

消弭盲點、強化您的 SOC： Symantec[®] Threat Hunter 洞察分析

目錄

概覽

前言

重新思考入侵偵測：Symantec Threat Hunter

資安維運中心(SOC)所面臨的挑戰

Threat Hunter 分析能力

協作力量帶來了快速且有效的應變

Threat Hunter 及時應變，成功阻止 Cicada 攻擊

結語

概覽

快速偵測與事件應變，仰賴三項關鍵要素：

- 資料——涵蓋組織內部與全球層級。
- 人工智慧——用以處理龐大的資料量。
- 人類威脅專家與研究人員——在入侵行為實際顯現之前，識別出偵察嘗試。

Threat Hunter 是 Symantec[®] Endpoint Security Complete(SEC)的一項全新功能，整合了上述三大關鍵要素，讓資安團隊得以快速應變資安事件、阻止入侵行為發生。

我們世界級的威脅分析師，正是當年揭露 Stuxnet 與 WastedLocker 的同一批網路資安專家。他們會審查來自全球客戶遙測資料的機器學習洞察分析結果，並直接透過 SEC 產品主控台，向組織提供攸關潛在入侵事件的重要洞察，提醒資安維運中心(SOC)團隊注意組織可能遭遇的入侵嘗試。

這些洞察內容可能涵蓋攻擊行動細節、攻擊者所使用的工具、戰術與程序，並附上應變指引建議。SOC團隊可運用這些經過人工審查的資安事件資訊，透過 SEC 豐富的工具組合採取適當行動，包括隔離裝置、套用政策以允許或封鎖應用程式、限制合法應用程式的不當行為等。

「Threat Hunter與委外代管服務的差別在於，我們並不是要取代客戶的SOC團隊，也不是要接管客戶的整體環境。我們的核心宗旨，是提供盡可能完整、且具備可執行性的資訊，藉此強化客戶團隊的能量，讓客戶能夠迅速應變。這項服務的定位，其實更像是第二雙眼睛，專門找出那些可能因為SOC人員被其他優先事項壓得喘不過氣，而遭到疏漏的關鍵攻擊。」

前言

要因應當今手法精密的威脅，組織所需要的，遠不僅止於端點防護平台與端點偵測與回應(EDR)解決方案。他們需要全新的工具，來防範自身的防護盲點，以及攻擊者在組織內部所採用、傳統工具難以察覺或阻止的戰術與技術手法。其中一項盲點，正是尚未被發現的入侵跡象。即使SOC團隊已備妥許多用於偵測威脅的工具，卻經常被龐大的資料量所淹沒。更重要的是，他們往往缺乏足夠的資源，去追查每一則警示，更遑論發掘規模龐大、遍及全球且持續進行的鎖定式攻擊。

SESC 透過其 Threat Hunter 功能，提供了恰如其分的情境資訊。

重新思考入侵偵測：Symantec Threat Hunter

傳統的入侵偵測工具與技術，很容易錯失對組織最具威脅性的攻擊。這類工具通常僅擷取組織內各連接端點(例如：端點裝置、電子郵件、代理伺服器)的個別掃描結果。由於這種做法無法對新興威脅提供全域可視性或情境資訊，資安團隊必須自行手動比對關聯這些掃描結果，並整合來自外部來源、範圍有限的威脅情報。此外，由於多數組織並不具備設計人工智慧演算法的專業能力，也缺乏調查攻擊組織的專業威脅研究人員，因此往往面臨威脅可視性缺口、偵測精準度不足，以及潛伏時間過長等問題。

Threat Hunter 讓資安團隊得以快速應變端點資安事件，並將攻擊造成的衝擊降至最低。Threat Hunter是SESC的關鍵功能之一，涵蓋能為整條攻擊鏈提供防護的各項技術，包括攻擊面縮減、攻擊防範、入侵防範，以及偵測與回應。Threat Hunter結合豐富的遙測資料、機器學習，以及世界級威脅研究人員的研究成果，為SOC團隊提供量身打造、具優先順序的資安事件通報與應變建議。

