
tenable.ad
#ADSEC
>_Harden. Detect.
Respond.

tenable.ad

Active Directory (AD) 已成為竊取公司重要資產攻擊者的首要目標。

業界錯誤地將高階攻擊假設為從組織外部開始，然後透過網路和端點，最終到達您的資料和重要資產的攻擊流。

遺憾的是，這忽略了一個無處不在的、功能強大的監管程式，它負責協調 IT 基礎架構中的一切：這就是 Active Directory。IT 安全專家對它漠不關心，然而攻擊者卻非常重視它。

95% >_ 財富 1000 大企業使用 Active Directory

100M >_ 安全決策每天都是由大型目錄基礎架構處理

85% >_ 的管理層人員承認管理 AD 的安全模型遇到困難

10% >_ 的年營業額等於網路安全解決方案的平均成本，這一比例還在增加

80% >_ 國際企業受到稽核

25 >_ 有嚴重的錯誤配置

95% >_ AD 配置有漏洞

它為什麼這麼重要

Active Directory 的基礎架構是保障您的公司安全的關鍵。使用者憑證、收件箱、企業資料和財務資料，它們都由該基礎架構管理，而且這種基礎架構也相當於連接到您公司網路系統的萬能鑰匙。

然而，AD 的設計使其易於存取，且暴露在嘗試入侵您的企業網路的攻擊者面前。只需利用一個漏洞，就能威脅到整間公司的安全。

>_ Magellan Health
2020 年 4 月

>_ Cognizant
2020 年 4 月

>_ 世界衛生組織
2020 年 3 月

>_ 聯合國
2020 年 1 月

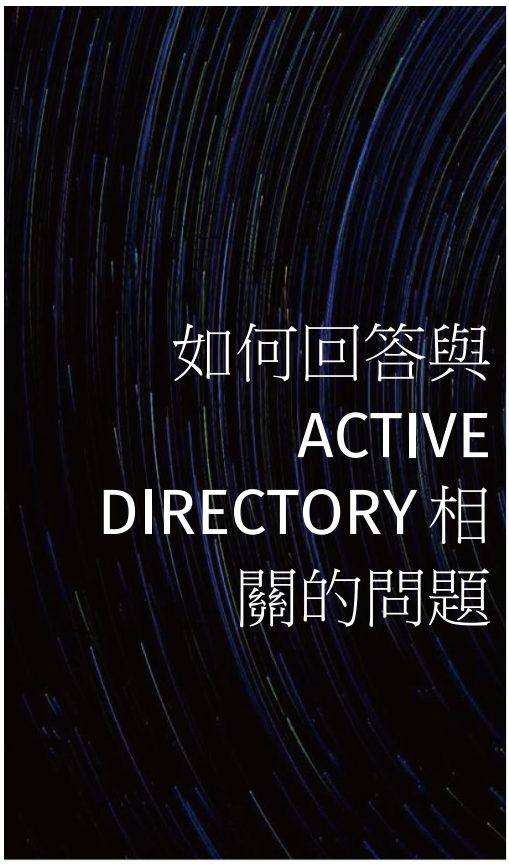
>_ 巴爾地摩
2019 年 6 月

>_ Norsk Hydro
2019 年 3 月

>_ SingHealth
2018 年 10 月

為什麼現有的防禦方案無法奏效

- 大多數安全工具的作用主要是偵測進攻，而非強化您的 AD 基礎架構的配置安全度，因此無法真正做到首先阻止進攻。
- AD 基礎架構很複雜，且也不斷改變中。它有數千條可並存執行的規則，這會讓看起來無關緊要的錯誤配置在幾分鐘內就產生許多重大漏洞。



如何回答與 ACTIVE DIRECTORY 相關的問題

1. 目前的 AD 基礎設施安全嗎？
2. 當做出配置改變，是又創造另一個攻擊 AD 的途徑嗎？
3. 如何發現及矯正 AD 中的錯誤配置？
4. 有人正在攻擊您的 AD 嗎？
5. 如果您懷疑正遭受攻擊，您如何調查發生了什麼？
6. 如果受到攻擊，是不是有人製造了「後門」並稍後再來？

