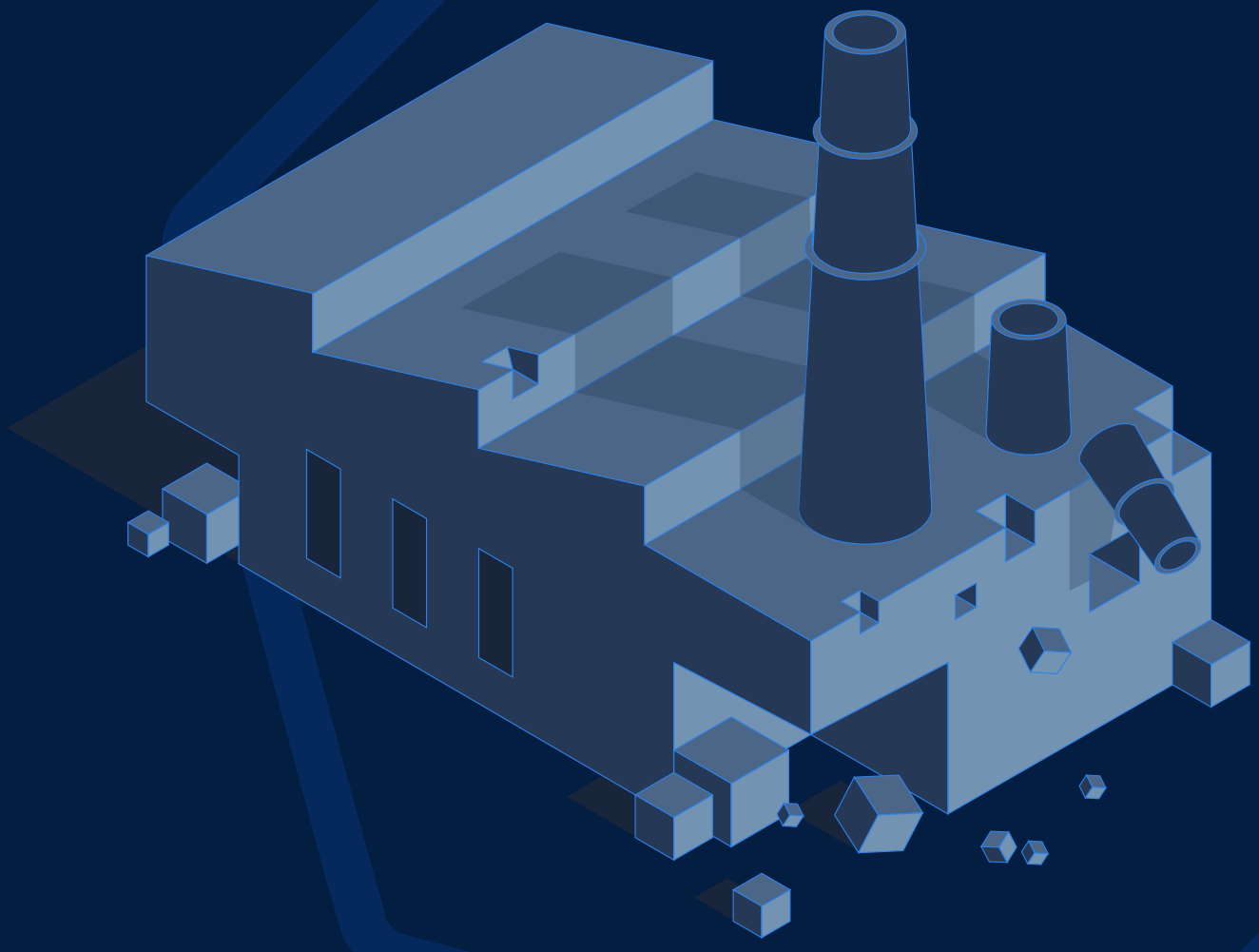
tenable.ad

企業面臨的全球風險：

ACTIVE DIRECTORY 攻擊造成的影響



無論您的職務是執行長、財務長、行銷長或任何其他非 IT 管理職，您是否聽過 Active Directory (AD)？事實上，您無時無刻都在使用它。當您登入裝置、開啟電子郵件、存取應用程式或共用檔案時，都會使用到 Active Directory。它是建立 IT 基礎架構的基石。