Threat Hunter 與傳統的委外代管偵測與回應服務不同之處在於，賽門鐵克企業事業部團隊並不會取代SOC團隊，而是以情報與洞察分析，強化SOC團隊的能力，而非單純提供戰術層級的事件監控。多年來，賽門鐵克 Threat Hunter 團隊始終站在業界尖端資安研究的最前線，識別並追蹤部分最難以捉摸的進階持續性威脅組織。憑藉他們對攻擊者所使用工具、戰術與程序的深入洞察，得以從最細微的線索中拼湊出完整樣貌，詳細呈現貴組織當下正在發生的攻擊事件全貌。他們深知如何應變，也能為您提供指引。

Symantec Threat Hunter 及時攔截 WastedLocker 勒索軟體

EvilCorp並非只是電視劇裡虛構的公司名稱，而是一個真實存在、手法精密的網路犯罪集團，即便其首腦已遭美國聯邦調查局(FBI)起訴，該集團依然持續活躍、未見收斂。2020年6月，Evil Corp 針對美國多家大型企業，發動了一波名為 WastedLocker 的鎖定式勒索軟體攻擊。這波攻擊，原本足以輕易讓這些企業全數陷入癱瘓。

此次攻擊鎖定的目標，多數為大型企業，其中八家名列財星500大企業(Fortune 500)。除了一家例外——一家由海外跨國企業於美國設立的子公司——其餘遭鎖定的組織，全數皆為美國本土企業。攻擊的目的，是藉由加密受害者絕大多數的電腦與伺服器，癱瘓其 IT 基礎架構，藉此勒索高達數百萬美元的贖金。

發現與調查結果

最初的入侵管道，涉及 SocGhosh 攻擊框架，該框架透過遭入侵的合法網站，以偽裝成瀏覽器更新程式的壓縮 JavaScript 檔案形式，遞送至受害者端。第二個 JavaScript 檔案則運用 whoami、net user、net group 等命令，對電腦進行剖析。接著，攻擊者利用 PowerShell 下載更多與偵察相關的 PowerShell 指令碼。一旦攻擊者成功取得受害者網路的存取權限，便會結合使用 Cobalt Strike 與多種就地取材式攻擊工具，竊取憑證、提升權限，並在網路中橫向移動，於多台電腦上部署 WastedLocker 勒索軟體。

這波攻擊活動，由賽門鐵克鎖定式攻擊雲端分析技術，主動於多個客戶網路中偵測發現。賽門鐵克 Threat Hunter 團隊隨即審查並驗證了相關活動，很快便發現這些活動，與公開文件記載中 WastedLocker 攻擊早期階段的活動高度吻合。

Threat Hunter 團隊的即時應變

這項發現，讓賽門鐵克 Threat Hunter 團隊得以識別出更多同樣遭 WastedLocker 鎖定的其他組織，並找出攻擊者所使用的其他工具、戰術與程序。這些資訊，讓賽門鐵克分析師得以針對攻擊的每一個階段，強化賽門鐵克的防護能力。與此同時，賽門鐵克 Threat Hunter 團隊也向 68 家客戶發出了早期預警，向他們說明其網路已遭攻擊者入侵，且攻擊者正著手為部署勒索軟體攻擊鋪路。透過主動以電話與電子郵件聯繫客戶，該團隊成功協助中斷了這波攻擊行動。若這些攻擊得逞，恐將造成數百萬美元的損失、營運中斷，甚至可能對整條供應鏈造成骨牌效應般的衝擊。

資安維運中心(SOC)所面臨的挑戰

及早偵測資安事件，能讓後續矯正作業更為輕鬆；然而，資安團隊在試圖偵測並徹底掌握進階攻擊全貌的過程中，面臨著多重挑戰，包括警示疲乏、需要更多情境資訊、人力配置問題，以及需要一張安全網。

誤判所帶來的警示疲乏

資安工具會產生大量警示，形成一種「重量不重質」的窘境，資安分析師每天可能收到多達10,000則警示。為了處理這些警示，SOC分析師必須逐一深入調查，判斷其真偽。由於其中許多屬於誤判，SOC分析師的工作負擔因此變得更加沉重。數量不斷攀升的警示，需要進行分類、追蹤與驗證。這個過程令人疲憊不堪，資安團隊也因而承受龐大壓力、疲於奔命。結果就是，由於一天之內不可能處理完所有警示，關鍵警示很容易就此被忽略而漏接。

