DATASHEET

One Identity Safeguard for Privileged Analytics

偵測與預防特權存取相關的安全風險

效益

- 追蹤使用者活動並建立視覺化報表，提供深入的 IT 系統活動細節
- 不間斷的分析按鍵動態與滑鼠移動以進行連續驗證
- 利用機器學習，根據基線活動分辨異常行為
- 運用脈絡資訊和根據連線記錄建立風險對策優先性，縮短安全事件的偵測時間
- 減少安全預警雜訊，讓你能夠專注於重要事件
- 於潛在惡意活動觸發預警時，中斷任何連線以強化安全性

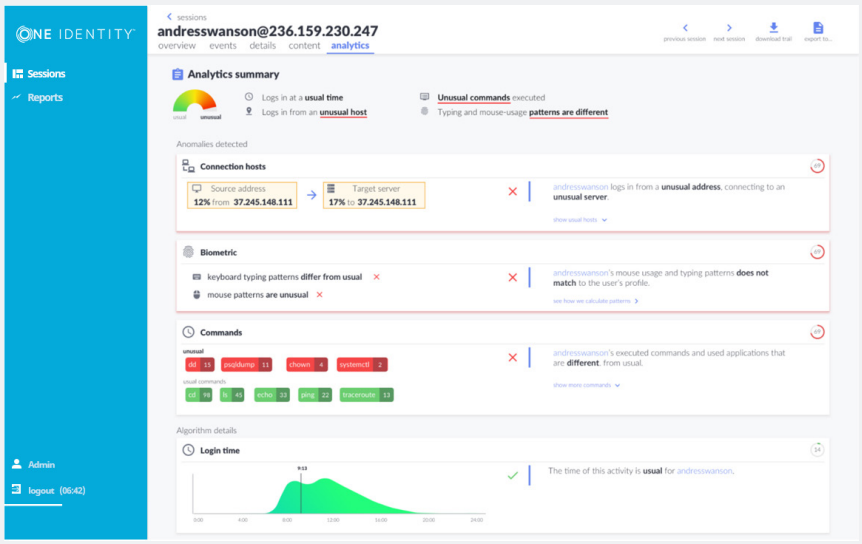
綜覽

身為 IT 安全管理人員，你應該「確認」而非只是「認為」公司將永遠不會遭受特權帳號外洩事件。今天，企業平均需要花 206 天 1 才能找出安全漏洞。時間就是金錢 - 同時也是風險。因此，不論原因出自一個被劫持的特權帳號或者是不遵守安全規則的管理者，其未被發現的時間越長，就會給予滲透者更多時間去挖掘和竊取資料，並負擔更多罰金和昂貴的鑑識成本。

除了你信任的管理者之外，你可能還必須將特權存取權提供給其他人，包括來自外部顧問單位的委外管理者，他們的辦公室可能設在全球任何地方。因此，你如何確保擁有特權存取的管理者正當而無惡意使用？

你可以透過 One Identity Safeguard for Privileged Analytics 知道誰是最具風險的使用者，並且持續監控新的內外威脅，以及偵測異常的特權行為。這個強大的方案協助你掌握特權使用者及其行動的完整能見度，並且能在出現問題時採取立即行動以預防資料外洩。

[1] Ponemon's 2017 Cost of Data Breach Study



輕易判斷風險使用者和行為

從分析摘要報告快速判斷使用者活動是否異常和具有潛在風險。摘要報告包含異常指令、生物特徵活動以及主機連接清單。

功能

辨識風險使用者

Privileged Analytics 根據風險分類規則，評估使用者權限以辨識高風險帳號。當權限出現變更而將使用者移到高風險狀態時，Safeguard 將主動發送通知。這可以避免來自非必要或休眠帳號的風險，預防遭他人惡用。

即時偵測未知威脅

Rules-based 安全性將無法偵測新的外部攻擊方法或惡意的內部人員。Safeguard for Privileged Analytics 即時追蹤使用者活動並建立視覺化，讓你更能掌握 IT 環境的眞實狀態。它不需要使用預先定義的關聯規則，而可以直接運用你既有的連線 (session) 資料。

不用型態比對

利用型態比對方法偵測「已知惡意」行爲往往會出現不正確的結果。Safeguard for Privileged Analytics 使用的是從你的 IT 環境收集而得的資料，據此建立一個「正常」行爲基線，然後運用多種機器學習演算法以偵測異常行爲。

螢幕內容分析

Safeguard for Privileged Analytics 藉由分析特權存取期間的螢幕內容並了解使用者送出的指令和視窗抬頭，以建立更完整的特權使用者常用指令與應用程式基線行爲檔案。此種細緻的分析有助於辨識典型行爲，以及偵測特權帳密竊盜。

行爲生物特徵

每一位使用者都有特定的行爲型態，即使是執行相同的動作時亦然，例如鍵盤輸入或移動滑鼠。Safeguard for Privileged Analytics 內建的演算法會檢視這些行爲特徵 (由 Safeguard for Privileged Sessions 捕捉)。按鍵動態與滑鼠移動分析有助於判斷是否屬於入侵行爲，同時也可以作爲一種連續的生物特徵驗證。

減少預警雜訊

Privileged Analytics 根據風險和異常等級對使用者事件分類，並標示出最可疑的事件，從而減少 SIEM 產生的預警雜訊。預警可以傳送至 SIEM 或由安全分析師在直覺式的使用者介面上查看優先事件清單，讓他們能夠專注於最重要的事件。

自動化回應

在大多數攻擊場合中，高衝擊性的事件在發生之前往往會有一個偵察階段。因此，這個階段的偵測與回應是預防遭受攻擊損害的關鍵。Privileged Analytics 與 Safeguard for Privileged Sessions 之間的無縫整合，確保不論何時發生高度可疑的事件或者偵測到惡意行爲都能自動切斷連線。

關於 One Identity

One Identity 協助企業建立正確的身分識別與存取管理 (IAM)。我們提供獨特的方案組合，包括身分識別管理組合、存取管理、特權管理、以及身分識別即服務方案，讓企業能夠充分發揮潛能而不會因爲安全問題而受到阻礙，同時有效的防範威脅。詳細資訊請參觀： OneIdentity.com