如何了解惡意程式感染後對 AD 造成異常設定變動?

前提：近來駭客攻擊鎖定 Active Directory 攻擊的比例升高，攻入 AD 就可加速病毒感染的效率。透過一些駭客工具就可進行帳號提權、進而改變 GPO 限制原則，透過 GPO 大量派送加密勒索病毒，進行程式注入攻擊。

因此可透過 Netwrix 來了解是否有嘗試登入(密碼暴力攻擊)活動、異常提權、臨時性帳號活動、GPO 設定的異常變動紀錄，有助於調查不尋常的嘗試登入或可疑設定變動。

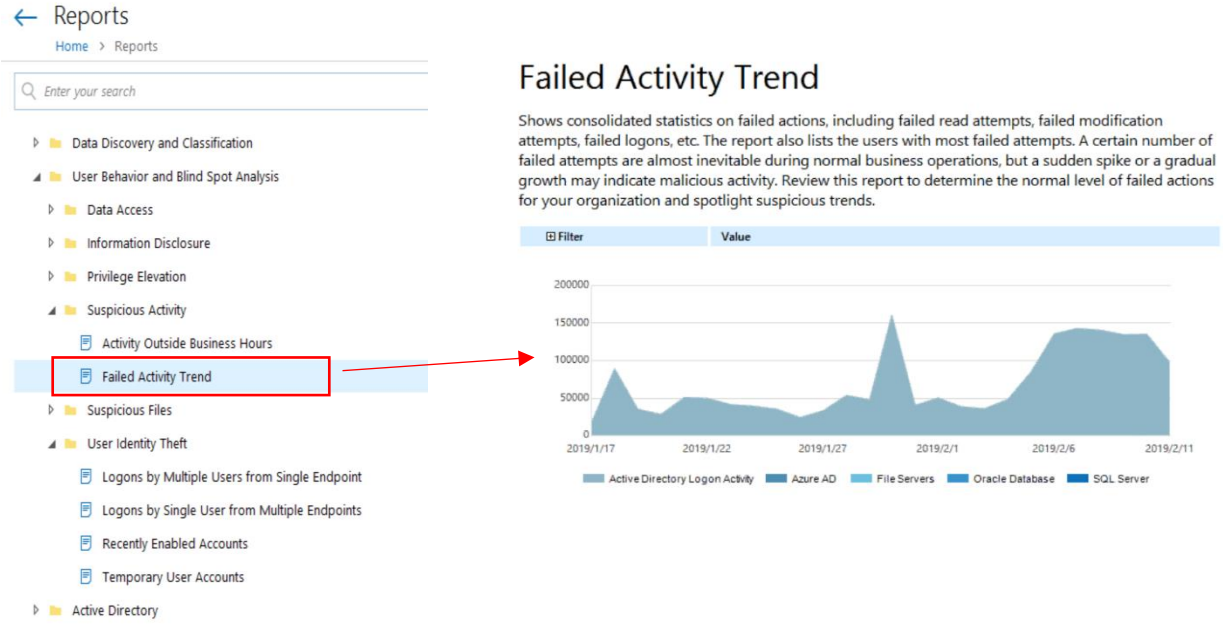
本情境適用於: Netwrix for 9.8 及以上版本，監看 Active Directory 模組

Netwrix 調查範例：

1. 嘗試登入失敗活動檢查

1-1 失敗活動趨勢觀察

報表動線：User Behavior and Blind Spot Analysis→Suspicious Activity → Failed Activity Trend 報表

