析師可以快速輕鬆地了解並消化攻擊順序中發生的事情。這有助於設定政策，防止類似的攻擊再次發生。

探索每家 EDR 供應商提供的警示可視化功能是個好主意。尋找能夠直觀呈現與警示相關所有事件的解決方案。您應該可以選擇個別程序或事件，以查看其信譽、TTP (戰術、技術與程序)、使用的命令列及其他資訊。可視化應提供警示期間所發生事件的可執行資訊，包括應用預防的位置、來源，以及攻擊者可能嘗試的行動。應該滿足這些要求。

威脅獵捕

威脅獵捕對於業界而言並非新事物，但對於許多安全團隊，尤其是那些剛開始使用 EDR 的團隊而言，絕對是個新概念。威脅獵捕是在公共和私有雲伺服器、端點和網路中追蹤入侵指標 (IOC)。這些 IOC 可能是入侵或資料外洩的訊號。

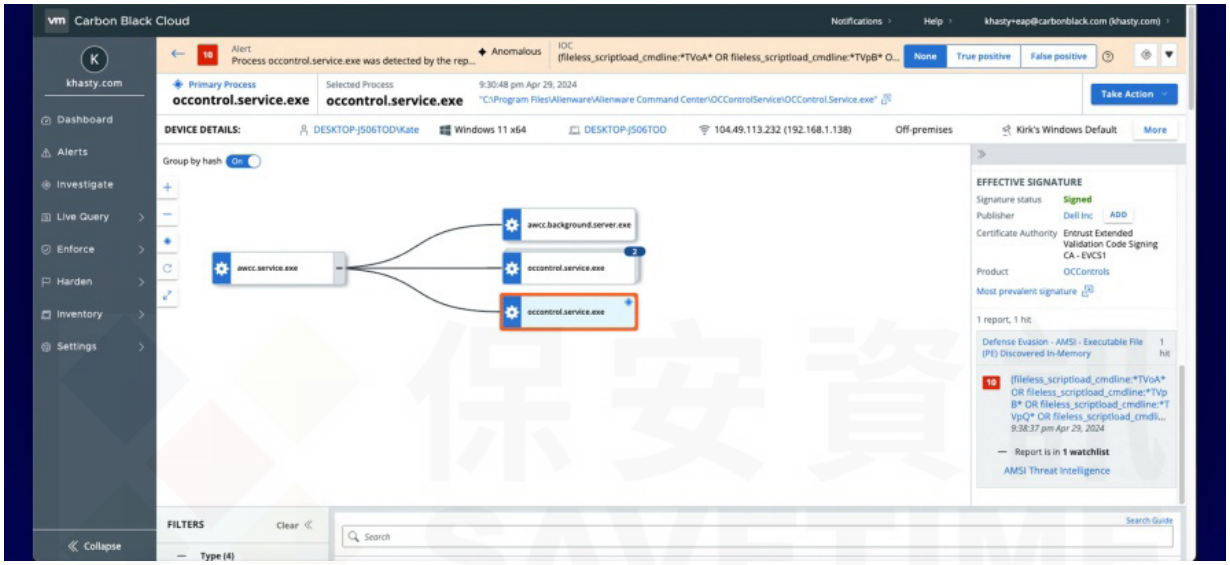
威脅獵捕與事件回應不同，因為威脅獵捕是主動性，而事件回應是被動性。不過，這兩種角色是相輔相成。事實上，許多安全團隊會指派員工負責威脅獵捕的任務；這些員工通常也都是成功的事件回應者，他們的經驗有助於他們準確判斷攻擊者行為方式，以及他們下一步可能採取的行動。

為了簡化威脅獵捕程序並確保其有效性，請尋找能收集全面資料和廣泛威脅情報的解決方案，讓您能獲得所需的所有資訊，以主動獵捕威脅、發現可疑行為、瓦解進行中的攻擊、快速修復損害、管理弱點並處理防禦漏洞。優異的解決方案可讓您搜尋未篩選的原始端點資料，即使端點已離線也沒問題。透過建立自動化的觀察清單，您應該可以在大型企業中擴展您的追捕行動，而且絕不會追捕相同的威脅兩次。

鑑識調查

準確指出入侵是如何發生，包括識別 TTP 和瞭解攻擊者的路徑，對於防止未來發生類似的攻擊是至關重要。這就是廣泛可視性的來源：鑑定調查員能存取的資料越多，他們的分析就越徹底。

您的 EDR 解決方案應該能夠將整個攻擊鏈視覺化。這可讓您更容易找出事件的根本原因。分析師也應該能夠快速逐層分析攻擊的每個階段，以深入瞭解攻擊者的行為、縮小安全漏洞，並從每個新穎的攻擊技巧中學習。



攻擊可視化的範例，這是 Carbon Black EDR 所啟用的鑑識調查用例的一部分。

Carbon Black EDR：進階威脅需要進階的防禦系統

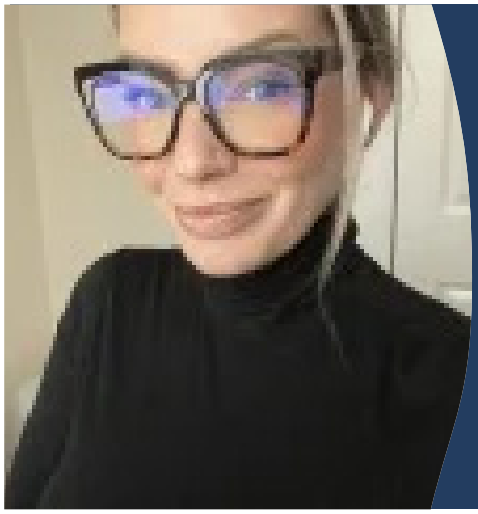
威脅發展得如此迅速，您很可能正在考慮部署 EDR--如果不是現在，也會很快。上述例子都是您在 EDR 平台上做出策略性選擇的論據。對越來越多的組織而言，這個選擇就是備受好評的 EDR 解決方案『Carbon Black』，Carbon Black 是 EDR 的先驅，現在是 Broadcom 企業安全集團解決方案組合的一部分。

Carbon Black EDR 為安全團隊提供全面且整合的方法，偵測進階的攻擊並作出回應。您可立即存取最完整的攻擊畫面，將冗長的調查時間從數天縮短到數分鐘，這是分秒必爭的重要優勢。安全團隊可以主動尋找威脅、發現可疑行為、瓦解主動攻擊，並搶在攻擊者之前解決防禦漏洞。

Carbon Black EDR 強大支援本文所討論的每個使用案例--從事件回應、遠端修復和警示視覺化，到威脅獵捕和鑑識調查。事實上，Carbon Black EDR 提供所有端點可視性和情境化資訊 (包括歸因、威脅者的詳細資訊和其他攻擊資訊)，以便快速回應以限制損害和阻止橫向移動。Carbon Black EDR 旨在追蹤攻擊者，讓他們無處遁形。

親自瞭解 Carbon Black EDR 如何為您提供下一道防線。立即聯絡我們安排示範。

原廠網址：https://www.security.com/product-insights/5-top-edr-uses-cases
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2024/5



關於作者

阿麗莎・史密斯 (Alisha Smith)

博通企業安全部門產品行銷負責人

阿麗莎・史密斯 (Alisha Smith) 是博通企業安全部門產品行銷負責人，該部門負責提供賽門鐵克和 Carbon Black 的網路安全解決方案。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。