tenable.ad™

必不可缺：

確保您的 SOC 能夠警覺身分問題

白皮書

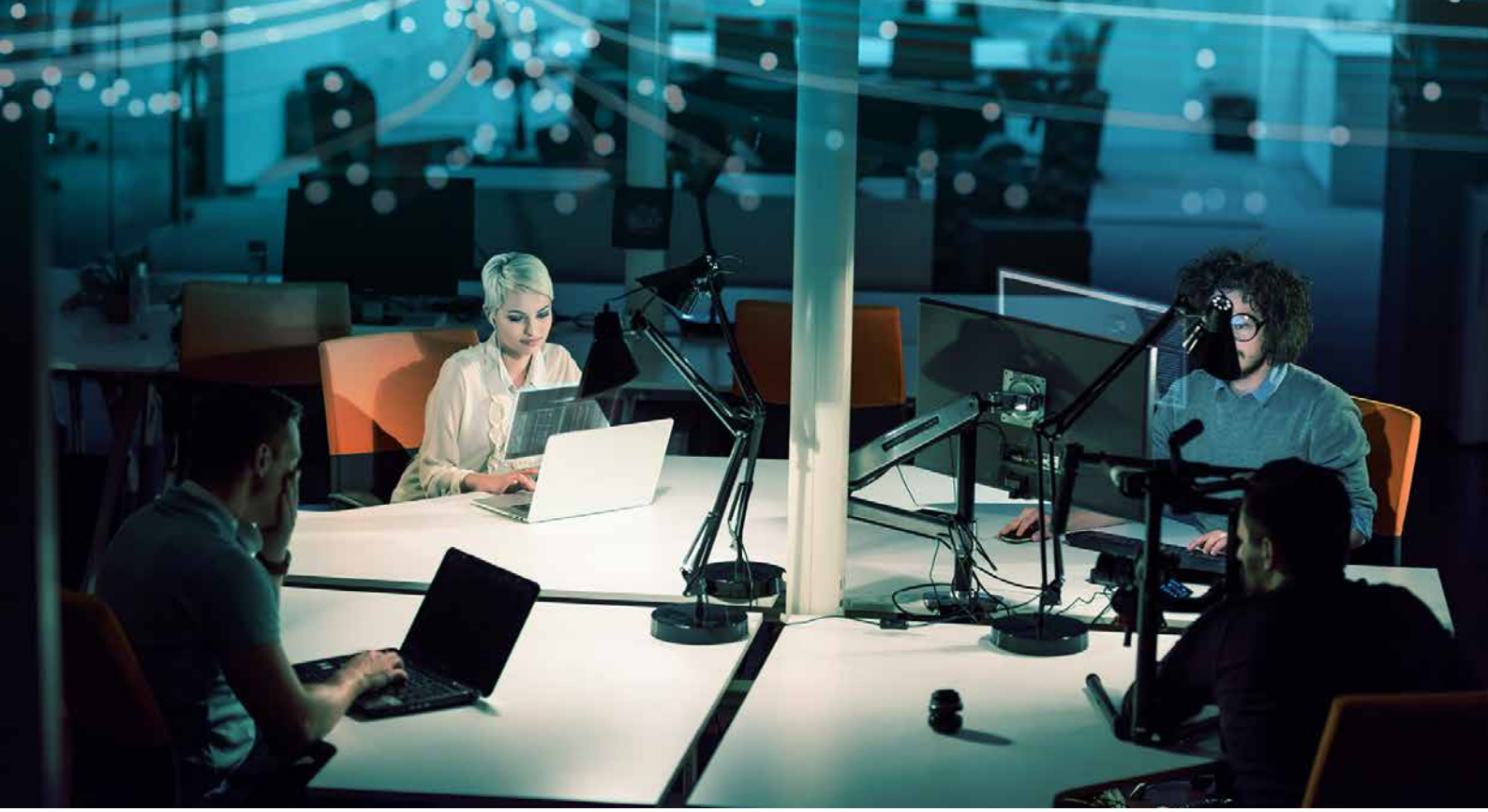
簡介

SOC (安全作業中心) 團隊是建構任何企業時的必要組成，因為這些團隊始終站在第一線對抗大型企業網路犯罪。但由於複雜的網路攻擊日益增加，且以關鍵身分資產 (如 Active Directory (AD)) 做為目標的威脅比例不斷成長，SOC 分析師紛紛認為使用傳統 SIEM 部署讓他們感到力不從心。從眾所周知的 AD 攻擊警示數量以及這類攻擊的成功率，即可明顯看出這點。