Enterprise Strategy Group針對資安成熟度與業務賦能之間關聯性所做的研究顯示，截至2020年3月，將近三分之二的領先組織，會忽略其資安警示與事件中的25%，原因在於逐一深入處理每一則警示並不切實際(出處：Enterprise Strategy Group, The Relationship Between Security Maturity and Business Enablement [May 5, 2020])。此外，Ponemon Institute的研究也顯示，識別出一起入侵事件的平均耗時為197天，而平均圍堵時間則為69天(出處：Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview [July 2018])。由此可見，SOC團隊顯然需要一套方法，協助縮短偵測與圍堵時間，並妥善處理未被處理的警示。

業界長久以來普遍認為，只要將警示進行關聯比對，就能解決警示過載的問題。然而實際上，關聯比對與篩選作業同樣不容易達成。真正需要的，是人類的專業判斷，加上由專家所打造的演算法。

需要更多情境資訊

SOC分析師若要妥善處理警示，需要掌握攻擊與攻擊者的所有細節，才能聚焦於偵測與矯正作業。然而，除非對入侵指標 (IOC) 與特徵碼名稱具備深入理解，否則很難得知有哪些指標可能遭到疏漏，也難以判斷哪些個別事件之間彼此相關、哪些又互不相干。

資安團隊需要清楚了解一則警示為何嚴重，也需要各種線索，協助判斷組織正在何處、以何種方式遭受攻擊。此外，他們也需要全面掌握攻擊者及其戰術、技術與程序的一切資訊，才能做出最佳判斷，阻止威脅行為者存取其網路與資產。

人力配置問題與安全網的必要性

由於威脅數量過載，加上分析師為保護組織所承受的工作步調，因人力配置問題而漏接警示的風險確實存在——而這也會帶來實際的業務衝擊。根據 Ponemon Institute 於 2019 年 4 月完成的研究報告，資料外洩事件的平均成本高達 392 萬美元(出處：Ponemon Institute, Cost of a Data Breach Report 2019 [April 2019])。內部 SOC 團隊需要清楚知道，萬一有所疏漏，還有另一支配備強大工具的專業分析師團隊，能夠補位揪出可能遭到忽略的漏網之魚。

Threat Hunter 分析能力

Threat Hunter 結合了地方與全球層級的遙測資料、機器學習分析，以及由賽門鐵克專業威脅獵捕專家人工審查驗證的分析結果，藉此揪出原本可能規避偵測的攻擊行為。

涵蓋地方與全球層級的龐大遙測資料集

Threat Hunter 的分析能力，仰賴一個規模龐大的全球資料集。我們具權威性的資料湖，蒐集了賽門鐵克整體產品組合中所有產品的事件資料，涵蓋端點、網路、電子郵件與雲端應用程式。Threat Hunter 同時也蒐集其他客戶可能曾經歷過的威脅細節，藉此擴展全球視野。這個龐大的資料集，讓 Threat Hunter 得以建構出更優異的分析能力，並隨著新資料的持續匯入而不斷精進。

「這是一種『有人在背後溫和守護著你』的安心感。即使是已擁有自身威脅獵捕團隊的成熟組織，這張安全網依然深具價值，因為我們是從截然不同的全球視角出發，進行威脅獵捕工作。我們檢視的並非單一客戶的資料，而是橫跨所有客戶的整體資料樣貌。透過在其他客戶網路中偵測到相同的攻擊行動，我們得以向可能同樣受影響、卻尚未察覺任何跡象的客戶，發出早期預警。舉例來說，某個SOC團隊或許只看得見攻擊者行動的前三個步驟；但憑藉我們的全球視野，我們早已知道接下來三個步驟會是什麼。正因為Threat Hunter提供了這樣的全球知識，SOC 團隊才得以主動搜尋，並防範這些後續步驟的發生。」