本指南可協助您瞭解當這個重要的 IT 支柱被破壞時會有什麼後果。有些人甚至認為這是不可能發生的超現實情節。說不定這只是幻想喪屍啟示錄的情節能夠成真的資安怪咖的臆想實驗。

我們有幸撰寫了這份文件，祝您閱覽愉快。

高度風險

身為 IT 基礎架構的全域協調器，Active Directory 的設計是單一失敗點。另一方面，Active Directory 樹系則隨著企業的組織結構、業務架構及合併與併購案而不斷發展。因此，就構建而言，Active Directory 就是安全機制快速惡化的異類系統。

話雖如此，這個脆弱環節位於中央導致的企業層級真正風險到底是什麼？

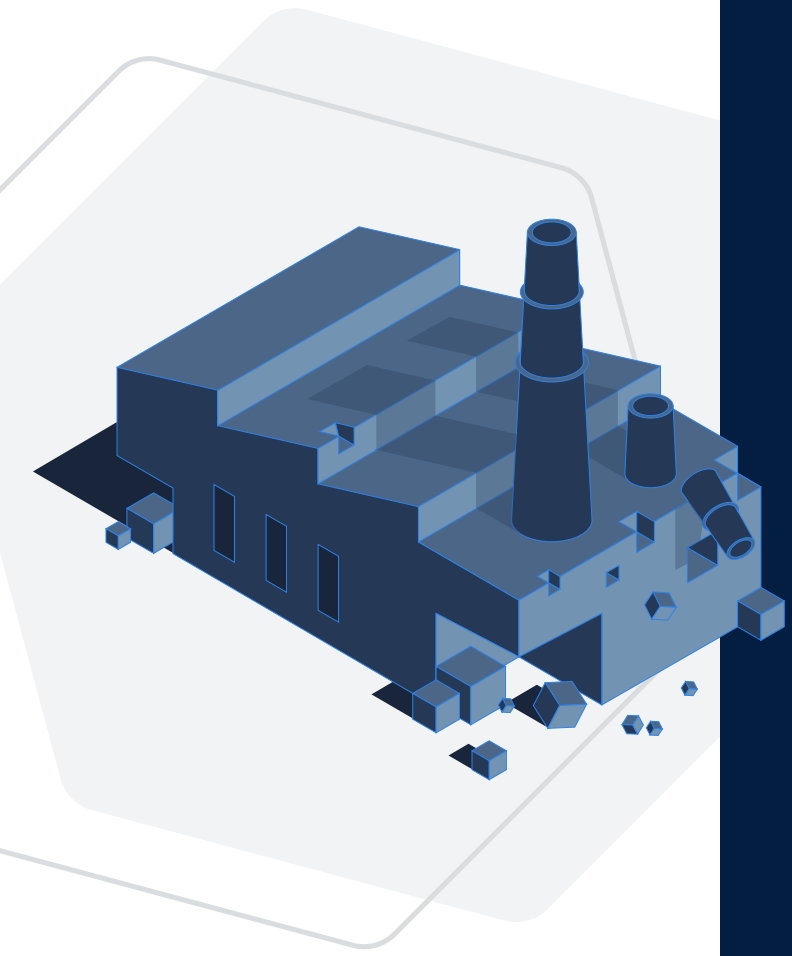
業務 (不) 連續性

這是 Active Directory 不安全性對產業和企業所造成的最顯著威脅。工廠停工、飛機停飛、員工無法存取電子郵件… 讓企業的業務停擺並不是 007 電影中的情節，也不是過度焦慮的資安專家的惡夢。

駭客有兩種惡意利用 Active Directory 的手段，這些手段最會造成業務受到重大衝擊：

- **讓 Active Directory 本身陷入癱瘓。**攻擊者可暗中破壞企業 IT 的基礎，進而造成使用者和應用程式無法登入系統及存取所需資源。這種戰術也許看似游擊戰，但也還是有一些充分記載、雖說應對略嫌不足的程序可供駭客使用，讓他們得以在全新基礎架構重建之後，依舊持續存在於受害者的 AD 中。尋找、摧毀、重複。