雖然 SIEM (安全資訊與事件管理) 是一個強大的解決方案，通常可用來監視網路基礎架構，但並非針對 AD 安全這類目的所設計。SOC 團隊利用一般 SIEM 來防禦 AD 免於遭受威脅和惡意軟體攻擊，往往會面臨各種挑戰，因而可能造成以下結果：

- 對於游走於網路中的真正威脅能見度不佳
- 資料外洩應變延遲
- 即時攻擊變得神不知鬼不覺
- 資安分析師疲於奔命

本白皮書會探討 Tenable.ad 這個針對 Active Directory 需求所量身訂做的 SIEM 前置解決方案，如何加強安全防禦機制並大幅提升 SOC 的效率。



SOC 團隊和 Active Directory 安全

在過去幾年內，我們見證到以 AD 為目標的網路攻擊與日俱增。

請思考主要勒索軟體攻擊者，例如 LockBit 2.0、Conti 和 BlackMatter，全都是使利用 AD 來引入或傳播惡意軟體。無論是透過刺探利用 AD 設定錯誤或後門程式，很顯然地，惡意的攻擊者日益瞭解要放肆存取受害者的網路有多麼容易。

只要 AD 在攻擊路徑中的核心地位不變，SOC 團隊就必須要監控瞬息萬變的 AD 目標威脅態勢。但他們要怎麼做？

我們來仔細探討一番。

在某個平凡的日子裡，SOC 使用 SIEM 工具來監控網路，並且對於有關資安事端的警示做出應變、分流並判斷警示的嚴重性，在網路上執行弱點掃描，然後產生評估報告。一些較為複雜的功能可能包括執行進階搜尋威脅來偵測隱藏在網路中的潛在威脅。

儘管 SOC 團隊預期隨時要提高警覺以及運用有效的應變和修復策略，但在網路攻擊日益猖獗的時期，SOC 可能左右著大型企業的存亡！若對於 AD 曝險沒有適當的能見度，您就有可能偵測不到攻擊破綻中的威脅，並且讓威脅從傳統的 SIEM 的缺口溜進來。

SIEM 無法顧及 AD 安全之處

在避免對於 SIEM 的功能言過其實之際，真相是 SIEM 從未針對 AD 安全的任何細節所設計。這使得 SOC 團隊必須努力解決迫切的問題。

首先，SOC 團隊必須定期更新 AD 所發生的狀況，以便能夠即時偵測到攻擊。這對於 SIEM 解決方案而言幾乎是不可能的。事實上，SIEM 主要的一項限制，是其無法即時偵測到異常行為。

其次，監控 AD 的 SIEM 解決方案通常會使 SOC 團隊疲於應付大量誤報，而相互關聯規則通常會致使產生大量的這類誤報。這會讓資安分析師採取進一步的行動來判斷受到標記的是否為所需的事件，進而造成龐大的負擔，使 SOC 功虧一簣。想像一下必須從數百萬個事件中，人工確認警示究竟是出自惡意事件、錯誤事件還是必須處理的事件是多麼困難的事！

第三，大多數攻擊者在有機可乘時，都會在 AD 中建立大量後門程式。因此，如果偵測到單一設定錯誤或惡意行動，安全專業人員就應進行搜尋特定於 AD 的威脅行動，確認是否啟動了任何其他後門程式。這遠超出 SIEM 的範圍。

另一項重大考量，是排山倒海的 AD 安全事件使得 SOC 專業人員疲於奔命。您最不樂見大型企業發生的狀況就是 SOC 中心瀕臨崩潰。

在提到 AD 安全時，很顯然 SOC 的期望與他們可以使用的工具 (此指 SIEM) 往往會有落差。這也表示，如果您的 AD 基礎架構中出現神不知鬼不覺的攻擊，事情可能很容易急轉直下。

事件記錄並不足夠

多年來，我們全都犯了一個錯誤，認為事件記錄包含了我們管理目錄中出現不合規之處時所需的所有資訊。有鑑於 SOC 團隊在解讀 Active Directory 安全或甚至在偵測網域攻擊時所遭遇到的困難，很顯然地，事件記錄不可或缺，但往往並不足夠。