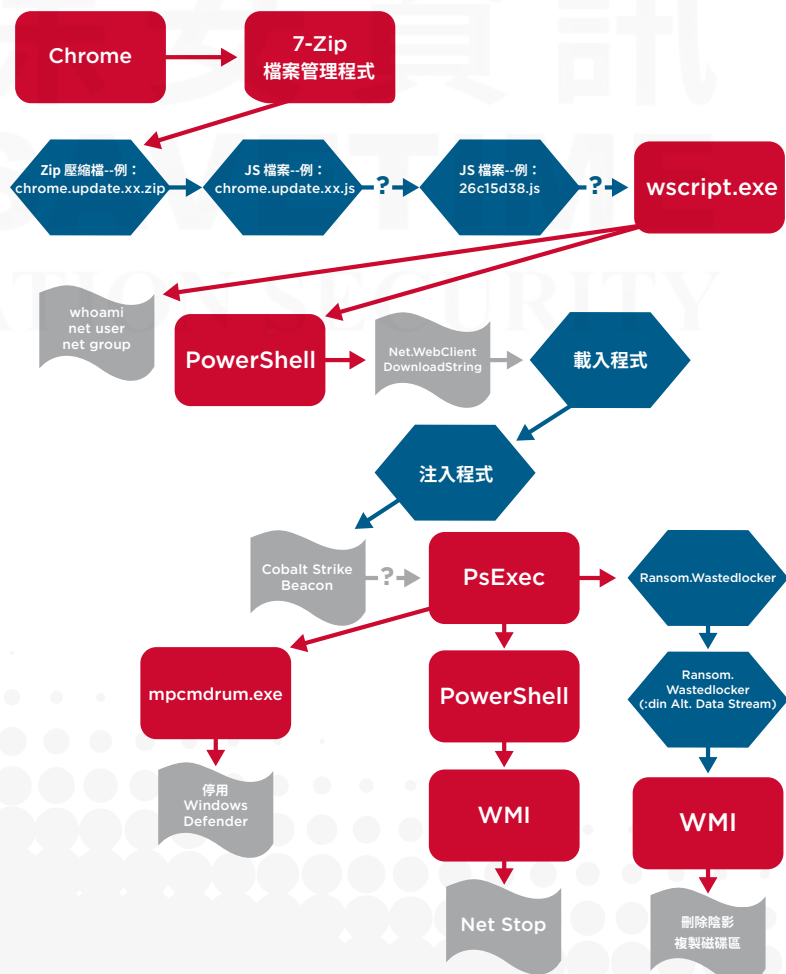
「Threat Hunter與企業內部威脅獵捕團隊最大的不同之處，在於我們能取得賽門鐵克的全部遙測資料，涵蓋端點，以及電子郵件、網路、雲端等各種資料來源。我們能運用這些資訊，將威脅回溯至特定的攻擊途徑、驗證攻擊是否真實存在，並取得更多情境資訊。舉例來說，由於我們掌握電子郵件資料，因此能將惡意程式回溯至某封特定郵件中所遞送的惡意檔案。」

鎖定式攻擊分析

Threat Hunter 的分析能力，是以鎖定式攻擊分析為基礎，其中涵蓋用於偵測入侵事件、PowerShell 活動、橫向移動，以及命令與控制信標活動的各項分析應用程式。鎖定式攻擊分析運用進階機器學習與雲端人工智慧技術，篩查資料湖中的資料，藉此識別資安事件，並持續提供演進中的分析能力。資料科學家憑藉深厚的專業知識，持續開發運行於此資料湖之上、更為優異的全新人工智慧演算法。此外，資安分析師也會評估這些洞察分析結果並提供回饋。這種由人工進行的演算法再訓練，能進一步精進分析引擎，藉此降低誤判、強化正確警示的判斷準確度。

當演算法偵測到可疑活動時，Threat Hunter 研究團隊便會審查該活動，並在警示中附註攻擊者戰術、技術與程序的詳細資訊，藉此提供攻擊的完整情境脈絡，讓 SOC 分析師得以快速識別威脅。請參閱下圖。

圖1：Threat Hunter能追蹤入侵行為與攻擊發生點之間的各個中間步驟。在此過程中，Threat Hunter的鎖定式攻擊分析技術與分析師，都能在流程中的任一環節察覺惡意活動，大幅提升客戶快速找出並徹底清除威脅的能力。