- **利用 Active Directory 傳送具破壞性的惡意軟體。**破壞性惡意軟體並不是什麼困難的高科技。像 Stuxnet 這樣高度精密的承載例外，如今的消費性勒索軟體已經足以有效進行毀滅工作。那些攻擊中的唯一挑戰是分散：必須讓這種惡意軟體安裝在數量夠多的端點上，大規模復原才會變得不可行。就這方面來說，駭客若想在基礎架構中橫向移動，利用 Active Directory 弱點是唯一的可行選擇。近年癱瘓生產環境功能的每一起大規模基礎架構攻擊的核心中，都有一個 Active Directory 弱點。



案例：

2020 年 12 月：全球軟體公司 SolarWinds 發生重大入侵事件。該公司的網路及基礎架構被滲透，導致旗下平台 Orion 遭到入侵。當時的存取讓攻擊者趁機開始散布混入惡意軟體的更新，傳送給終端使用者。

2019 年 12 月：美國管線成為勒索軟體攻擊的目標，攻擊者滲透設施網路的 IT 區段，擴大控制後進入企業的操作技術 (OT) 部分。結果，天然氣壓縮設施被迫停擺兩天。

2019 年 12 月：全球公司 Travelex 被 Sodinokibi 勒索軟體攻擊，迫使該公司暫停所有系統。結果，客戶無法使用 Travelex 應用程式及網站付款或交易。

2018 年 3 月：Norsk Hydro 旗下管理工廠設備的系統遭到 LockerGoga 加密及中斷連線，被迫改為人力作業。Hydro 官方曾表示，本次資安事端相當嚴重。

2017 年 12 月：法國公司 Schneider Electric 旗下的工業控制系統遭惡意軟體入侵，被迫關閉中東一處電廠的運作。資安研究人員的分析顯示，本次攻擊是一個民族國家發起。

2017 年 6 月：NotPetya 勒索軟體的一次攻擊使丹麥貨運巨擘 Maersk 的多座港埠停擺二天，因此產生的相關支出估計達 3 億美元。

2011 年 4 月：Sony 的 PlayStation Network 遭到協同攻擊，使服務停擺一個月，估計損失達 1.71 億美元。

品牌受損及客戶信任

在今日的網路犯罪造成的損害中，上述是目前最明顯的。個人識別資訊 (PII) 外洩幾乎每週都躍上新聞頭條，大眾的反應也因此傾向變得…… 焦慮。

2016 年初期，經濟學人智庫的一份調查訪問了 282 位公司高層成員所關心的網路安全議題：「公司對客戶的商譽」高居第一。有鑑於品牌是一間公司的重要保護傘，也難怪調查結果如此。品牌受損會產生漣漪效應，衝擊該品牌的所有產品與服務。此外，大眾資料外洩時常引來多年的客戶及股東訴訟。