Active Directory 安全性遇到的問題

1.存在大量的弱點可被利用

- 經過多年的發展和重組，AD 可能存在數百個隱藏的弱點和攻擊途徑
- 也是橫向移動的機會

2.不斷湧現新的攻擊途徑

- 在大型組織中，每天都會出現多種新的攻擊途徑。
- 複雜的威脅參與者只需要短短 17 分鐘的時間，即可完成從最初的感染到控制網域。

3.數十年無效的偵測技術

- 一些最惡毒的攻擊（例如，DCSync 和 DCShadow）會留下零追蹤，無法被傳統基於日誌和代理的偵測策略捕獲。

4.事故回應的噩夢

- Active Directory 會建立大量的日誌，消除這種雜訊消耗會導致事件回應和威脅搜尋資源。當分秒必爭變得很重要時，複雜性就是您的敵人。

二十年 AD 安全基礎未變

80% 的攻擊會使用 AD 執行橫向移動和權限提升

60% 的新惡意套裝軟體包含針對 AD 錯誤配置的特定程式碼

針對大型企業的大規模勒索感染增加 — AD 是惡意軟體的主要設計攻擊行為

針對大型企業的大規模勒索感染增加 — AD 是惡意軟體的主要設計攻擊行為

TENABLE.AD 重塑 AD 的安全性

Tenable.ad 能鞏固您的 AD 基礎架構，強化您的安全營運中心 (SOC) 對 AD 的威脅偵測能力，讓您的事件回應和威脅搜尋團隊能調查與 AD 相關的威脅。這些功能無需安裝代理和特權。

