tenable.ad

Tenable.ad 規格書

系統規格

硬 體 :

監聽端:

2Cores(2.6Ghz) /Memory:12GB/
Disk: 50GB

管理分析平台:

8Cores(2.6Ghz)/Memory:16GB/
Disk: 200GB

儲存資料庫:

8Cores (2.6Ghz)/Memory: 8GB/
Disk: 300GB(c:150/d:100/e:50 GB)

作業系統:

Windows 2016/2019英文版

產品特性

持續偵測並防止 ACTIVE DIRECTORY 攻擊

持續監控並偵測Golden Ticket、DCShadow、暴力密碼破解、密碼噴濺、DCSync 等Active Directory 攻擊。Tenable.ad 的攻擊洞察和剖析可使SIEM、SOC 或SOAR 更完善，以便企業能快速應變及遏阻攻擊

系統透過IOE(Indicators of Exposure):

- 找出Active Directory 設定中隱藏的所有弱點
- 搜尋威脅AD 安全的潛藏問題
- 用簡易方式剖析每個錯誤設定
- 每個問題都能獲得建議的修復方法
- 建立可管理AD 安全的自訂儀表板以降低風險
- 搜尋危險的信任關係
- 掌握AD 的所有變更

系統透過IOA(Indicators of Attack):

- 察覺您的AD 中正在進行的攻擊
- 從精準的攻擊時程將每個威脅視覺化
- 將攻擊資料合併於單一檢視畫面
- 建立AD 變更和惡意行動之間的關聯
- 分析AD 攻擊的深入詳細資訊
- 直接根據資安事端瞭解MITRE ATT&CK ®框架的說明

產品優勢

- 無需代理程式、無需特殊權限、沒有延遲。

  無需代理程式和特權即能預防並偵測精密的Active Directory攻擊。
- 涵蓋雲端

  即時檢查Azure Active Directory 網域服務、AWS Directory Service 或Google Managed Service for Active Directory 的安全。
- 任何地點都能部署

  Tenable.ad 提供了有兩種架構設計的彈性。內部部署讓資料保存在企業內部，並且在您的掌控之下。SaaS 則能讓您充分運用雲端。