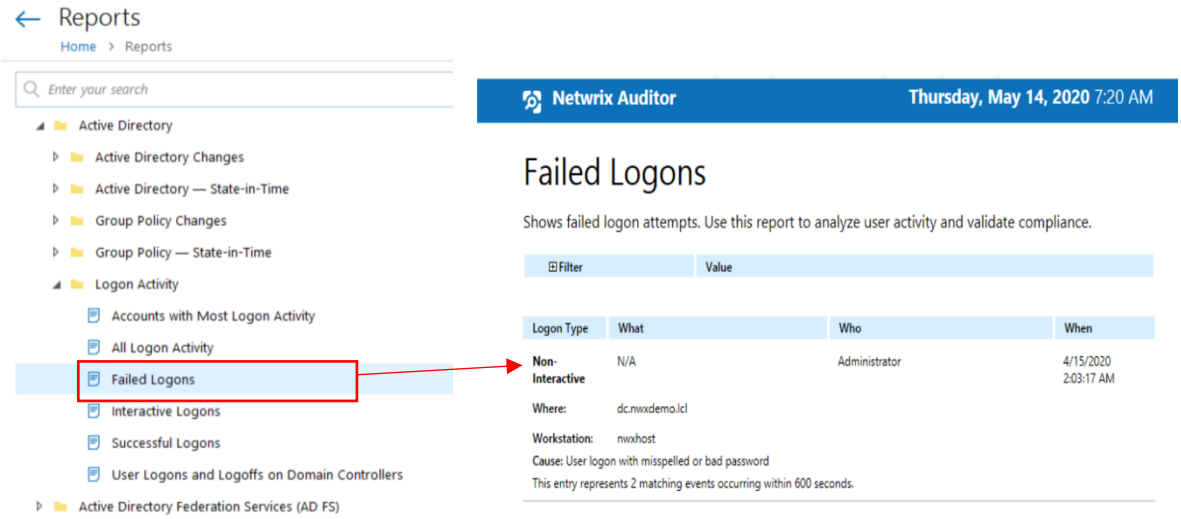


從該報表過濾條件中 Datasource 點選” Active Directory Logon Activity” 及想要查找時間區間，就會出現嘗試登入失敗活動趨勢統計圖及人員次數總統計。

1-2 登入失敗活動進階分析

- **分析嘗試登入失敗原因**

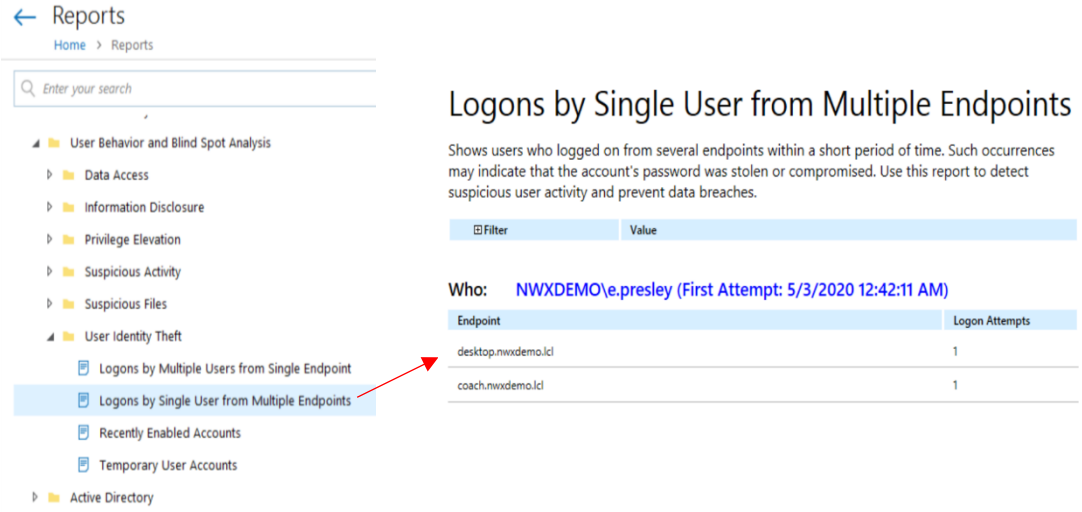
報表動線： Active Directory → Logon Activity → Failed Logon 報表



報表紀錄中會顯示嘗試登入失敗的類型(Logon Type)、時間、帳號、登入 DC 名稱(Where)、使用者電腦名稱(Worksation)、失敗原因...等資訊
從中可觀察到是否有被利用字典檔產生的奇怪帳號或密碼進行嘗試登入活動，及運用程式進行規律性的嘗試登入活動。

