SOC 分析師最常遇到的 25 個 Windows 事件 ID

1. 4624 – 登入成功 2. 4625 – 登入失敗 3. 4648 – 使用明確憑證嘗試登入 4. 4672 – 為新登入指派特殊權限 5. 4634 – 登出 6. 4688 –已建立新進程7. 4689平台已允許執行Windows . 5158 – 阻止 Windows 過濾平台連線 10. 1102 – 已清除審核日誌 11. 4720 –已建立使用者帳戶 12. 4726 –已刪除使用者帳戶 13. 4732 – 已將成員新增至啟用安全的本機群組 14. 4738 –使用者帳戶已新增成員至啟用安全的全域群組 17. 4768 – 請求 Kerberos TGT 18. 4769 – 請求 Kerberos 服務票證 19. 4776 – 嘗試憑證驗證 20. 4798 – 枚舉使用者的本機群組成員身分21. 5140 – 存取網路5058 – KDC 服務已停止 24. 4703 – 分配使用者權限 25.事件 ID 4743 – 電腦帳戶已移動

1.事件ID 4624 –登入成功

·它代表什麼：記錄系統成功登入。
·為什麼重要：對於識別合法使用者或
未經授權的攻擊者已存取系統。
·分析師如何使用它：分析師追蹤這些事件以驗證登入是否來自授權用戶，以及登入時間、位置或方法是否與典型的
用戶行為一致。

·範例用例：當使用者從不尋常的位置（例如不同的國家/地區）登入時會觸發警報，這可能表示帳戶
已被盜用。
·緩解措施：實施多因素身份驗證 (MFA)，使用 VPN 進行遠端
存取並實施強密碼策略。
·偵測：針對來自不尋常的 IP 位址、地理位置或很少遠端登入的帳戶的登入設定警報。

2.事件ID 4625 –登入失敗

·它代表什麼：捕獲失敗的登入嘗試，通常是由於不正確的
證書。
·為什麼重要：重複登入失敗可能表示有暴力破解或憑證
填充攻擊。
·分析師如何使用它：分析師監控失敗的登入嘗試以識別異常的登入模式，特別是來自不熟悉或黑
名單 IP 位址的登入模式。
·範例用例：高權限帳戶多次登入失敗
（admin、root）被偵測到，這可能表示攻擊者試圖強行進入。

·緩解措施：在一定次數的失敗嘗試後設定帳戶鎖定策略，並
需要 MFA。
·偵測：對短時間內多次登入失敗發出警報，特別是對於
特權帳戶。

---

3. 事件 ID 4648 – 使用明確憑證登入嘗試

·意義：當進程或服務使用明確的憑證（例如為網路資源提供的憑證）登入時，會記錄此事件。

·重要性：可以指示橫向移動或升級，其中明確傳遞憑證以進行系統存取。

·分析師如何使用它：監控這些登入是否有異常系統或帳戶
訪問，特別是在非工作時間。
·使用案例範例：攻擊者入侵帳戶並使用明確的憑證在網路內橫向移動。

·緩解措施：使用最小特權存取控制，並將明確憑證的使用限制在基本服務範圍內。

·偵測：設定外部敏感資源的明確憑證使用警報
正常的商業活動。

---

4. 事件 ID 4672 – 指派給新登入的特殊權限

·它代表什麼：當新登入被指派特殊權限時記錄，例如
作為管理權利。
·重要性：追蹤帳戶何時獲得關鍵系統的特權存取權限，
這可能表示存在濫用或權限提升。
·分析師如何使用它：注意新的或意外的特殊權限分配
這可能表示橫向移動或升級。
·使用案例範例：一般使用者帳戶意外取得管理員權限，這可能是憑證竊取或惡意行為的跡象。

·緩解措施：限制重要人員的特權訪問，並確保定期審查使用者角色。

·偵測：當非管理帳戶被授予特殊權限時發出警報
或在奇怪的時間。

5.事件ID 4634 –註銷

·代表意義：捕獲註銷事件，指示使用者何時成功從系統註銷。

·為什麼重要：註銷事件確保會話安全關閉，並協助
監視用戶何時意外保持登入狀態。
·分析師如何使用它：分析師監控註銷事件以追蹤帳戶是否保持登入時間超過預期或是否發生未經授權的註銷
活動。
·使用案例範例：使用者在工作時間意外註銷，這可能表示會話劫持或異常終止。

·緩解措施：設定基於時間的註銷策略並對不活動採用會話逾時。
·偵測：當帳戶的活動時間超出正常會話持續時間時，設定註銷事件警報。

6.事件ID 4688 –已建立新進程

·意義：表示系統上已建立了一個新進程。
·為什麼重要：流程的創建可能預示著潛在的
惡意軟體或未經授權的腳本等惡意活動。
·分析師如何使用它：分析師追蹤流程的創建，特別是那些源自未知或不受信任位置的流程。

