DATASHEET

針對 ACTIVE DIRECTORY 曝露風險和即時攻擊提供持續能見度的 ADAssessor

Active Directory (簡稱 AD) 是微軟的產品，由若干服務組成，用於管理 Windows 網路上的權限和網路資源的存取。由於它是所有企業資源的主要資訊來源，並且與商業應用程式緊密整合，因此成為攻擊者的高價值目標。

攻擊者可以針對 Active Directory 中曝露的風險，迅速取出整個網域上的敏感性資料，例如使用者帳戶、系統帳戶或受信任的網域資訊等。此資料提供了敵人要鎖定的目標，例如特權帳戶、安全權限重疊且有較高權限的群組，或是關鍵性系統，例如受信任的網域控制器、生產伺服器或儲存敏感性資料的資料庫等等。AD 包含了攻擊者要擴大存取範圍、建立持續性潛伏、提升權限、進行橫向移動和識別攻擊目標所需的資訊。

Active Directory 的安全性通常非常難以維護，因為除非企業組織進行詳盡的審核，否則許多曝露的風險是不容易被發現的。藉由識別關鍵性的 AD 所曝露的風險，並對會鎖定這些風險的攻擊發出告警，企業組織便能在攻擊者危害到其 AD 資料之前提高自身的安全。

偵測到的曝露風險：

- **危險的委派**
- **危險的信任**
- **AdminSDHolder 的不一致性**
- **DCShadow**
- **密碼噴灑 (Password Spray)**
- **其他曝險**

Attivo Networks ADAssessor 解決方案針對關鍵性網域、電腦和使用者等級的曝露風險提供持續性的能見度，以迅速修正這些弱點。且該解決方案會持續監控 AD，查看當中活動是否顯示正受到攻擊。

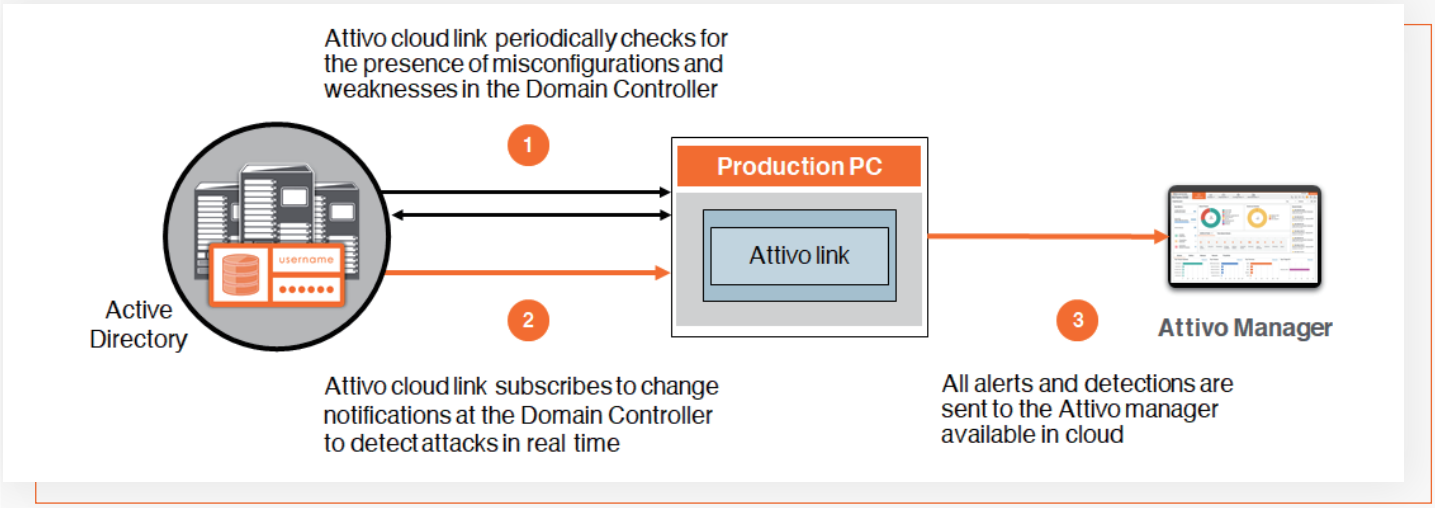
企業組織面臨的挑戰

- 大多數的企業組織會監控日誌中是否存在異常行為，但此舉並無法對 Active Directory 提供即時的評估，以於設定和政策的變更中偵測出可能會導致攻擊者利用的弱點。
- 當多重層級的 IT 團隊管理 Active Directory 時，有可能在不了解增加變更所可能造成曝露風險的情況下進行變更。
- 既有的安全控管措施不支援 AD，也無法偵測到來自暴力攻擊 (Brute Force Attack)、DCsync、DCshadow 和類似攻擊策略的大規模變更。

ADASSESSOR

ADAssessor 解決方案是一個獨立的產品，能針對易受攻擊的 AD 曝險提供持續性的能見度，並即時偵測出進階的 Active Directory 攻擊。該解決方案與 Attivo Networks ADSecure 解決方案協作提供先進的 Active Directory 防護。

一旦企業組織部署了 ADAssessor，它就能偵測出其 AD 環境當中的弱點，包括不當的設定 (Misconfiguration)、過多的權限或是資料曝露的風險等。然後，它會在攻擊者能加以利用之前修正這些弱點，終至縮減 AD 的攻擊面和風險。ADAssessor 可以持續執行或是依需要執行，它會自動監控 AD、分析變更，並識別出可能是惡意活動的新曝險。



1. Attivo雲端連線會定期檢查網域控制器中是否存在不當的設定或弱點
2. Attivo雲端連線支援控制器上的通知變更，以實時檢測攻擊威脅
3. 所有告警和偵測都會發送到 Attivo雲端管理器

效益

- 針對 AD 安全基本防護(Security Hygiene) 問題提供能見度，並對網域、電腦和身份等級的主要曝險發出可採取行動的告警。
- 即時針對 AD 權限提升進行偵測，並對存取 AD 資訊提供精細化的限制，而不會影響到企業商務營運。
- 持續深入地了解與憑證、特權帳戶、老舊帳戶、共享憑證和身份攻擊路徑有關的身份和服務帳戶風險
- 易於部署：該解決方案從單一端點執行，而且不需要有 Active Directory 的存取特權。

有關Attivo Networks

Attivo Networks 是偵測橫向移動攻擊以及防止權限提升的領導者，提供一個能反制威脅活動的優越防禦體系。透過網路欺敵和其他戰術，Attivo ThreatDefend 平台是個獲得客戶實證易於擴展的解決方案，不依賴特徵的辨識就能拒止、偵測、破解攻擊者、縮小網路攻擊面。產品透過防止和誤導攻擊活動，在關鍵性的被攻擊點提供創新且有專利的防禦，包含在端點、Active Directory、雲端，並橫跨整個網路。犯罪現場證據保存、自動化攻擊分析，以及第三方資安工具的整合簡化事件回應。以欺敵為主的防禦策略不斷發展，其功能緊密地搭配 MITRE ATT&CK® 框架運作，是美國國家標準技術研究所特別出版 (NIST Special Publication) 和 MITRE® Shield 不可或缺的一部份。