- **了解同一帳號是否有多個登入來源電腦**

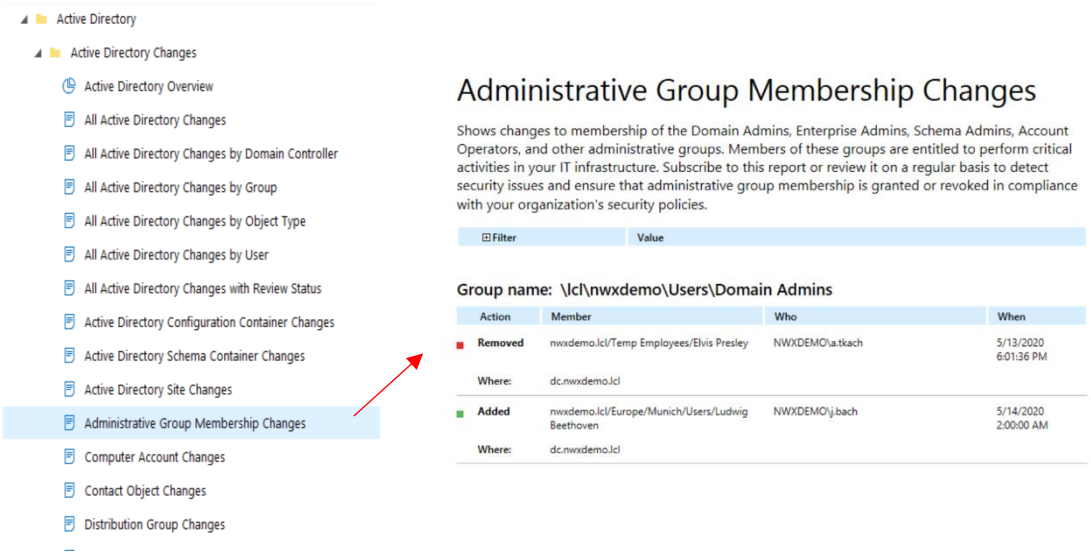
報表動線：User Behavior and Blind Spot Analysis→User Identity Theft → Logons by Single User from Multiple Endpoints 報表



2. 提權變動檢查

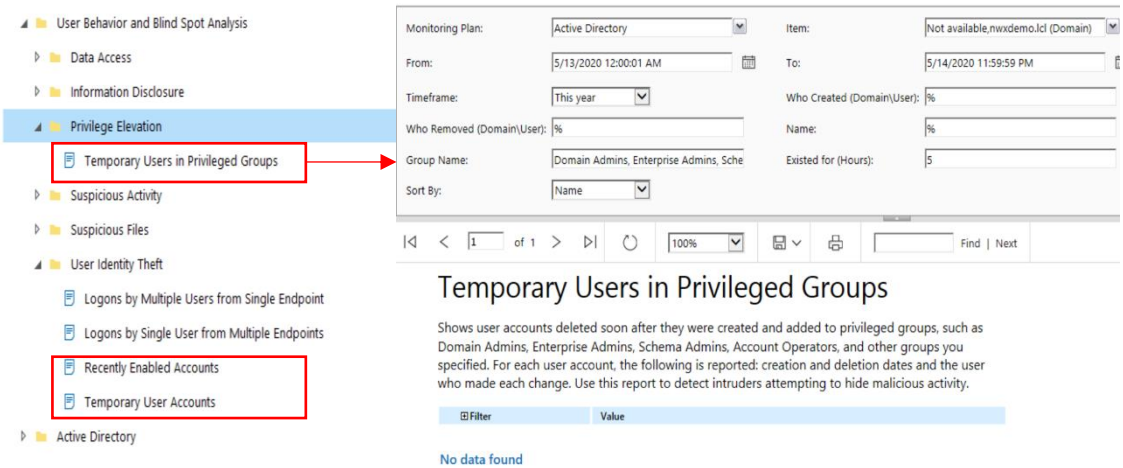
2-1 檢查管理者群組成員是否有變動

報表動線：Active Directory → Active Directory Changes → Adminstrative Group Membership Changes 報表



