Privileged Threat Analytics ™

偵測可能對企業造成重大影響的最嚴重網路攻擊、發送告警並做出回應

挑戰

網路攻擊者會不斷提高其攻擊技能以便在網路中進行操作而不被察覺。一旦入侵，攻擊者就會儘可能隱秘地偵察整個網路，提升權限，直到接近目標。攻擊者會使用特殊權限憑證偽裝成已授權的使用者，避免引起注意。因此，要偵測到攻擊者是否侵入網路並做出回應，企業將面臨監控使用者活動方面的各種挑戰。

需要分析太多資料

在大數據時代，有太多資料需要分析。無論是僅僅依靠 SIEM 解決方案，還是採用全方位分析工具，通常，企業會嘗試僅採用一項解決方案來分析所有資料。但是，由於範圍是如此的廣泛，資安分析師會被資料「淹沒」，因此無法發現系統被入侵的跡象。如果不進行有針對性的資料收集來確定最關鍵的攻擊手段，企業將收到大量的告警及錯誤警報，並因此而應接不暇。

不確定如何回應資安事件

處理與特殊權限帳號相關的告可能極具挑戰性，因為這些帳號通常由多名使用者共用，因此很難查明告警的來源。即使偵測到出現異常的特殊權限活動，傳統的監控解決方案也缺乏必需的關鍵資訊，無法快速做出事件回應。

無法保持精確監控

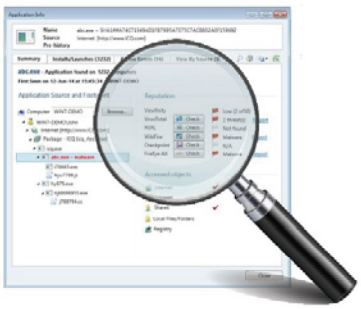
傳統的監控及偵測工具往往需要大量維護作業。首先，資安團隊需要瞭解並定義什麼是「正常」活動，然後，資安團隊需要定義並偵測「異常」活動。這整個過程需要耗費大量時間，以調整報告，編寫新規則，更新原則等。

解決方案

CyberArk 特權威脅分析 (Privileged Threat Analytics) 是一款聰明的資安解決方案，可幫助企業偵測正在進行攻擊的異常特殊權限活動、發送告警並做出回應。透過僅分析特殊權限活動，而不是分析 IT 網路上的所有資料，CyberArk 特權威脅分析能夠就最嚴重的惡意活動發送針對性的、有級別的告警。

該解決方案會從多個來源 (包括 CyberArk 數位金庫、SIEM 及網路流量監聽) 收集一組特定資料，然後，分析引擎將運用一組統計學上複雜的確定性 (deterministic) 演算法，透過確定惡意特權帳號及使用者活動，幫助企業在攻擊過程的早期階段偵測到入侵跡象。這讓資安團隊在企業被迫停止業務之前有機會阻止網路攻擊。

確定潛在的攻擊之後，CyberArk 特權威脅分析就可以與已整合的 CyberArk 解決方案進行協作，加速威脅回應。CyberArk 企業密碼金庫可自動接收可能已遭到入侵的帳號的相關告警，並立即更新憑證或帳密以遏制攻擊。如果收到與高風險特權使用者活動有關的告警，資安團隊可以透過 CyberArk 特權連線管理器即時查看可疑連線，並視情況斷開連線，阻止攻擊者繼續進行攻擊。



CyberArk 儀表板：此儀表板以直觀的方式顯示一段時間以來偵測到的事件，其中顯示偵測到一次 Golden Ticket 攻擊。儀表板上同時提供惡意使用者及機器等關鍵資訊；資安分析師可以進行深入分析，瞭解與所有安全事件有關的更詳細資訊。

CyberArk 特權威脅分析可以：

- **偵測嚴重攻擊並發送告警：**由特權帳號安全領域專家編寫的演算法僅分析 IT 網路內的最關鍵活動。本解決方案旨在偵測在網路中存取多台機器的活動、提升權限、帳密與憑證盜竊及可疑的命令列活動等攻擊跡象並就此發送告警。
- **在每一項告警中提供可作為行動依據的情報：**每項告警均包含詳細的使用者級別情報，包括惡意使用者、已被攻破的電腦、IP 地址、發生事件的日期及時間等，可幫助資安團隊快速回應威脅。
- **自動回應安全事件：**偵測資安事件只是第一步。資安團隊必須分析告警，遏制威脅，然後採取補救措施並從事故中復原。CyberArk 解決方案提供自動回應功能，可撤銷疑似被盜的憑證，立即遏制偵測到的威脅，而無需人為介入。

優勢

CyberArk 特權威脅分析可幫助企業：

確定以前無法偵測的攻擊。通常，攻擊者會潛伏數月甚至數年時間進行滲透，而未被偵測到。CyberArk 特權威脅分析會分析相關資料，以協助偵測最嚴重的攻擊並發送告警，如外洩的特殊權限憑證或帳密、惡意特權使用者活動及 Kerberos 攻擊。

限制攻擊者進行攻擊的時機。透過專注於分析特權帳號活動、特權使用者活動及關鍵攻擊向量，CyberArk 特權威脅分析能夠幫助企業比傳統偵測工具更早偵測到網路攻擊。這樣，資安團隊就可以立即甚至自動做出回應，阻斷攻擊企圖。

提高資安團隊的工作效率。透過專注於分析特權帳號，CyberArk 特權威脅分析可協助事故回應團隊優先處理涉及特權帳號及憑證的告警。每項告警均包含詳細的、可作為行動依據的資訊，可協助資安團隊快速做出回應。告警可直接發送到 SIEM 儀表板，以透過單一介面進行分析。

全方位解決方案

CyberArk 特權威脅分析是 CyberArk 特權帳號安全解決方案的一個元件，此款全方位解決方案旨在主動保護及管理特權憑證及帳號，隔離並監控特權連線，以及偵測並回應異常的特權帳號活動。該解決方案中的產品可進行獨立管理，也可以作為全方位特權帳號安全解決方案進行集中管理。

規格

CyberArk 特權威脅分析可整合 CyberArk 數位金庫 v7.1.6 及更新版本 Windows 用戶端：

支援的瀏覽器：

- Chrome 26 及更新版本
- Firefox 20 及更新版本
- Internet Explorer 9.0

PTA 伺服器

支援的平台：

- VMware Player 4.0 及更新版本
- VMware Workstation 8.0 及更新版本
- VMware ESX/ESXi 4.0 及更新版本
- Hyper-V for Microsoft Windows Server 2012 R2

最低虛擬機要求

- 8 核心 CPU
- 16GB RAM 記憶體
- 2TB 硬碟儲存空間

PTA 網路感測器

PTA 網路感測器（PTA Network Sensor）是連接網路、監聽網路流量並進行深度資料封包檢測的元件。可以設定單一 PTA 伺服器以接收來自多個 PTA 網路感測器的資料。

支援的平台

PTA 網路感測器在 CentOS 7.x 上運行，並且可安裝在實體電腦或虛擬機器上。

最低伺服器 / 虛擬機要求

- 8 核心 CPU，8GB RAM 記憶體
- 200 GB 硬碟儲存空間
- 管理介面網路卡，監聽網路卡