·範例用例：未經授權的使用者建立了一個可疑進程，這通常與勒索軟體等惡意軟體有關。

·緩解：使用端點偵測和回應 (EDR) 工具來阻止未經授權的進程並維護已知的白名單。

·偵測：針對從異常位置或異常執行檔（例如暫存資料夾或未知路徑中的程序建立)設定警報。

7.事件ID 4689 –進程已結束

·它代表什麼：捕獲進程的終止。
·重要性：終止的進程，特別是安全關鍵進程，可能表示攻擊者正試圖隱藏其活動的痕跡。

·分析師如何使用它：分析師追蹤終止的進程以識別實例
重要進程被惡意行為者強行停止或破壞。
·使用案例範例：攻擊者終止防毒軟體或系統監控
避免被發現的過程。
·緩解措施：限制對關鍵系統進程的存取並保持強大的安全性
配置。
·偵測：當關鍵安全程序意外終止或
多個行程快速連續結束。

---

8. 事件 ID 5156 – 允許 Windows 過濾平台連接

·意義：當 Windows 過濾允許連線時記錄
平台（WFP），例如透過防火牆或網路過濾器。
·重要性：此事件有助於監控和確認合法連接，同時允許分析師偵測未經授權或可疑的
流量。
·分析師如何使用它： SOC 分析師使用它來驗證允許進入關鍵系統的流量，特別是來自意
外或未經授權的來源的流量。
·範例用例：合法使用者連接到系統，但如果連接來自外部 IP 或不熟悉的來源，則會引起懷
疑。
·緩解措施：定期審核防火牆配置並限制不必要的服務
和港口。
·偵測：對允許連接到敏感系統或服務發出警報
未知或外部來源。

---

9. 事件 ID 5158 – Windows 篩選平台連線被阻止

·它代表什麼：捕獲 WFP 阻止連接的情況，例如當
連線違反了網路過濾規則。
·為什麼重要：阻止網路連線是一種關鍵的防禦機制，
阻止潛在的惡意流量到達內部系統。
·分析師如何使用它：分析師監控被阻止的連接以檢測可能的
惡意流量嘗試。
·使用案例範例：攻擊者嘗試連線到 C2 伺服器（命令和控制），但被防火牆阻止。

·緩解措施：定期檢查並更新防火牆規則，以阻止已知的惡意 IP
和交通類型。
·偵測：當關鍵基礎設施受到已知惡意 IP 或意外來源的連線嘗試時設定警報。

10.事件ID 1102 –稽核日誌已被清除

·意義 :此事件表示安全性稽核日誌已清除，
這可能是惡意活動的危險信號。
·重要性 :攻擊者通常會在攻擊後清除日誌以掩蓋其痕跡。此事件對於偵測篡改或後利用活動至關重要。
·分析師如何使用它 :分析師密切監視任何清除日誌的嘗試，因為這表明試圖掩蓋惡意行為。

·使用案例範例 :攻擊成功後，攻擊者會清除日誌以抹去其行為的任何證據。

·緩解措施 :限制對安全日誌的存取並配置日誌記錄以防止清除。
·偵測 :當日誌清除發生時發出警報，特別是對於通常
沒有日誌清除權限。

11.事件ID 4720 –已建立使用者帳戶

·它代表什麼 :記錄新使用者帳戶的建立。
·重要性 :未經適當授權建立新的使用者帳戶可能表示攻擊者正在設定後門或持久存取。

·分析師如何使用它 :分析師監控使用者帳戶的創建，特別是在正常業務流程之外時。

·範例用例 :攻擊者在入侵
系統來維持對環境的控制。
·緩解措施 :定期審核使用者帳號建立狀況，並對下列行為實施嚴格控制：
帳戶管理。
·偵測 :設定警報，以防意外建立使用者帳戶或具有
管理權限。

12.事件ID 4726 –使用者帳號已被刪除

·它代表什麼 :此事件捕獲使用者帳戶的刪除。
·重要性 :攻擊者可以利用刪除帳戶來抹除其存在的痕跡或停用安全控制。

·分析師如何使用它 :分析師監控任何帳戶刪除，特別是
特權帳戶。
·使用案例範例 :攻擊者刪除被入侵的使用者帳戶，以消除其存在的證據。

·緩解措施 :僅允許授權管理員刪除帳戶。
·偵測 :設定任何意外帳號刪除或高權限刪除的警報
特權帳戶。

---

13. 事件 ID 4732 – 成員已新增至啟用安全的本機群組

·它代表什麼：當使用者被加入到啟用安全性的
本地組織。
·重要性：未經批准的群組成員身分變更可能表示攻擊者提升了他們的權限或獲得了
對資源的未經授權的存取權限。
·分析師如何使用它：分析師追蹤群組成員身分的變更以偵測任何未經授權的特權提升。