Tenable 使用四個資訊來源來評估 Active Directory 的安全等級，並偵測與目錄相關的攻擊：

- 適用於 Windows 的事件追蹤 (ETW)：這是一個很有效的核心層級追蹤協助工具，讓您可將核心或應用程式定義的事件記錄到記錄檔案。您可以即時利用事件並使用模式偵測

- NTDS.dit：Active Directory 資料庫 (NTDS.dit) 中所做的變更會從網域控制器複製到網域控制器。您可以訂閱複製 API 來即時擷取這些變更
- 系統磁碟區：SYSVOL (系統磁碟區) 目錄也會在 Active Directory 網域控制器之間進行複製；這個目錄非常重要，因為其中包含群組原則範本 (GPT)，用於檔案型資料並儲存軟體原則、指令碼和部署資訊
- 誘捕系統：使用誘捕系統可使透過 ETW 收集的資訊更完善，並提供精確的方法來精進模式及大幅降低誤報

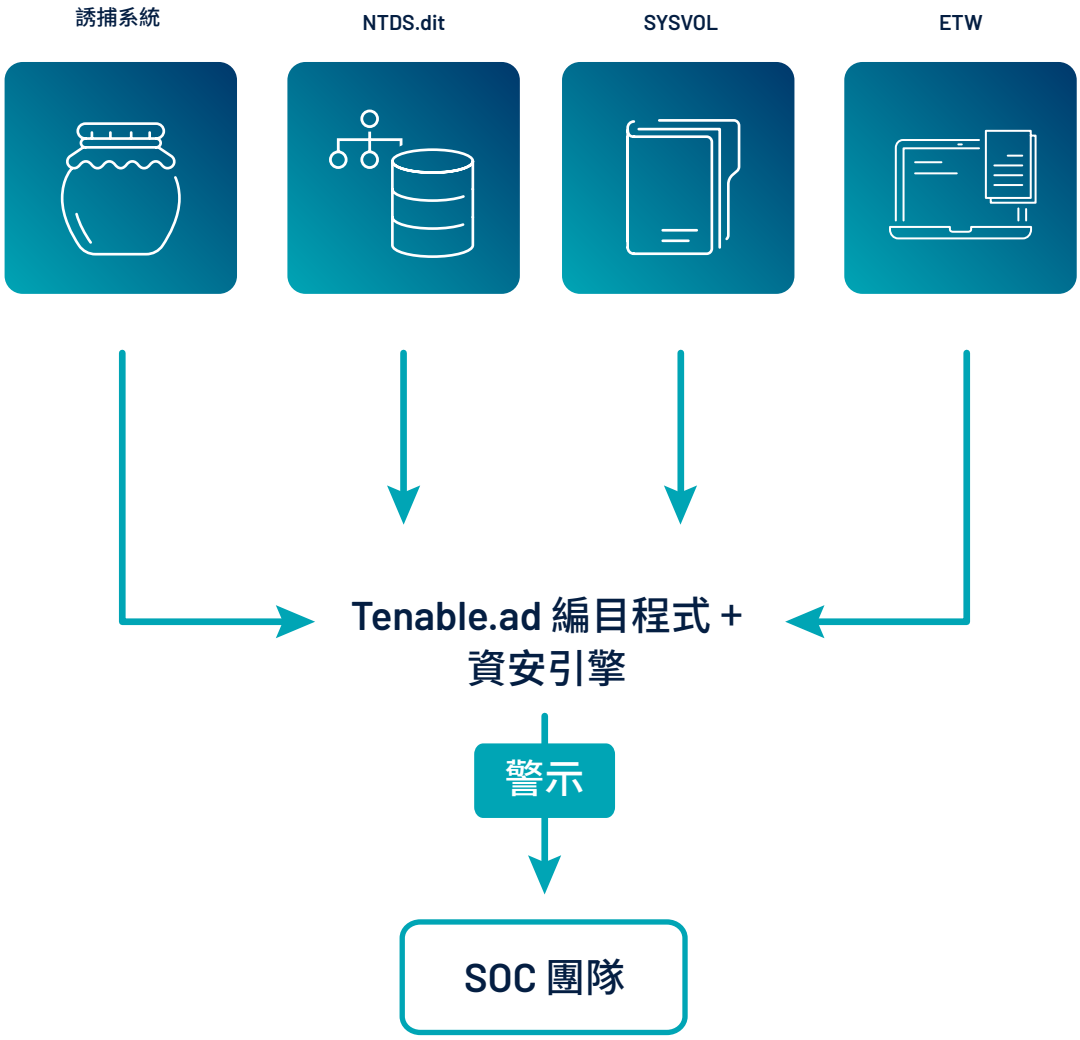


圖 1. Tenable.ad，四個資料來源

顯而易見地，同時使用四個資料來源而非僅使用一個資料來源更能全盤掌握情況。

利用 Tenable.ad 實現更高的 SOC 工作效率

網路安全專業人員都知道，資料外洩的問題不在於發生的可能性，而是在於發生的時間。在大部分企業中，在發生資安事端時，SOC 團隊會聯絡網路團隊和/或端點團隊，釐清異常端點或使用者的所在位置，然後決定遏制之道。這個流程效率不彰，需要花費數天才能完成修復。為了快速應變攻擊 AD 的威脅，您的 SOC 需要一種專精於 AD 的解決方案，來應對所有與監控 AD 安全有關的複雜工作。

