FIREEYE™

產品型錄

Active Directory 安全評估

減輕 Active Directory 錯誤設定、過程缺陷和攻擊方法的風險

優點

- 瞭解組織的 Active Directory 環境的目前狀態
- 主動緩解經常利用的 Active Directory 錯誤組態和設定
- 透過強化通用攻擊面來降低資安事件的風險和影響
- 實施更嚴格的策略以最小化特權存取
- 在 Active Directory 環境中增加可見性和偵測
- 從戰略上改善 Active Directory 基礎設施的總體資安狀況

為何選擇 FireEye Mandiant

FireEye Mandiant 自 2004 年以來就站在網路資安與網路威脅情報的最前線。我們的資安事件回應團隊站在全球最複雜入侵事件的最前線。透過利用對手、機器和受害者的綜合情報資源，我們對威脅實施者及其快速變化的戰術、技術和程序 (TTP) 有著深刻的理解。

我們的 Active Directory 安全評估 (ADSA) 是基於廣泛的事件回應經驗、全球遏制和補救服務以及新興威脅情報而開發的。

從此評估中得出的實用指南和建議反映了經過測試和審查的技術，這些技術已成功從用戶端環境中消除了攻擊者並幫助解決威脅。

透過使用這種主動方法，組織可以增強其 Active Directory 安全狀況，並防止發生利用 Active Directory 環境中常見漏洞的事件。

概觀

Active Directory 非常複雜且難以維護，尤其是隨著技術和組織的發展。組織經常難以正確地維護設定並保持最新的 Active Directory 安全強化性。

在 ADSA 安全評估期間，Mandiant 幫助您的組織改善能有效保護 Active Directory 環境及其支援基礎結構所需的關鍵流程、設定標準、安全性和監視控制項。

我們的作法

Mandiant 專家與客戶組織的主要利益相關者協作，舉辦了一系列現場工作坊，以根據現有技術和流程執行資料進行收集和指令檔輸出分析。我們的專家使用此資訊來評估體系結構 (包括本機和基於雲端的環境)，並確定 Active Directory 基礎結構中可能存在的攻擊路徑。

Mandiant 的顧問建議了一些方法來強化特權使用者之存取和特權存取管理，增強 Active Directory 中惡意事件的可見性和偵測，並提供建議性戰略路線圖，以改善用戶端 Active Directory 基礎結構的總體資安狀況。

圖 1. 服務生命週期。

ADSA 重點領域

- 森林結構和信託
- 操作過程
- 監控與回應
- 特權帳戶和存取管理
- 群組政策控制和執行
- 權限委派
- 服務帳戶和服務主要名稱 (SPN)
- 遠端存取控制和強化
- 端點設定和強化
- 與 Microsoft Azure 和 Microsoft Office 365 整合

產出成果

評估結束時會提供一份詳細的報告，其中包括：

- 該環境的現有 Active Directory 資安設定的概觀快照
- 與目前技術和操作過程保持一致的特定 Active Directory 安全性之最佳實例做法
- 限制、管理和監視環境中特權使用者之存取權和帳戶的實用建議
- 進一步加強 Active Directory 基礎結構安全性的詳細建議

要知道更多關於 FireEye，請前往：**www.FireEye.com/services**

FireEye Taiwan | 台灣火眼有限公司
| 10683 台北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE /
taiwan@FireEye.com

關於 FireEye, Inc.
FireEye 是一間情報主導的資安公司。FireEye 以流暢、可擴充的客戶資安作業延伸，提供了混合創新資安技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平台。藉由此方法，FireEye 得以讓對於準備、預防及回應網路攻擊感到苦惱的組織，消除資安機制的複雜性和重擔。