·範例用例：攻擊者將自己加入到具有管理權限的群組中
權限來增加對系統的控制。
·緩解措施：定期審核群組成員資格，並限製成員資格變更
值得信賴的管理者。
·偵測：針對敏感或特權群組的新增設定警報。

14.事件ID 4738 –使用者帳戶已更改

·意義：此事件表示現有使用者帳戶已被修改，
例如更改密碼或更改群組成員資格。
·為什麼重要：帳戶變更，尤其是未經適當授權的變更，可能會
表示特權帳戶被濫用或存在攻擊者活動。
·分析師如何使用它：分析師使用它來檢測對使用者資料的未經授權的更改
帳戶，特別是那些具有較高權限的帳戶。
·使用案例範例：攻擊者更改受損帳戶的密碼以防止被發現。

·緩解措施：實施強密碼原則並確保記錄和審查關鍵帳戶的變更。

·偵測：當敏感帳號屬性被修改時設定警報，特別是在正常工作時間之外進行修改。

15.事件ID 4740 –使用者帳號被鎖定

·意義：當使用者帳戶因超過以下時間而被鎖定時，將記錄此事件：
允許的登入失敗次數。
·重要性：帳戶鎖定通常是由於暴力破解嘗試或憑證填充而發生的，這表明存在潛在的惡
意行為。
·分析師如何使用它：分析師監控這些事件以偵測暴力攻擊和
不尋常的帳戶鎖定模式。
·使用案例範例：暴力攻擊在多次失敗後鎖定使用者帳戶
登入嘗試。
·緩解措施：強制執行帳戶鎖定策略並使用 CAPTCHA 或 MFA 來防止自動攻擊。

·偵測：設定多個帳戶鎖定警報，特別是來自相同來源的帳戶鎖定
或高權限帳號。

---

16. 事件 ID 4756 – 成員被加入到啟用安全的全域群組

·它代表什麼：當成員被加入到啟用安全性的
全球集團。
·重要性：全域群組成員資格的變更可能會影響存取控制，未經授權的新增可能表示存在惡意活動。

·分析師如何使用它：分析師追蹤此事件以確保敏感的全域群組不會被未經授權的使用者修改。

·範例用例：攻擊者將自己加入到具有廣泛權限的群組中，
這可能允許存取敏感資料。
·緩解措施：定期檢視全域群組成員資格，並確保只有經過授權的
人員可以做出改變。
·偵測：針對全域群組的變更設定警報，尤其是「網域管理員」等敏感群組。

17.事件ID 4768 –請求Kerberos身份驗證票證（TGT）

·意義：當使用者要求票證授予票證時，記錄此事件
（TGT)來自 Kerberos 金鑰分發中心（KDC）。
·重要性： TGT 請求是身分驗證過程的關鍵部分，並且可能成為試圖劫持或冒充使用者的攻擊者的目標。

·分析師如何使用它：分析師追蹤 TGT 請求以偵測異常情況，例如不尋常的
可能預示著憑證被盜的票證請求。
·使用案例範例：攻擊者使用竊取的憑證請求特權帳戶的 TGT，試圖冒充受害者。

·緩解措施：使用強密碼進行 Kerberos 驗證，並定期監控不尋常的 TGT 請求模式。

·偵測：針對偏離正常使用模式的 TGT 請求設定警報（例如，
短時間內數量很高）。

---

18. 事件 ID 4769 – 已請求服務票證

·它代表什麼：記錄從 KDC 要求服務票證的時間
存取網路服務。
·為什麼重要：服務票據可能在橫向移動攻擊中被濫用，例如
例如使用傳遞票證（PTT)技術。
·分析師如何使用：分析師使用此事件來偵測異常的服務票證請求，例如來自未經授權的使用者或裝置的請
求。
·使用案例範例：攻擊者請求他們通常不會存取的系統的服務票證，這通常是作為橫向移動攻擊的一部分。

