Change Auditor Threat Detection

主動偵測 Microsoft 環境中的使用者威脅

大多數組織均仰賴 Active Directory (AD) 作爲驗證和授權的主要來源，使其成爲駭客、網路恐怖分子及心懷不滿之離職員工的主要目標。然而，這些組織可能沒有意識到對 AD 安全而言更直接的威脅，其實是來自有意或無心的內部人員。更糟的是，AD 的複雜本質讓人難以在出現威脅時順利找出。過去以規則爲基礎的使用者威脅偵測方式會產生大量警示，讓您根本不可能逐一進行調查；導致完全錯失找出眞正威脅的機會，而讓組織暴露在資料安全漏洞的風險之下。那麼，您該如何即時分析在環境中發生的所有使用者活動，以保護業務免於中斷呢？

Change Auditor Threat Detection 可建立個別的使用者行爲模式來提供獨特的使用者威脅偵測方法，藉此偵測可能表示有可疑使用者或帳戶遭入侵的異常行爲。Change Auditor Threat Detection 會分析使用者活動，並使用專有的先進學習技術、使用者和實體行爲分析 (UEBA) 及精密的評分演算法，來評定組織中風險最高的使用者，找出潛在的使用者威脅，並減少誤判警示的干擾。最終您將能弭平原生稽核工具產生的缺口，確實維持環境的安全。

功能

即時稽核記錄分析

即時有效率地分析大量的稽核資料，包括 AD 變更、驗證及檔案活動。可從這些原始活動事件建立使用者基準，並主動偵測使用者的異常行爲，以便您立即察覺潛在的可疑活動。

Change Auditor Threat Detection 可協助您輕鬆迅速地偵測可疑的使用者活動，以保護環境與使用者的安全。

優點：

- 可根據使用者的行爲模式主動偵測威脅。
- 可減少與規則型威脅偵測相關的大量警示。
- 可檢視脈絡中的安全警示，輕鬆迅速地判斷其嚴重性。
- 可藉由使用者行爲基準，輕鬆偵測出使用者的異常行爲。
- 可根據現有的稽核資料找出威脅，以確實減輕對基礎架構的影響。

使用案例：

Change Auditor Threat Detection 可讓您輕鬆迅速地發現威脅，包括：

- 異常的 AD 活動
- 濫用具權限帳戶
- 暴力破解攻擊
- 資料外洩
- 不當的系統或資源存取
- 惡意軟體
- 權限提高
- 橫向移動

系統需求

CHANGE AUDITOR COORDINATOR

(伺服器端元件)

處理器：四核心 Intel Core i7 同級或更佳處理器

記憶體：至少 8GB RAM 或以上，建議使用 32GB RAM 或以上

CHANGE AUDITOR CLIENT

(用戶端元件)

處理器：雙核心 Intel Core i5 同級或更佳處理器

記憶體：至少 4GB RAM 或以上，建議使用 8GB RAM 或以上

CHANGE AUDITOR AGENT

(伺服器端元件)

處理器：雙核心 Intel Core i5 同級或更佳處理器

記憶體：至少 4GB RAM 或以上，建議使用 8GB RAM 或以上

如需系統需求的最新詳細清單，請造訪 support.quest.com/change-auditor

自動化使用者行爲分析 (UEBA)

完全不需要由管理員輸入或設定，即可建立使用者活動模式。使用無人監管的先進機器學習功能，自動建立使用者行爲基準，並將使用者活動的每個層面模型化，包括使用者的登入模式、管理活動以及檔案和資料夾存取行爲。

精密的行爲異常偵測

根據使用者的行爲基準，自動比較每個使用者動作，以找出是否有異常的使用者活動。精密的威脅指標偵測與多層級風險評分可確保僅標示出最嚴重的異常活動，以顯示風險最高的使用者行爲。

模式型使用者威脅偵測

只有在偵測到關聯的異常使用者行爲模式時，才會發出 SMART 使用者威脅警示。並非仰賴規則來偵測特定的活動，而是在活動發生時自動分析所有使用者活動，並透過精密的使用者行爲模式偵測，找出環境中最可疑的使用者。精密的全域模型化可確保僅標示出最重要且最相關的使用者行爲模式，以大幅減少個別活動和誤判造成的干擾。

精準度高的使用者分析

Change Auditor 會建立稽核記錄來回饋給分析功能，因此用來主動偵測環境威脅的所有原始事件資料原先即已包含以下重要資訊：

- 變更的始作俑者
- 變更的內容
- 變更的時間
- 變更的地點
- 變更的來源 IP 位址或工作站

有別於原生 Windows 事件記錄，Change Auditor 可確保不錯過任何重要的使用者動作，以防止在使用者行爲分析中出現嚴重缺口。

脈絡中的安全警示

在從警示當中發現的威脅指標脈絡中，檢視所有可疑的使用者活動警示。各個異常行爲都會顯示在使用者基準活動的脈絡中，並顯示觸發警示的所有原始事件，清楚指出發出警示的原因，並簡化調查工作和後續行動。

輕量型使用者威脅偵測

運用現有的 Change Auditor 基礎架構和稽核資料將使用者行爲模型化，因此不需要部署不必要且效率不彰的其他代理程式和伺服器。單一虛擬應用裝置便是實現進階使用者威脅分析所需的唯一其他基礎架構。

關於 QUEST

Quest 的宗旨是以簡單的解決方案解決複雜的問題。爲了達成此理念，我們堅持提供優異的產品和服務，並秉持簡單經營業務的整體目標。我們期望能爲您帶來兼顧效率與效益的技術，讓您和貴組織可以減少耗費在 IT 管理上的時間，進而投入更多時間發展業務創新。

Quest
www.quest.com
如果您在北美洲以外地區，可在我們的網站找到當地辦事處的資訊。

DataSheet-ChangeAuditorThreatDetection-TW-KS-zh_TW-WL-32855