這正是 Tenable.ad 的專精之處。

您的安全團隊能利用 Tenable.ad 在 AD 中洞察一切、預測最重要的事、並且採取行動以因應風險，在他們受到攻擊之前就中斷攻擊路徑。

以下所列的四個方法可供您的 SOC 團隊更深入洞察您 AD 環境中所有潛在安全問題。

1. 適用於 Active Directory 的 SIEM 前置解決方案

網路上的關鍵元件 (如 AD) 需要特定的解決方案。Tenable.ad 是專為 AD 所設計的 SIEM 前置解決方案。Tenable.ad 會將要傳送給 SIEM 的資訊標準化並精心篩選，如此一來，您就不必在 SIEM 層級花費數個月或數年來建立 AD 相互關聯規則。Tenable.ad 會將「AD 情報」加入您的 SIEM，因此能降低誤報。這可讓您免於承受在使用一般的事件稽核 AD 時漏掉重大弱點的風險。

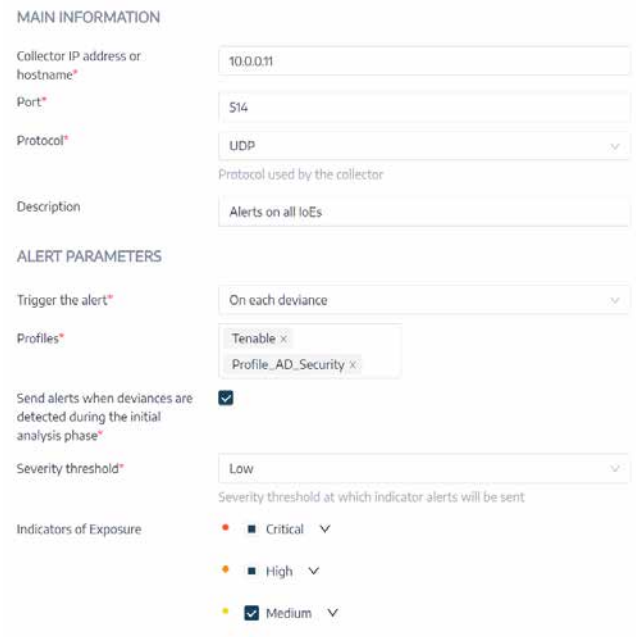


圖 2. 對 SIEM 設定 SYSLOG 警示

2. 擷取 SYSVOL 變更

您可以根據從 AD 資料庫和 SYSVOL 即時掃描的資料，利用 Tenable.ad 來建立及傳送警示給您的 SIEM。居心不良的攻擊者濫用群組原則物件 (GPO) 做為惡意軟體投送系統的情況並不常見。這是因為 GPO 設定修改位於 SYSVOL，所以一般 SIEM 幾乎無法偵測及理解 GPO 設定修改。反觀 Tenable.ad 則會即時掃描 SYSVOL 並理解 GPO 語言，如此一來，您將不會遺漏對 GPO 進行的惡意變更。