·緩解措施：監控異常服務單請求並實施更嚴格的控制
服務票發行。

·偵測：當系統要求服務票據時發出警報
由用戶。

---

19. 事件 ID 4776 – 電腦嘗試驗證帳戶的憑證

·意義：當電腦嘗試驗證憑證（例如登入)時，將記錄此事件。

·重要性：這些事件對於偵測與未經授權的存取嘗試相關的身份驗證失敗很有用。

·分析師如何使用它：分析師監控此事件，以查找憑證驗證失敗，
識別暴力破解或 NTLM 中繼等攻擊。
·範例用例：攻擊者重複嘗試使用被盜的
憑證來存取關鍵系統。
·緩解措施：實施強而有力的身份驗證控制並監控登入嘗試是否有異常活動。

·偵測：對失敗的身份驗證嘗試設定警報，並將其與其他事件關聯起來以取得妥協指標。

---

20. 事件 ID 4798 – 列舉使用者的本機群組成員身份

·意義：當攻擊者或管理者列舉特定使用者帳戶的本機群組成員身分時記錄。

·重要性：枚舉群組成員身分可能是攻擊者
偵察階段尋找高價值目標。
·分析師如何使用它：分析師觀察這些事件以偵測任何偵察
旨在識別特權群體的活動。
·範例用例：攻擊者列舉本機群組來識別高權限
帳戶或系統。
·緩解措施：透過實施適當的使用者權限來限制對群組成員資格列舉的存取。

·偵測：當發生群組成員身分列舉時發出警報，特別是對於具有特權存取的使用者。

21.事件ID 5140 –存取了網路共享對象

·意義：當網路共享或目錄對象
透過網路存取。
·為什麼重要：監控網路共用存取有助於偵測未經授權的
存取或可疑的文件共享活動。
·分析師如何使用它：分析師監視此事件以檢測未經授權的訪問
關鍵文件共享和數據。

·使用案例範例：攻擊者在竊取使用者帳戶後存取儲存在網路共用上的敏感檔案。

·緩解措施：對文件共用實施存取控制並要求進行適當的身份驗證
用於存取敏感資料。
·偵測：對敏感共享的存取或可能造成異常存取模式的警報
表示妥協。

---

22. 事件 ID 5152 – Windows 篩選平台阻止了連接

·意義：當連線被 Windows 過濾平台封鎖時記錄，例如當防火牆規則或安全過濾器封鎖連線時。

·為什麼重要：阻止未經授權的連線有助於保護關鍵
系統免受外部攻擊或未經授權的存取。
·分析師如何使用它：分析師監控被阻止的連接以檢測和確認
惡意或可疑流量。
·使用案例範例：攻擊者嘗試使用已知的惡意 IP 位址存取系統，但被防火牆封鎖。

·緩解措施：定期檢查和更新防火牆規則，以阻止已知的惡意
交通。
·偵測：當嘗試阻止連線時設定警報，特別是來自不受信任來源的連線。

---

23. 事件 ID 5058 – 金鑰分發中心服務已停止

·它代表什麼：當金鑰分發中心 (KDC)
服務停止運作或被竄改。
·重要性： KDC 對於 Kerberos 驗證至關重要，停止它會嚴重影響系統存取或助長 Kerberos 票證操縱等攻擊。

·分析師如何使用它：分析師專注於 KDC 服務中斷，因為他們指出
系統受損或受到攻擊。
·範例用例：攻擊者試圖停止 KDC 服務以利用
Kerberos 驗證中的漏洞。
·緩解措施：確保 KDC 服務受到保護並定期監控。
·偵測： KDC 服務意外停止或重新啟動時發出警報。

---

24. 事件 ID 4703 – 已指派使用者權限

·意義：當使用者權限（例如備份操作員)分配給
一個帳戶。
·為什麼重要：使用者權限的無理變更可能表示特權
升級企圖或濫用。

·分析師如何使用它：分析師監控這些事件以偵測意外的變化
可能表明被剝削的使用者權利。
·使用案例範例：攻擊者透過將自己新增至具有提升的使用者權限的帳戶（例如備份操作員)來提升
權限。
·緩解：限制和審核對敏感角色的使用者權限分配。
·偵測：當對正常管理操作以外的帳戶進行使用者權限分配時設定警報。

25.事件ID 4743 –電腦帳戶已移動

·它代表什麼：當電腦帳戶移至 Active Directory 內的新組織單位 (OU) 時觸發此事件。

·為什麼重要：行動電腦帳戶可能表示攻擊者正在
試圖隱藏受感染的系統或操縱其權限。
·分析師如何使用它：分析師監視此事件以偵測 AD 內電腦帳戶位置的未經授權的變更。

·範例用例：攻擊者將受感染的系統移至單獨的 OU 中，以
避免在審計過程中被發現。
·緩解措施：鎖定 Active Directory 中行動電腦帳戶的權限並執行定期審核。

·偵測：設定電腦帳戶位置變更的警報，特別是當
它們涉及不應該移動的系統。