「Threat Hunter所提供的情境資訊十分重要——尤其是在賽門鐵克無法掌握部分網路可視性的情況下。當我們針對某台電腦上偵測到的特洛伊木馬提供情境資訊時，這些SOC分析師便能將該資訊，與範圍更廣的入侵指標(IOC)清單相互結合，並套用至我們缺乏可視性的網路範圍。相較於某些端點客戶，可能根本未曾留意特洛伊木馬的偵測結果、也完全未與賽門鐵克有任何層面的溝通，這無疑是一項極具價值的附加效益。」

賽門鐵克 Threat Hunter 團隊

賽門鐵克 Threat Hunter 團隊，在因應防護盲點方面具備獨特優勢。賽門鐵克分析師以訓練有素的專業眼光審視關鍵資安事件，並在攻擊者即將發動——或已經發動攻擊時，於 SESC 產品內設定相應通知。透過這樣的做法，賽門鐵克 Threat Hunter 分析師得以引導 SOC 團隊，將注意力聚焦於真正需要關注的重點領域。

賽門鐵克 Threat Hunter 分析師，除了多年來始終站在業界尖端資安研究的最前線之外，同時也具備數十年操作賽門鐵克全球資料的豐富經驗。這份經驗，更因其業界專業知識，以及打造工具以深入理解威脅態勢的技術能力，而更加深厚扎實。憑藉他們集結而成的專業才能，得以針對發生在SOC環境之外、威脅與戰術技術的演變趨勢，帶來全球視野的洞察。

協作力量帶來快速且有效的應變

賽門鐵克 Threat Hunter 團隊個別提供的洞察分析，背後有賽門鐵克整體產品組合的集體力量作為後盾。一旦發現攻擊行動，Threat Hunter 分析師便會與賽門鐵克資安應變(Security Response)團隊攜手合作，共同分析攻擊、確保防護機制已到位，並精確找出攻擊的性質。賽門鐵克資安應變團隊會著手改善既有的防護措施，並視需要建立任何額外的控管機制。這些新增與更新後的防護措施，會分發至該組織內部，藉此阻止攻擊。其他客戶同樣能因此受惠——他們可能同樣受到相同威脅影響，卻尚未察覺任何跡象。這項新的防護措施，會全球性地發布給所有賽門鐵克客戶，讓新的控管機制得以在整個賽門鐵克客戶社群中全面實施。

由 Threat Hunter 促成的威脅調查，構成了「從偵測走向防範」這套強大流程的一環，過去的偵測結果，將轉化為更強而有力的防範政策。透過回溯連結至由惡意行為所觸發的警示，並調整相應的行為隔離政策，SOC分析師得以運用每一次調查，實際且持續地強化其端點安全防護態勢。我們完全整合的防範與端點偵測及回應解決方案，能以獨到之處，讓SOC分析師的工作更具效率、更具成效。請參閱下列圖表。

圖2：Threat Hunter分析師針對具可疑活動的警告，進行審查並套用其洞察分析結果。分析師的評註會直接呈現於EDR主控台中，讓SOC團隊得以完整掌握入侵指標(IOC)，以及組織內受影響的人員與機器。