這些事件都會受到廣泛報導，反覆損害品牌和產品。

資料外洩與中斷業務攻擊相反，並非每次都需要有效的 Active Directory 入侵…… 只不過經常如此，而且會因為入侵是否需要深度入侵基礎架構而異。

案例：

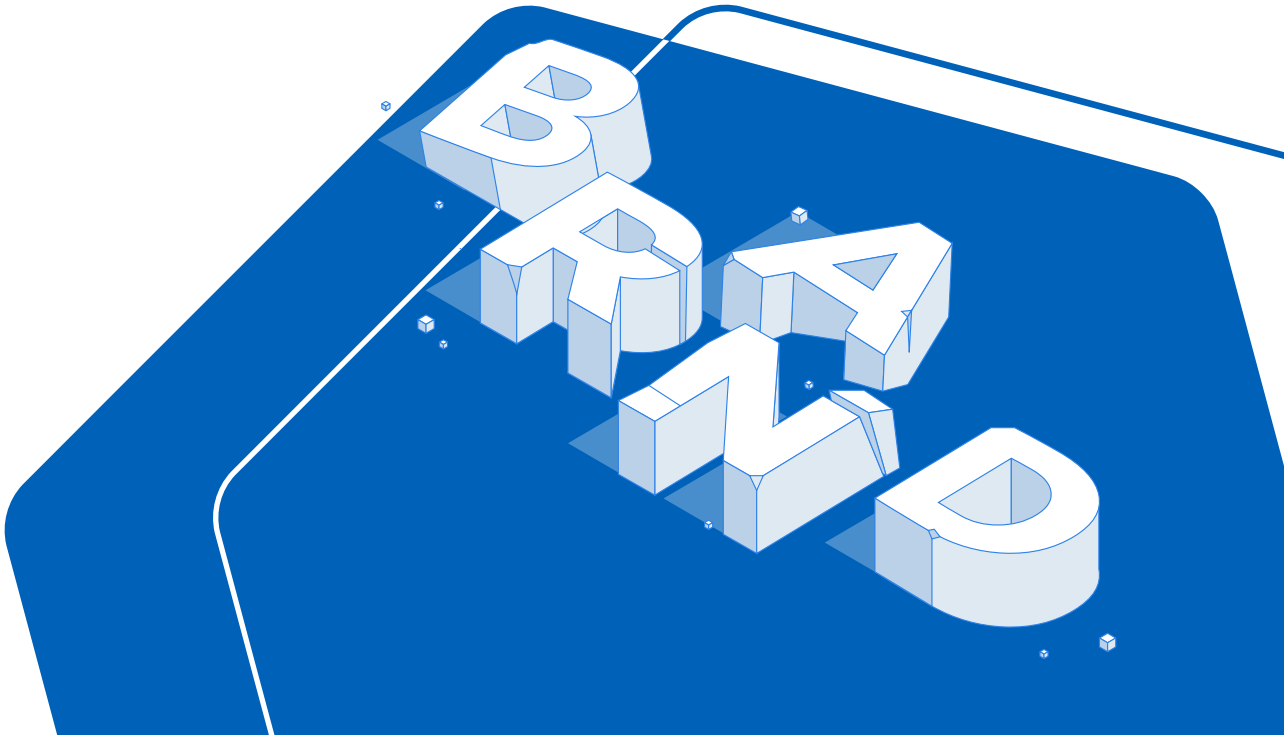
2020 年 12 月：Egregor 勒索軟體攻擊了 Kmart，為這個已經舉步維艱的品牌帶來更多混亂。

2020 年 3 月：聯合國的三個地區辦公室共 42 台伺服器遭到入侵，影響到 3,000 至 4,000 位聯合國工作人員。

2018 年 9 月：SingHealth 的基礎架構遭到入侵，影響 150 萬筆個人紀錄，以及 16 萬名病患的處方細節，新加坡總理李顯龍先生的資料亦在其中。

2014 年 11 月：索尼影業遭到入侵，資料被惡意軟體刪除，駭客在網路上張貼員工的個人資料與未釋出的影片。FBI 調查顯示，該攻擊的幕後主使者為北韓。

2014 年 3 月：網路罪犯從 Target 竊取了 4 千萬筆信用卡號碼，更有 7 千萬個帳戶遭到入侵。



失去競爭力與智慧財產遭竊

在步調快速的創新導向數位世紀中，智慧財產 (IP) 是一間大型企業的血肉與靈魂。智慧財產失去控制不僅有損顏面，更會直接威脅到企業的存續。

一般來說，科技業的藍圖與產品在公開發布幾個月之前便設計完成，讓 IP 竊賊有足夠先機，能搶先填補技術缺口，使競爭優勢失效。在重要的國家產業中，IP 遭竊會產生任何大型企業都不願在旗下紀錄中見到的地緣政治後果。最後，遺憾的是，媒體與電玩產業如今已經習慣見到旗下的 AAA 級產品在進入電影院及商店之前，就已被洩漏。

隱密外洩這些資料仍是駭客工作中最簡單的一部分，但並非最瑣碎的。駭客真正的挑戰在於一開始就能夠存取資料，因為在初次感染之後，攻擊者鮮少能存取自己覬覦的資產。若想找出有價值的資料，就需要擁有來去不同系統的能力，直到繼承或模擬出適當的存取權。目前只有一個方法能辦到這點，也就是利用 Active Directory 的弱點。

案例：

2010 年 1 月：極光行動是針對數十間科技公司的一連串攻擊，包含 Google、Adobe、Juniper、Yahoo、Symantec、Northrop Grumman、Morgan Stanley、Dow Chemical。