找出並修復現有的漏洞

>_ 立即探查、瞭解和記錄現有漏洞

>_ 按照我們的分步修復策略來執行，阻止攻擊

發現攻擊路徑

>_ 立即偵測出新的漏洞和錯誤配置

>_ 阻斷攻擊路徑，控制好威脅

即時偵測攻擊

>_ 獲得有關 AD 攻擊的即時警報和可行的解決方案

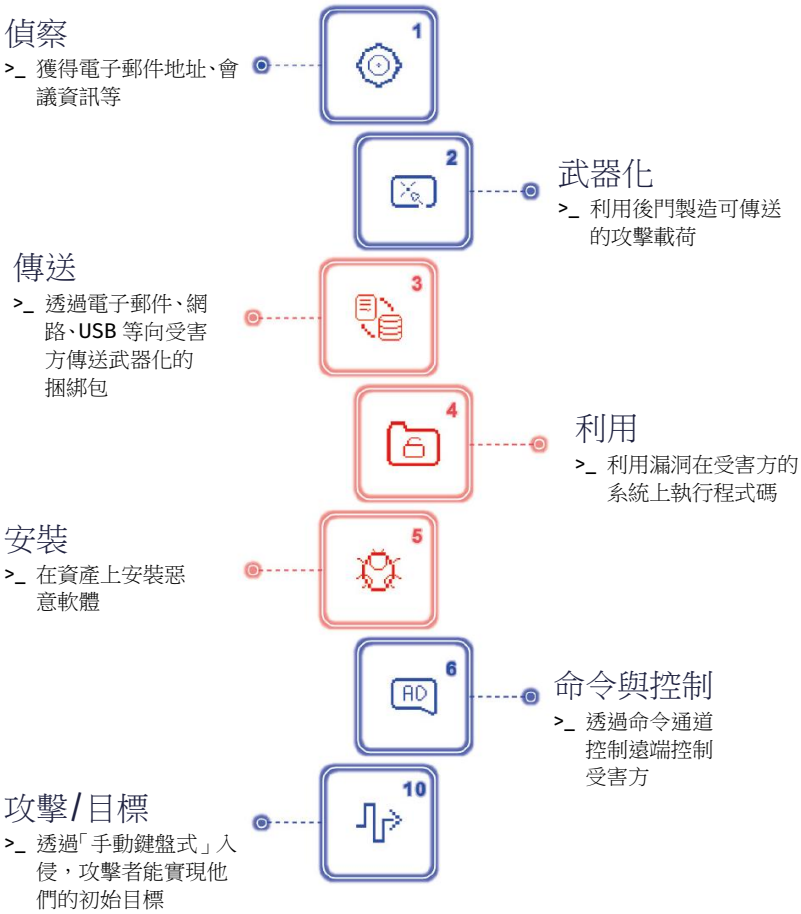
>_ 在您的 SIEM/SOAR/SOC 中視覺化通知並觸發回

調查事件和威脅

>_ 深入研究最完整的 AD 威脅追蹤軟體

>_ 在物件層和屬性層搜尋和關聯 AD 的變化

使用 TENABLE.AD 阻止 APT 攻擊殺傷鏈



傳送

阻止 — Tenable.ad 可識別會被利用的傳送方法並即時通知 SOC 團隊預先防堵。

偵測 — Tenable.ad 可即時偵測進行中的傳輸，以便立即減輕和解決威脅。

回應 — Tenable.ad 發出的警告和指標能讓 IR 團隊掌握根本原因，為暴露後的回應和增強各個過程提供指導。

利用和安裝

阻止 — 無論是錯誤配置，或是軟體有漏洞，Tenable.ad 都 能指導 SOC 團隊改進 AD，避免漏洞遭他人利用。

偵測 — Tenable.ad 擁有市場上最大的偵測平台，能發現 進行中的漏洞攻擊，並以機器速度觸發解決機制。

回應 — Tenable.ad 的詳細建議能協助 AD 管理員掌握被攻擊 物件和不合規伺服器的管理流程，並整體增強其基礎設施。

tenable.ad

保障 Active Directory 安全性並阻斷攻擊路徑

根據以往的經驗，每一條因資料外洩所致的頭條新聞報導的背後，都有一個脆弱的 Active Directory (AD)。80% 的攻擊會利用 AD 進行橫向移動和提權；而 60% 的新惡意軟體都含有利用 AD 錯誤配置的程式碼。AD 已成為攻擊者最喜歡的攻擊目標，透過利用已知瑕疵和錯誤配置，攻擊者就能提權並進行橫向移動。不幸的是，由於 AD 複雜度增加而造成的錯誤配置越積越多，大多數企業很難保證 Active Directory 的安全性，讓安全團隊無法在這些瑕疵成為影響業務安全的問題之前將其找出並修復。Tenable.ad 能讓您洞察 Active Directory 的一切變化，預測哪些異常或漏洞存在影響最大的風險，讓企業在攻擊者利用漏洞之前就阻斷其攻擊路徑。

保障 Active Directory 安全所面臨的挑戰

每間公司的 Active Directory (AD) 不斷發生的配置變化會限制對 AD 攻擊面的可見性，並常會導入新的攻擊路徑。很少有安全團隊擁有足夠的可見性和脈絡來探查和修復 AD 錯誤配置和漏洞。

安全人員的努力常常事半功倍。大多數 AD 的規模和複雜性使得手動監控不切實際，且無法做到即時偵測攻擊。事件回應和威脅搜尋受到阻礙，因為團隊無法看到所有隱藏的錯誤配置和相互關聯的關係。

Active Directory 安全性不足的後果

成功的入侵行為通常伴隨著對 Active Directory 的攻擊，以提權、橫向移動、安裝惡意軟體和竊取資料。因為攻擊者在 Active Directory 內的移動被偽裝成遵循現有的安全政策，所以他們能成功在日誌和其他監測工具中隱藏這些行為。當攻擊者成功竊取資料、勒索、破壞網路環境以至於影響公司聲譽時，這一切造成的損失都要算在不安全的 AD 系統頭上。

