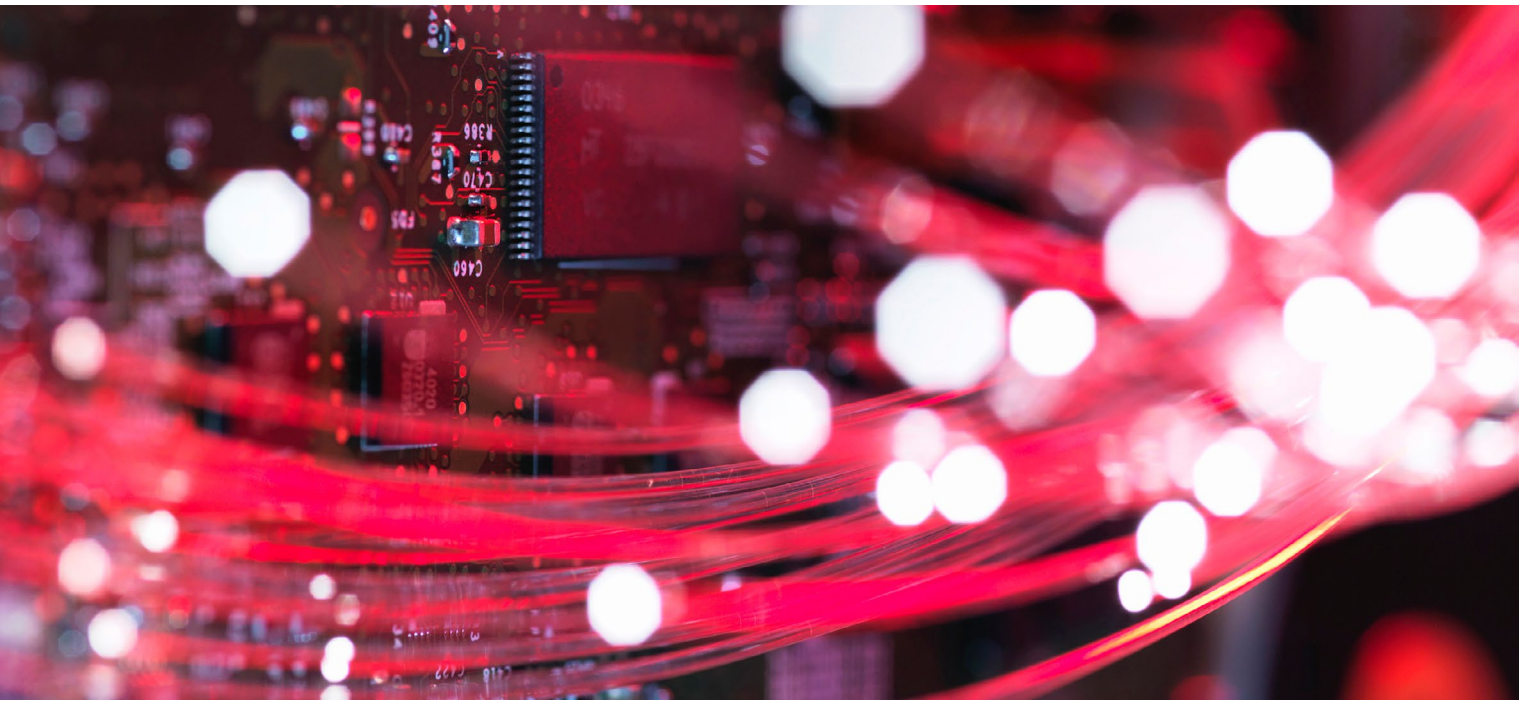
洞悉 Change Auditor Threat Detection

瞭解本進階解決方案是如何避免警示誤報，並全力鎖定風險最高的使用者



簡介

偵測異常使用者的可疑活動可說是一大挑戰。過去以規則爲基礎的使用者威脅偵測方式會產生大量警告，讓您根本不可能逐一進行調查；最後變成浪費時間對誤判窮追猛打，導致完全錯失眞正的威脅，讓組織暴露在資料安全漏洞的風險之下。但假使您擁有複雜的模式辨識技術，只有在使用者行爲的異常性到達一定程度，並百分之百確認爲憑證入侵或權限濫用事件時才觸發警示，該有多好？

Quest® Change Auditor Threat Detection 使用進階機器學習、使用者和實體行爲分析 (UEBA) 和 SMART 關聯技術，可正確鎖定異常活動並識別環境中風險最高的使用者，有效保護您的資料和業務。本技術概述接下來將說明 Quest® Change Auditor Threat Detection 的運作方式。