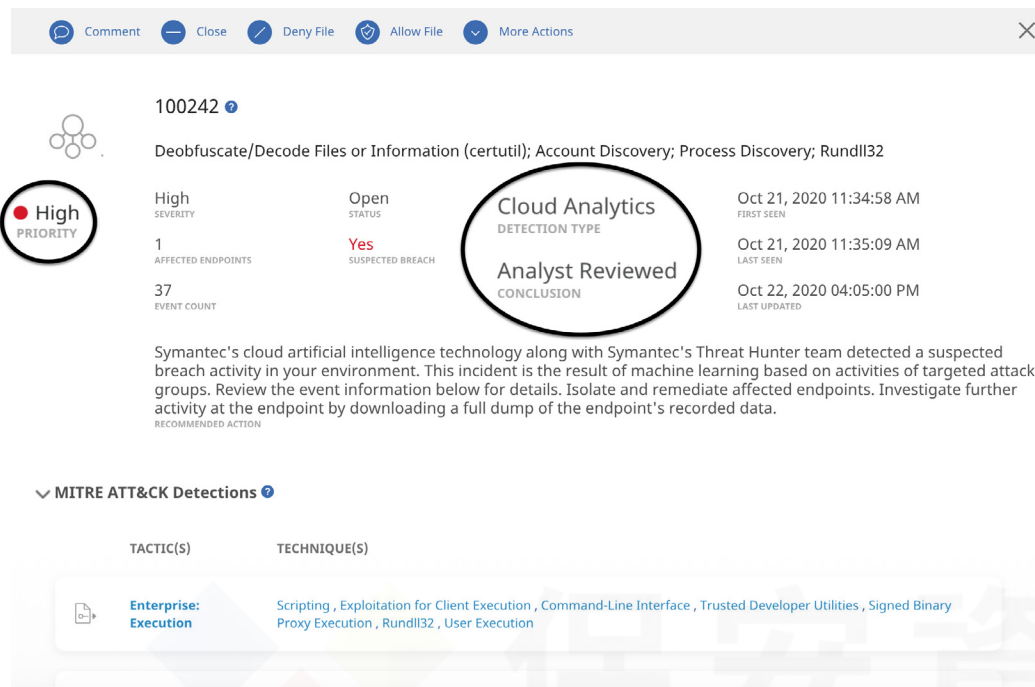
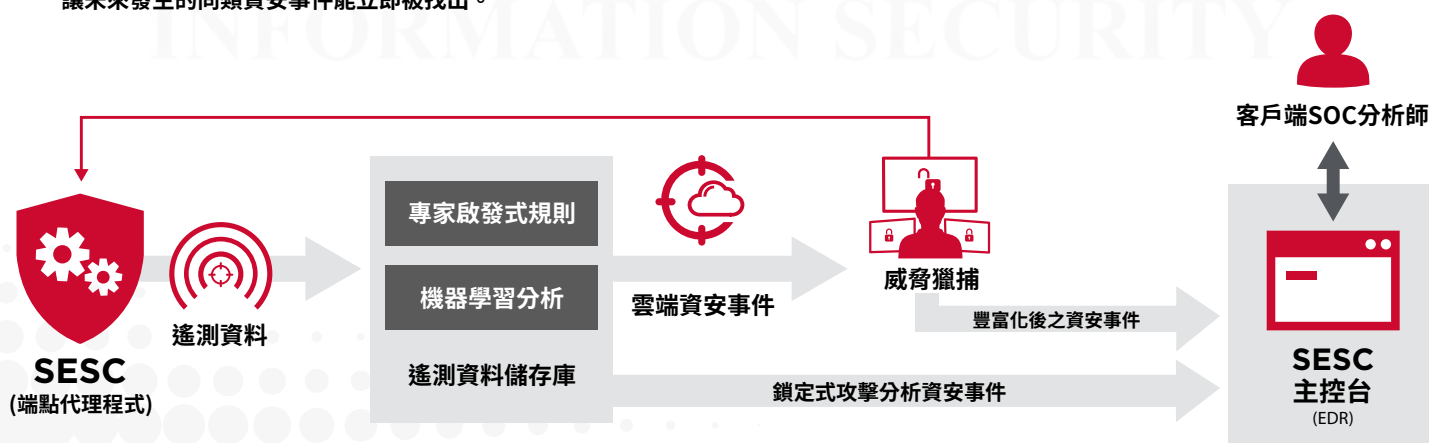


圖3：Threat Hunter 取用來自 SESC 代理程式的遙測資料，並將其饋入機器學習引擎，藉此識別資安事件，提供分析師進行後續分析與審查。Threat Hunter 分析師會將自身的經驗、工具與知識，套用於已標記的資安事件上，並可產出額外的洞察分析，協助客戶識別並控管組織內可能發生的攻擊行動。當 Threat Hunter 分析師所發現的資安事件經過定義與確認後，便會回饋至 Threat Hunter 的機器學習引擎中，讓未來發生的同類資安事件能立即被找出。