使用 TENABLE.AD 持續監測和預防 ACTIVE DIRECTORY 攻擊

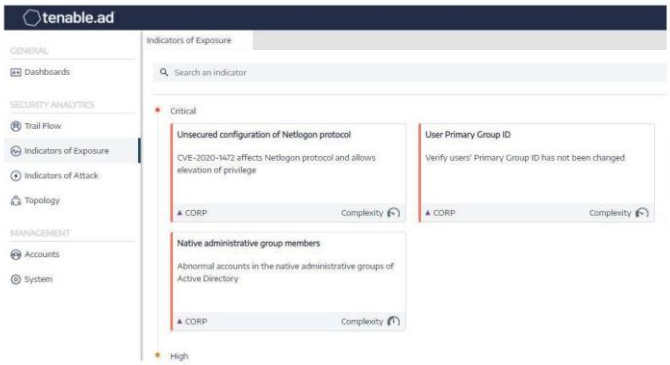
- 在 Active Directory 配置中找出所有隱匿的漏洞
- 探查威脅 AD 安全的基礎問題
- 用簡單的術語對所有錯誤配置進行深度分析
- 對所有問題提供修復建議
- 建立自訂資料儀錶板來管理 AD 安全性資料，藉此降低風險
- 識別危險的信任關係
- 掌握 AD 中的每一個變更
- 發現針對 AD 的所有攻擊
- 以正確的攻擊時間線展示各種威脅
- 將攻擊資料集合到單一視圖中
- 將 AD 變更和惡意操作相關聯
- 深度分析 AD 攻擊的詳細資訊
- 直接從事件詳細資訊中探索 MITRE ATT&CK® 說明

Tenable.ad 保障 Active Directory 的安全並阻斷攻擊路徑

Tenable.ad 擁有主動和基於風險的 AD 安全保障功能，讓您洞察所有漏洞，預測攻擊者會利用哪些路徑，並採取行動來偵測、阻斷和防止攻擊。

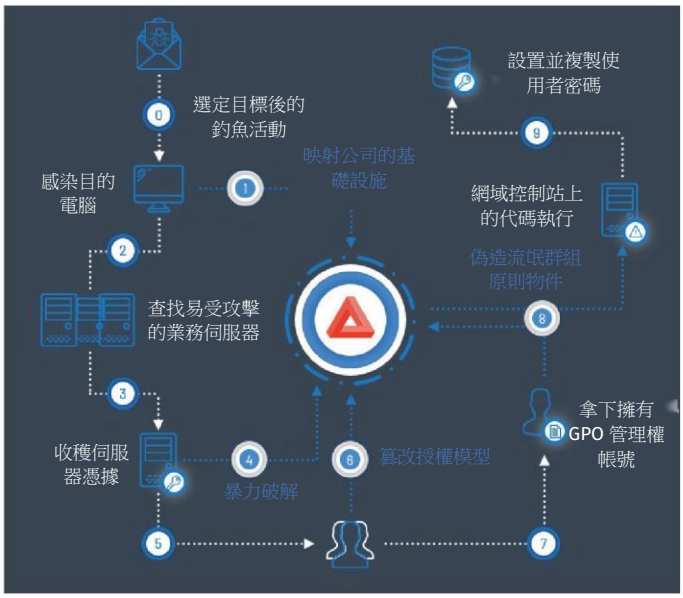
在攻擊發生前先找出並修復 Active Directory 漏洞

在您現有的 Active Directory 網域中探查漏洞並進行優先順序的排序，以及按照 Tenable.ad 的步驟修復指南減少風險暴露。透過加強 Active Directory，您能夠阻止攻擊者攻擊，阻斷他們的移動企圖，確保減少導致權限提升、橫向移動和惡意軟體執行的漏洞。



即時監測和回應 Active Directory 攻擊

持續監測 Active Di rectory 攻擊，如 Golden Ticket、DCShadow、 Brute Force、Password Spraying、DCSync 等。Tenable.ad 利用攻擊洞察豐富您的 SIEM、SOC 或 SOAR，因此您可以快速回應並阻止 攻擊。自動人。攻擊偵測能減少網路安全團隊的監測壓力，讓他們 有更多的時間處理其他重要事務。