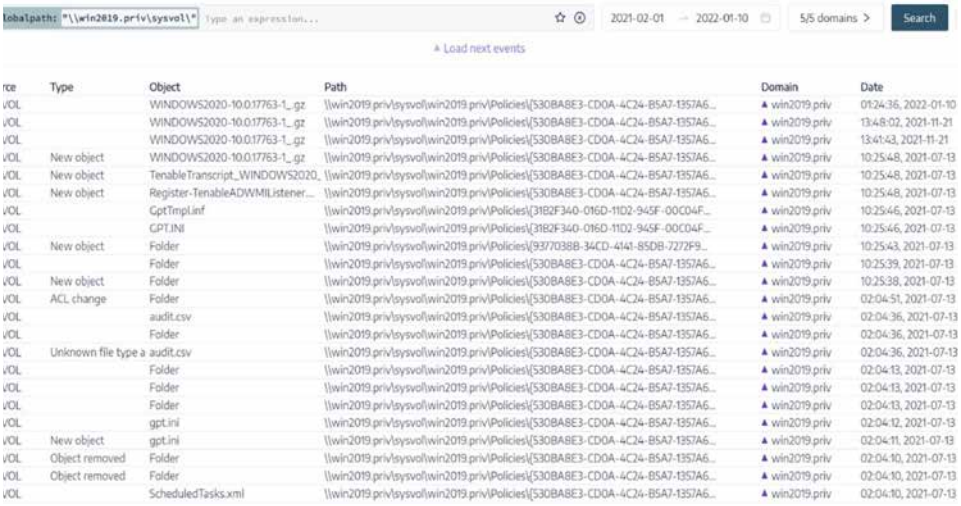


圖 3. 擷取 SYSVOL 中所做的變更

3. AD 攻擊的即時偵測

儘管 SIEM 可以偵測並警示特定的 AD 攻擊模式，實際上卻可能花費數個月的時間。此外，每當安全團隊搜尋到新的 AD 攻擊類型時，都必須變更 SIEM 設定。Tenable.ad 能讓 SOC 團隊精準掌握攻擊指標 (IoA)，提供真正即時的 AD 攻擊偵測。對 IoA 瞭若指掌可保障您免於遭受新型的 AD 攻擊模式，而不必在您的 SIEM 中進行複雜的設定變更。您可以設定警示，並根據攻擊類型及研究不合規之處來選擇警示嚴重性。

一旦惡意攻擊者透過盜用的網域帳戶而取得企業的內部網路存取權之後，會遭惡意攻擊者定期使用的一種攻擊，稱為 Kerberoasting。這種技術能讓攻擊者取得網域服務帳戶的密碼存取權，藉此提升其特權。由於觸發誤報的機率非常高，因此使用 SIEM 所提供的事件來偵測攻擊的難度相形也會提高，這一切都歸咎於攻擊的本質。為了偵測持續進行的 Kerberoasting 攻擊，Tenable.ad 採用一項欺敵技術，即誘捕系統戰術。「誘捕系統」能夠讓駭客認為他們正在使用橫向移動來入侵脆弱且充滿

漏洞的 AD 伺服器以及周遭系統和使用者帳戶，與此同時，他們實際上正陷入虛擬的欺敵環境。Tenable.ad中的誘捕系統戰術提供兩個優勢。第一，這種戰術能夠利用隔離誘捕系統上的動作交叉檢查 DC (網域控制器) 記錄，藉此準確搜尋攻擊事件。第二，這種戰術能大幅降低誤報的機會。