2-2 檢查是否有臨時性帳號變動

報表動線：User Behavior and Blind Spot Analysis→Privilege Elevation → Temporary Users in Privileged Groups 報表
或是
User Behavior and Blind Spot Analysis→ User Identity Theft →Recently Enabled Accounts 或 Temporary User Accounts 報表

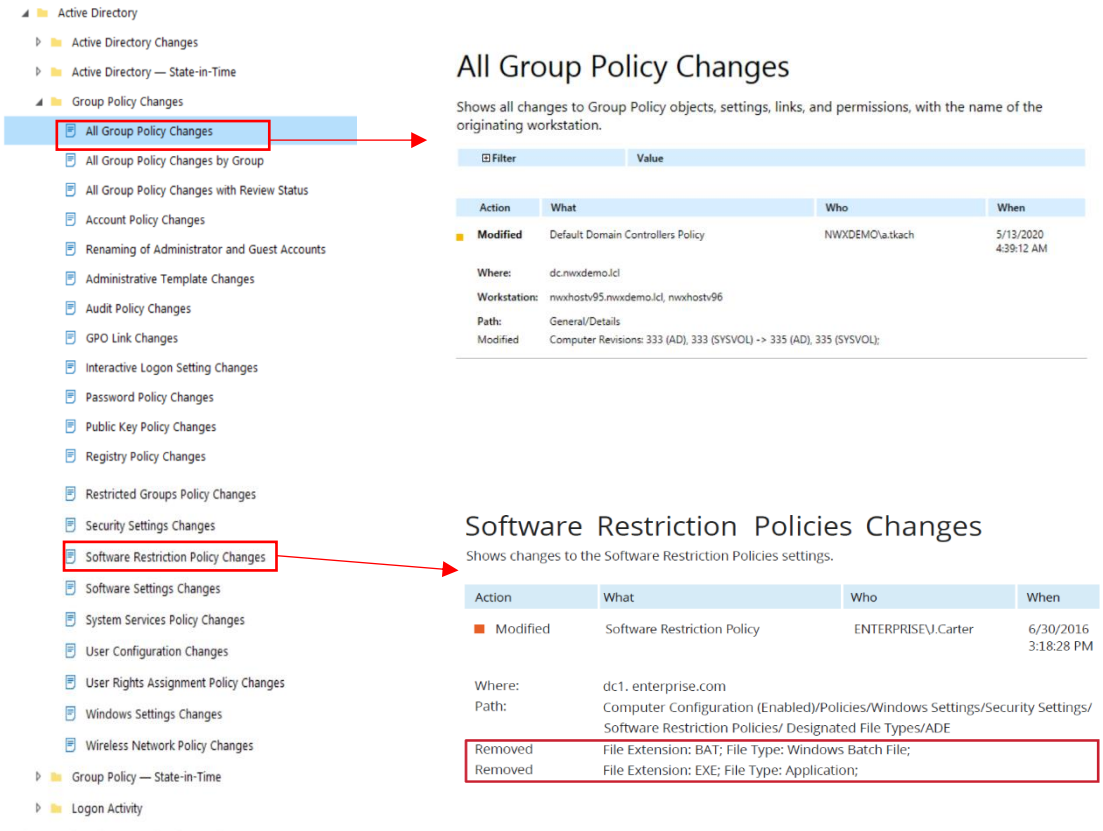


用來檢查是否有短暫時間內(如 5 小時)的帳號被啟用又很快被停用的行為。

3. GPO 設定變動檢查

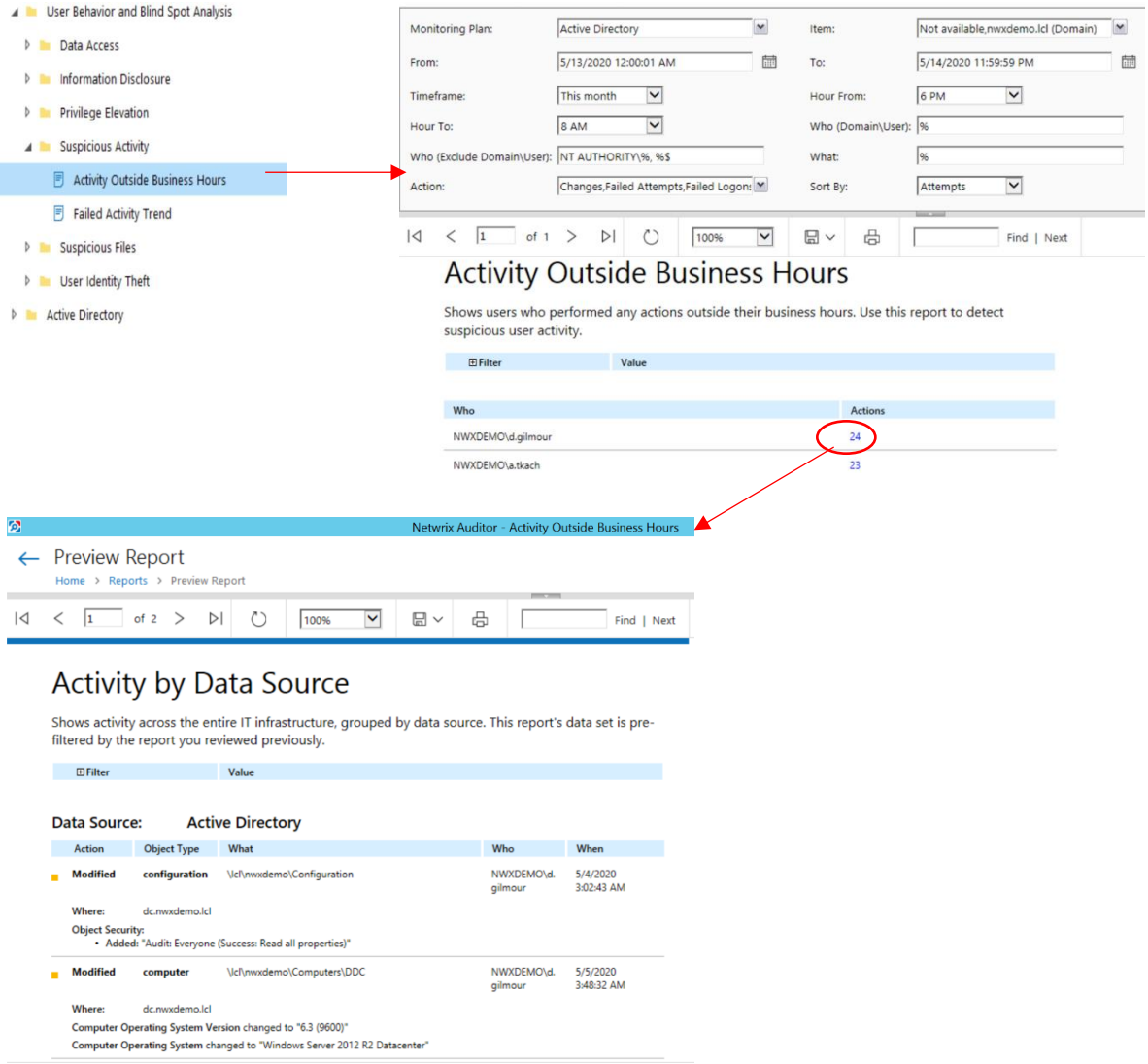
3-1 所有 GPO 設定變動檢查

報表動線：Active Directory → Group Policy Changes → All Group Policy Changes 報表　或　Software Restriction Policy Changes 報表