使用者威脅偵測流程

概覽

如圖 1 所示，威脅偵測流程包含以下步驟：

1. 分析記錄
2. 使用者行爲模型化
3. 偵測異常
4. SMART 關聯
5. 風險評分
6. 排定使用者和警示優先順序

圖 1. Change Auditor Threat Detection 輸入來源和威脅評估流程概覽

Change Auditor Threat Detection 可對上百萬個記錄進行分析，爲每位使用者建立準確的行爲基準

步驟 1：分析記錄

來自 Change Auditor 活動記錄的使用者活動資料將匯入 Change Auditor Threat Detection 引擎，並在此處進行即時分析，以建立環境使用者、群組、系統和檔案的全域地圖。此匯入記錄資料可包含：

- **驗證活動** (來自 Change Auditor for Logon Activity)
- **Active Directory 變更** (來自 Change Auditor for Active Directory)
- **檔案存取活動** (來自 Change Auditor for Windows File Servers、Change Auditor for EMC、Change Auditor for FluidFS 和 Change Auditor for NetApp)

步驟 2：基準使用者行爲模型化

Change Auditor Threat Detection 會利用機器學習和使用者行爲分析在紀錄資料流中對使用者行動進行多方面分析，並爲環境中各使用者的一般行爲逐步建立多維度 基準。**使用者行爲基準**由一組獨特的使用者識別項目所組成，這是爲了確保系統僅對異常行爲進行標記。舉例來說，基準可包含特定使用者一般登入時間、使用工作站、是否傾向從遠端據點登入，以及通常存取的檔案等資訊。

系統會頻繁更新使用者行爲基準，並持續提升準確度。定期更新基準的同時，Change Auditor 亦可對未知狀況進行邏輯性假設，把正常活動誤判爲警示的機會降至最低。Change Auditor 需要 30 天的稽核記錄才能建立使用者行爲的初始基準。

步驟 3：偵測異常

使用者行爲基準建立完成後，Change Auditor Threat Detection 會使用威脅分析和數十個預先定義的威脅指標，即時偵測異常的使用者活動。**威脅指標**會定義高風險活動，例如可疑的使用者登入、暴力密碼破解攻擊、Active Directory 異常變更和不正常檔案存取。然而，威脅指標不受限於特定原始事件，它們將透過機器學習，識別出可能共同構成威脅的不同事件模式。

特別是，隨著上百萬件原始事件匯入，Change Auditor Threat Detection 可分析人力動作項目、帳戶、位置和特定操作，藉此鎖定違反已建立基準的使用者行爲。系統會根據事件稀少性和嚴重性，對與威脅指標對應的異常行爲指派獨立風險分數。此異常偵測策略可確保系統將在由 Change Auditor 處理的上百萬件大多合法的原始事件中，僅標示出重要且顯示爲潛在可疑活動的行爲變更。

Significant (大量)

Multidimensional (多維度)

Anomaly (異常行爲)

Reduction (減少)

Technology (技術)

圖 2. SMART 關聯技術可大幅減少誤判警示數量。

步驟 4：SMART 關聯

威脅指標是 **SMART 警示**形成的基礎。SMART 這項關聯技術可對經常變更的動態行爲提供排定優先順序之結果 (請見圖 2)。SMART 使用結合統計和機器學習演算法，可識別異常現象間的獨特關聯，藉此降低誤判並協助鎖定任何其他安全解決方案無法找出的威脅。SMART 可透過即時識別異常實體行爲特殊順序並相互關聯，進而爲反映使用者行爲出現重大異常的警示排定優先順序並進行整合。

因此，縱使上百萬件原始事件可能觸發上千個威脅指標，僅有眞正可疑的行爲模式最終才會獲得分數。這代表 Change Auditor Threat Detection 介面將發出更少的警示，且誤判數量縮減，讓您無需浪費心力處理誤判 (請見圖 3)。且專屬機器學習演算法會在使用者行爲後方建立內容，可提供準確且高度相關的結果，協助分析人員識別使用者動機。