2014 年 11 月：索尼影業遭到入侵，資料被惡意軟體刪除，駭客在網路上張貼員工的個人資料與未釋出的影片。FBI 調查顯示，該攻擊的幕後主使者為北韓。

(網路) 內線交易

這類網路犯罪活動因為其本質而難以量化，不過近期多份實證研究發現，股價下跌與宣布發生外洩之間有強烈的關聯性。涉及網路內線交易的駭客集團可分為二種不同類別：

- 駭客交易者竊取未公開資料，據此進行交易，進而在自由市場中取得不公平的優勢。值得注意的案例就涉及了大規模竊取即將揭露的收益報告 (美國證券交易委員會案例，見下文)，或是大型企業或投資銀行併購計畫的初步跡象。

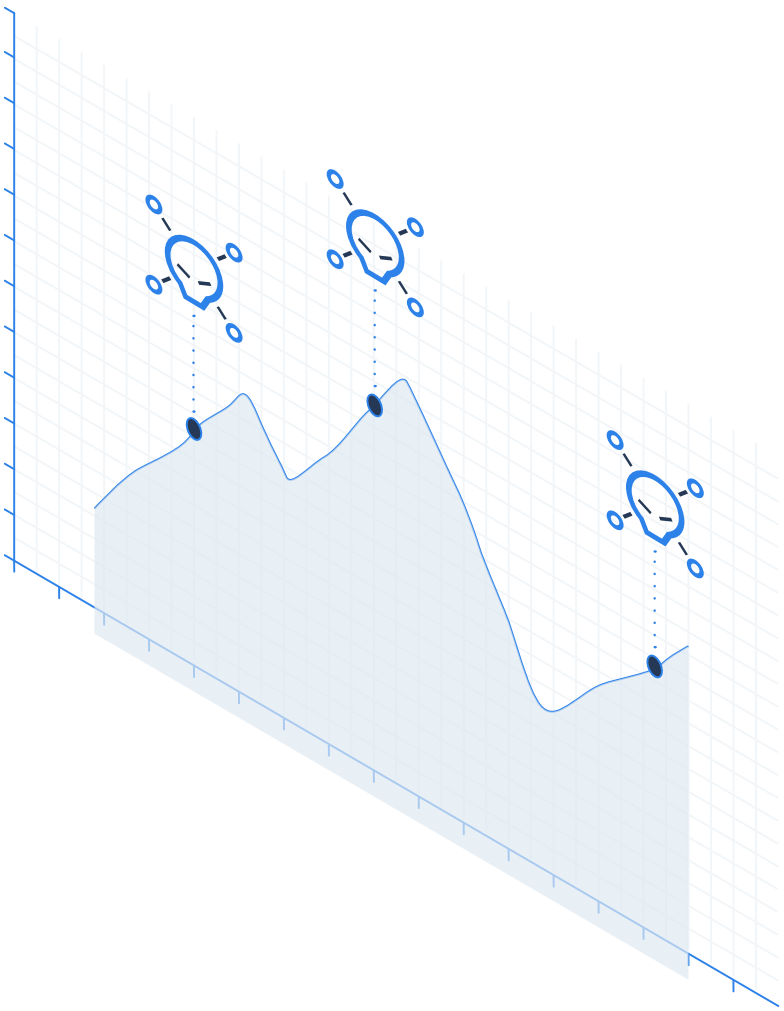
- 傳統的網路罪犯預期，受害公司的股價在揭露攻擊後將會下跌，因此加入了交易的做法，藉此提高發動攻擊的投資報酬率。

對於其他惡意軟體導向的網路犯罪來說，利用 Active Directory 仍是駭客唯一的有效手段，如此才能在企業的 IT 內部移動，直到取得目標資料的存取權。

案例：

2019 年 1 月：美國證券交易委員會 (SEC) 起訴了一群來自美國、俄國、烏克蘭的駭客，原因是他們 2016 年入侵了 SEC 的線上公司申報入口網站，利用未公開資訊進行交易。

2014 年 12 月：FIN4 網路犯罪集團被發現駭入了超過 100 間公司、投資顧問公司、律師事務所，尋找足以撼動市場的交易資訊，消息來源為網路安全公司 FireEye 的研究人員。