「有了賽門鐵克 Threat Hunter 分析師的協助，我們的客戶得以擁有業界最頂尖的資安研究人才作為後盾。」

Threat Hunter 及時應變，成功阻止 Cicada 攻擊

Cicada(又稱APT10)是一個進階持續性威脅(APT)組織，其對委外管理服務供應商(MSP)與委外管理資安服務供應商(MSSP)市場領域的高度興趣，早已有公開文件詳實記載。一旦成功入侵MSP，往往會連帶導致多家財星系列大型企業一併遭到入侵。2020年4月，賽門鐵克分析師觀察到與Cicada組織相關的威脅活動，此次攻擊鎖定的目標，是全球規模數一數二之MSP與MSSP供應商之一。近期Cicada已將目標轉向日本大型企業集團，這波活動同樣由賽門鐵克Threat Hunter團隊率先發現。

可疑的 PowerShell 活動

鎖定式攻擊分析技術，針對某組織內部的可疑PowerShell活動觸發警示。該PowerShell連上一台遠端伺服器下載內容，並在電腦上另外儲存了惡意檔案。每一個下載的檔案皆各不相同，每個案例中的PowerShell內容也各自具備部分獨特性。

攻擊者針對每一台遠端伺服器，僅鎖定一至兩台目標電腦使用，使得網路物件相關的入侵指標(IOC)，從全球防護的角度而言形同無用。

賽門鐵克 Threat Hunter 團隊，以部分共通的 PowerShell 特徵為線索，進一步在全球範圍內找出更多相關活動，最終發現十餘台遠端伺服器，正將內容推送至各個不同的目標。攻擊者一旦進入受害者主機，便會執行多支與偵察相關的指令碼，藉此找出具弱點的機器、繪製網路架構圖、檢查權限，並探測網域控制站。這些工具全數運用目標電腦上原生內建的應用程式執行。攻擊者投入相當大的心力，試圖清除與事件及 PowerShell 相關的系統紀錄，藉此規避賽門鐵克資安應用程式的偵測。

分享攻擊細節，促成有效隔離

賽門鐵克 Threat Hunter 團隊透過主動聯繫，向客戶說明其網路中發生的特定活動，成功阻止一場規模龐大的入侵事件。透過分享攻擊細節，賽門鐵克Threat Hunter團隊讓客戶得以立即隔離受影響的機器，運用該組織特有的獨特入侵指標(IOC)，找出網路中尚未運行 Symantec Endpoint Protection 的電腦，並展開攻擊活動的調查。透過主動與客戶保持聯繫，該團隊協助及早發現並阻止了這波攻擊，避免其他與該客戶有業務往來的組織一併受到波及。

「憑藉豐富的實務經驗，
[賽門鐵克Threat Hunter
團隊]得以針對發生在SOC
環境之外的威脅、戰術與
技術演變趨勢，帶來全球
視野的洞察。」

結語

最危險、最具破壞性的威脅，往往是您毫無防備、未曾預見的那一種。隨著鎖定式攻擊的複雜程度與數量持續攀升，企業需要減少分析師必須調查的資安事件總量，並確保應變人員能專注處理優先順序最高的事件。為達成此一目標，資安團隊需要協助，才能有效偵測出真正的攻擊。他們需要情境資訊，涵蓋所有關於攻擊與攻擊者的已知細節。由於他們必須以極快的步調保護組織，因此也需要一支後備力量，以防萬一漏接了關鍵事件。

賽門鐵克 Threat Hunter 作為 SESC 的關鍵功能之一，正是為了解決這些需求而生。Threat Hunter 結合了歷經時間考驗、能精準偵測的賽門鐵克鎖定式攻擊分析技術、賽門鐵克全球與地方層級的遙測資料，以及來自世界級威脅研究人員的攻擊分析能力。

透過 Threat Hunter，我們為您提供關於攻擊者、攻擊技術、受影響機器的詳細分析，以及矯正建議指引。我們藉此強化SOC團隊的能力，讓其得以快速結案端點資安事件，並將攻擊帶來的衝擊降至最低。

關於賽門鐵克

賽門鐵克是資安業界的長青樹，品牌享譽至今超過四十年。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進核心技術、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眾的長足進步。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，近年來Symantec很少出現在由公開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。(美籍華人王嘉康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召的一線廠商，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

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术型領導廠商，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安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，以及基於比原廠更熟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。