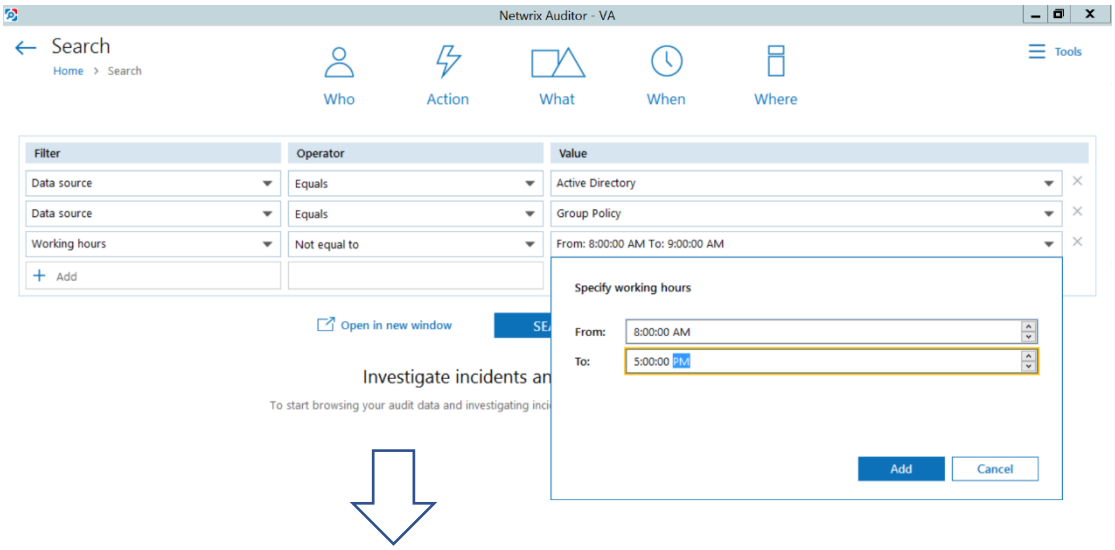
4. 非上班時間的 AD 變動檢查

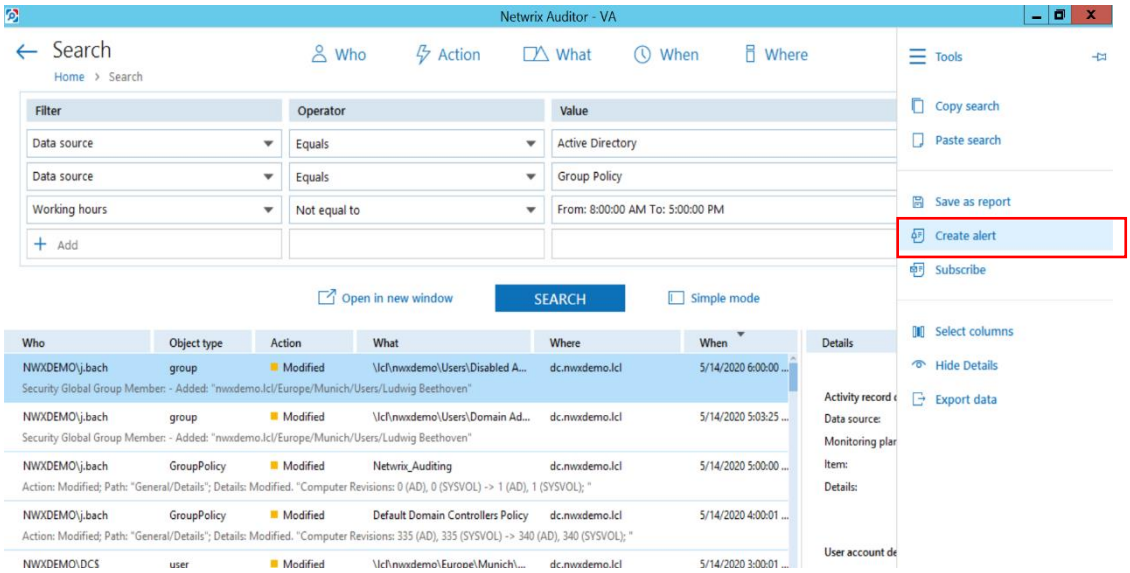
報表動線：User Behavior and Blind Spot Analysis→Suspicious Activity → Activity Outside Business Hours 報表



設定好非上班時間的時段，並於 DataSource 中點選”Active Directory”就會出現非上班時間對 AD Server 產生的變動紀錄。

也可另外運用 Alert 功能設定相關的即時警示 Email 通知：





設定成”非上班時段的 AD, GPO 設定變動警示通知”