直接的財物損失與股價

我們的產業如今擁有幾十年的網路勒索、破壞、竊案參照點。這段歷史至少有一個好的方面：攻擊造成的直接、立即財務支出已成為文獻充足的研究領域。

網路資安事端造成大型企業與股東直接且立即損失金錢的情況包含四方面：

- **股價突然下跌**
- **違法處分與起訴**
- **金錢掠奪**
- **IT 修復支出**

如上文解釋，針對 IT 基礎架構的大規模攻擊，某些時候若不利用一些 Active Directory 弱點，就無法成功。因此，上述損失都跟這項關鍵基礎架構不安全有關。

IT 修復支出本身依照 Active Directory 在資安事端之後的狀態而異，有可能巨幅成長：如果完全被入侵，那麼修復就真的會是全新基礎架構環境的重建，實際情況也常是如此。痛苦的重建過程通常得動員數十位員工及專業承包商，有時甚至需要數百人在夜間及週末重建整個架構，代價極大。

案例：

2020 年 4 月：全球 IT 系統整合商 Cognizant 遭到 Maze 勒索軟體攻擊。Security Magazine 事後報導，Cognizant 的第 2 季營收結果預計將損失 5 千萬至 7 千萬美元。

2018 年 1 月：日本的加密貨幣交易公司透露，一次入侵事件使該公司損失價值 5.3 億美元的 NEM 加密貨幣，可能成為史上最大的加密貨幣劫案。

2017 年 12 月：SoftBank 收購 Uber 約 15% 的股份。Uber 發生大規模客戶資料外洩 (且應對失當) 之後，上述交易評估 Uber 市值約 480 億美元。外洩事件發生的一個月前，Uber 的市值曾高達 680 億美元。市值下跌 30% 並非全是因為資料外洩，但是分析師認為這是重大因素。

2017 年 6 月：Yahoo! 發生兩次受到高度關注的外洩之後，身價預估下跌 3.5 億美元。之後，Verizon 以 44.8 億美元收購 Yahoo! 的營運業務。

2014 年 9 月：Home Depot 的 POS 系統受到攻擊，5,600 萬筆客戶的信用卡/簽帳金融卡資訊外洩。2016 年 3 月時，該公司同意支付 1300 萬美元償還購物者自行負擔的損失，並且花費至少 650 萬美元資助 1.5 年的持卡人身分保護服務。該公司因為外洩產生了總計 1.61 億美元的稅前支出。

2013 年 12 月：Target 的 POS 系統發生大規模外洩，造成多達 1.1 億人的信用卡/簽帳金融卡資訊和/或聯絡資訊遭竊。Target 的資訊長於 2014 年 3 月辭職，執行長於同年 5 月辭職。該公司估計，外洩造成的支出達 1.62 億美元。

掌握 Active Directory 安全

普遍而言，資安業界早期因應這項威脅的方式並不完美。不過打贏這場戰役也不是不可能。打擊 Active Directory 相關的網路犯罪如今已成為結構完整的研究領域，也產出了實際的風險緩解策略。

最佳做法

許多受信任的來源都說明了企業應該依循的最佳做法，以便強化與保護 Active Directory。其中最值得注意者為：

- **Microsoft：**https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- **NIST：**https://nvd.nist.gov/ncp/checklist/669
- **ANSSI：**https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory

這些建議將確保貴企業面對 AD 安全問題時，依循嚴謹的安全機制，減少暴露在上述風險中的程度。不過，若要偵測滲透貴公司強化後基礎架構的持續攻擊，上述建議無法 (或者只能稍微) 提供幫助。

即時監控

使用工具稽核 Active Directory 可辨識組態問題，但是稽核資料很快就會過期，結果必須持續監控 AD，以確保立即偵測出潛在威脅與入侵。

由於威脅態勢一直在改變，從 Active Directory 收集而來的事件應該參照威脅情報摘要進行分析，以確保發生問題時立即標記，並通知 IT 工作人員。遺憾的是，若缺乏專業化工具，這個方法難以實現。若分開來看，資安與 Active Directory 的人才庫已經相當貧瘠。聘請同時具備兩大領域技能的專業團隊幾乎是不可能的。考量到這點，若想大規模監控 Active Directory，唯一可行的解決方案是使用能夠組合專精於 AD 情報摘要與本機紀錄的專業化技術。

我們進行了一些深入分析，說明如何選擇合適的 AD 導向資安解決方案，不過這部分容我們之後再另文討論……

tenable.ad™

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

北美地區 +1 (410) 872-0555

zh-tw.tenable.com