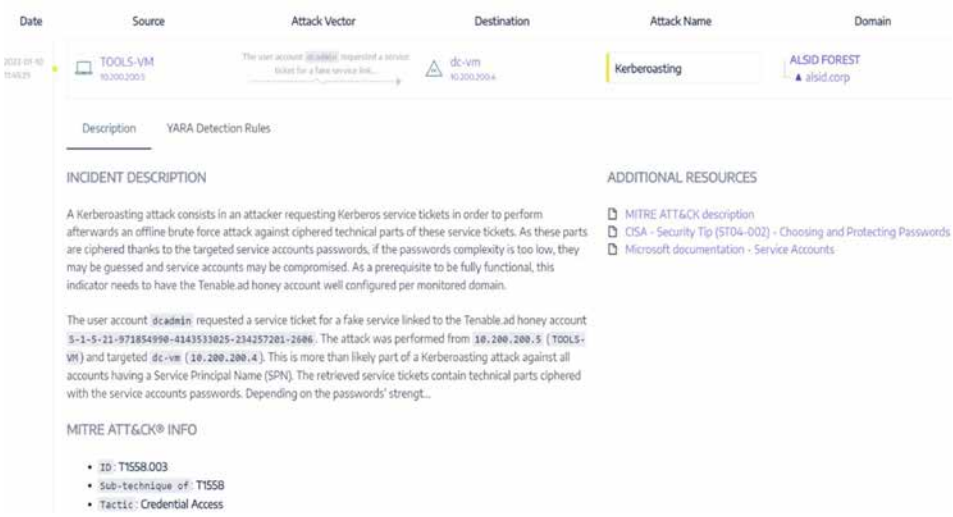


圖 4. 偵測 Kerberoasting 攻擊

4. 應對不留痕跡的攻擊

SIEM 解決方案仰賴事件紀錄，以掌握在 Active Directory 內正在進行的動作訊息。但像是 DCShadow 這種攻擊會仿造新型 DC 立即消失，藉此迴避記錄，因此假網域控制器的記錄絕對不會留下痕跡。SIEM解決方案可能會無法識別這些攻擊。反觀 Tenable.ad 並不需要等候活動記錄。反之，Tenable.ad 會利用原始的 AD 複製資料流和事件來獲取資訊，甚至在行動執行前就能取得資訊。如此一來，SOC團隊整裝待發，絕不會讓這些迴避記錄的特權攻擊有機可乘。

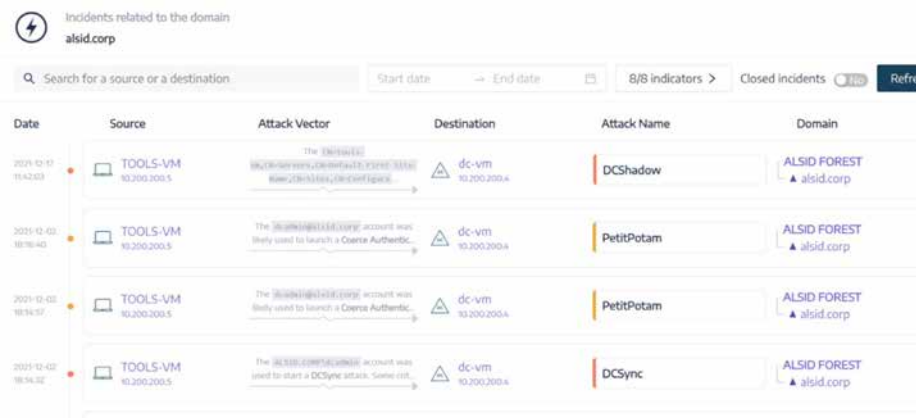


圖 5. 偵測 Active Directory 上正在進行的攻擊行動

總結

由於鎖定 AD 的攻擊絲毫沒有趨緩的跡象，SOC 團隊必須提高他們對 AD 攻擊破綻的能見度，且擁有一旦真的偵測到攻擊發生時已測試過的計劃。

儘管 SIEM 是整體安全的重要解決方案，但 SOC 團隊就 AD 安全目的使用 SIEM 時仍會面臨挑戰。常見的痛點包括其通用的特性、觸發的誤報數多到令人疲於應付，以及本白皮書中所討論的其他問題。專門針對 AD 的解決方案 (例如 Tenable.ad) 不只是單純填補傳統 SIEM 的缺口，還能與 SIEM 進行整合來提升 AD 安全。此外，Tenable.ad 會從四個不同來源而非單一來源擷取資訊，進而協助 SOC 團隊更妥善評估其 AD 基礎架構。這些來源包括 ETW、AD 資料庫、SYSVOL 和誘捕系統。Tenable 掌握了上述所有的功能，便能大幅提升 SOC 效率，而這正是令人心曠神怡的降低網路風險步驟。

	Tenable.ad	SIEM
識別現有的 AD 設定錯誤	是	否
根據攻擊嚴重性設定警示	是	否
即時偵測持續不斷的攻擊行動	是	有限，且需要定期更新設定
擷取並轉譯 GPO 層級的變更	是	否

表 1. 比較 Tenable.ad 與 SIEM 的功能

為了在不提升特權的情況下，使用無代理程式的解決方案保障貴公司 Active Directory 基礎架構的安全，請參閱我們網站上的 Tenable.ad 專區：zh-tw.tenable.com/products/tenable-ad

感謝您撥冗閱覽本文。

Tenable 行銷經理 Anjali George

Tenable 安全策略師 Sylvain Cortes

關於 Tenable

Tenable® 是一家 Cyber Exposure 分析公司。全球大約有超過 40,000 家企業仰賴 Tenable 協助瞭解並降低網路風險。身為 Nessus® 的創造者，Tenable 拓展了本身在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。在 Tenable 的客戶中，包含超過 60% 的財星 500 大企業、大約 40% 的全球 2,000 大企業以及大型政府機構。如需深入瞭解，請前往 zh-tw.tenable.com。

tenable®