從本機到雲端，無論您的 Active Directory 擴展到何處，靈活、羽量級的部署均可保障 Active Directory 的安全性。

- **無代理。無特權。無延遲。**

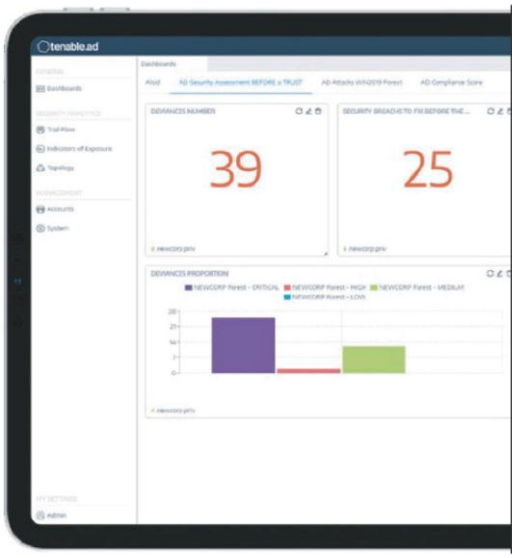
  在無代理和特權的情況下預防和偵測複雜的 Active Directory 攻擊。

- **涵蓋雲端**

  即時檢查 Azure Active Directory Domain Services、AWS Directory Service 或 Google Managed Service for Active Directory 的安全性。

- **在任何地方部署**

  Tenable.ad 提供兩種靈活的架構設計。本機部署可將您的資料保留在現場並置於您的控制之下。SaaS 可讓您利用雲端。



客戶信任 TENABLE.AD

「Tenable.ad 的整合能力非一日之功，它還提供了最底層基礎設施的高效安全監控，並且不會影響網路安全團隊的工作量。」
Thierry Augier
Lagardère 副資訊長和副資訊安全長

「Tenable.ad 的解決方案讓我們不再擔心 Active Directory 的安全問題，以便我們能關注新業務整合。」
Dominique Tessaro
VINCI Energies 資訊長

「Tenable.ad 為所有資訊安全長應該經常問的兩個問題給出了答案，這兩個問題分別是：我的網域夠不夠安全？我該如何獨立地證明這一點？」
Jamie Rossato
Orica 資訊技術和網路安全副總裁

AIRBUS HELICOPTERS · orange · HONDA · SAINT-GOBAIN · RENAULT · SINGAPORE AIRLINES · sky · Westpac · MICHELIN · LVMH · UNIBAIL-RODAMCO-WESTFIELD · SmarTone · BHP · NHS · ORICA · sodexo · ALTRAN · Lagardère · SPgroup · MMG · BNP PARIBAS · SAFRAN · SANOFI · POS MALAYSIA · noble group · INVESTMENT MANAGERS · VINCI ENERGIES · TOYOTA · somfy · HKT · 香港寬頻 · FINTECH · EURO INFORMATION · ORPEA GROUPE

提供 AD 基礎設施的即時攻擊面視覺化

1.找到並修復現有 AD 暴露風險

- 立即發現、繪製和評分現有的 AD 風險
- 遵循我們的逐步補救策略以避免攻擊

AD 管理員 · 藍隊 & 稽核團

2.發現新的攻擊路徑

- 不斷發現新的漏洞和錯誤配置
- 打破攻擊通道，控制您的威脅暴露

AD 管理員 · SOC 分析團隊

雲端化部署 & 私有化部

3.調查事件和回溯威脅

- 在物件和屬性級別搜尋和關聯 AD 配置變更
- 在您的 SOAR 觸發反應

SOC 分析團隊 · 攻擊溯源團隊

4.事故回應的噩夢

- 獲得有關 AD 攻擊的警報和可採取行動的補救計畫
- 協助 SOC 團隊在 SIEM 中視覺化通知和警報

事件回應 · 攻擊溯源團隊

無需安裝 Agents

不需要高級權限

即時分析

AD 原生 API 對接

關於 Tenable

Tenable , Inc 是一間 Cyber Exposure 公司。全球超過 30,000 間企業客戶（包括 54% 的財富 500 大企業、超過 30% 的 Global 2000 大公司）正透過 Tenable 多維度、全方位的持續安全風險視覺化解決方案，協助他們瞭解 IT/OT 安全態勢，降低網路安全風險，提升資訊安全應變能力。

欲瞭解更多資訊：請瀏覽：zh-cn.tenable.com
聯繫我們：請傳送電子郵件至 sales@tenable.com
或瀏覽 zh-cn.tenable.com/contact