隨著系統處理越來越多記錄資料，SMART 警示可同步進行改善以提供日益精準的使用者威脅偵測，和使用者行爲基準的運作方式類似。

透過爲異常動作建立關聯，SMART 關聯可減少誤判情況，並鎖定任何其他安全解決方案無法找出的威脅。

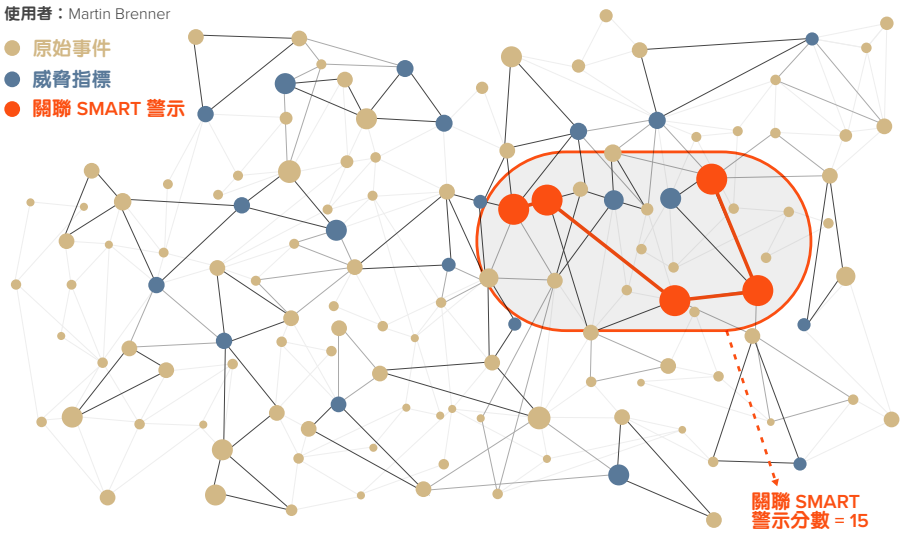


圖 3. 儘管上百萬件原始事件可能觸發上千個威脅指標，SMART 關聯仍可確保最終只有眞正可疑的行爲模式才會獲得分數。

Quest

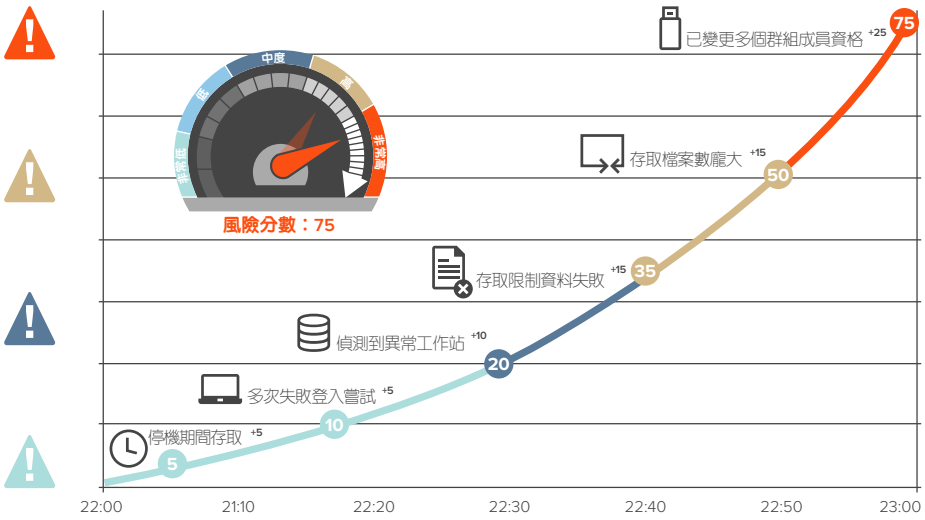


圖 4. 系統會對每位使用者指派風險分數，反映該名使用者涉及潛在可疑活動的機會。

Change Auditor Threat Detection 動態儀表板會標示出風險分數最高的使用者，讓您排定回應優先順序。

步驟 5：風險評分

系統會根據威脅指標的嚴重性，對每個 SMART 警示指派風險分數。系統會結合對各使用者識別出的所有 SMART 警示，計算出可反映使用者風險或可疑程度的整體**使用者風險分數**。也就是說，使用者風險分數即系統對特定使用者發出之所有 SMART 警示的個人風險分數彙總 (請見圖 4)。

步驟 6：排定使用者和警示優先順序

系統會將風險分數最高的使用者標示於 Change Auditor Threat Detection 儀表板的左側面板，對新興使用者威脅建立依嚴重性排序的動態監看清單 (請見圖 5)。Change Auditor Threat Detection 會對與環境其他活動相關的每位高風險使用者嚴重性評分，確保眞正的攻擊或權限濫用事件發生時，系統可立即鎖定目標。與高風險使用者關聯的 SMART 警示會列在右側面板，您即可輕鬆探索環境中的可疑行

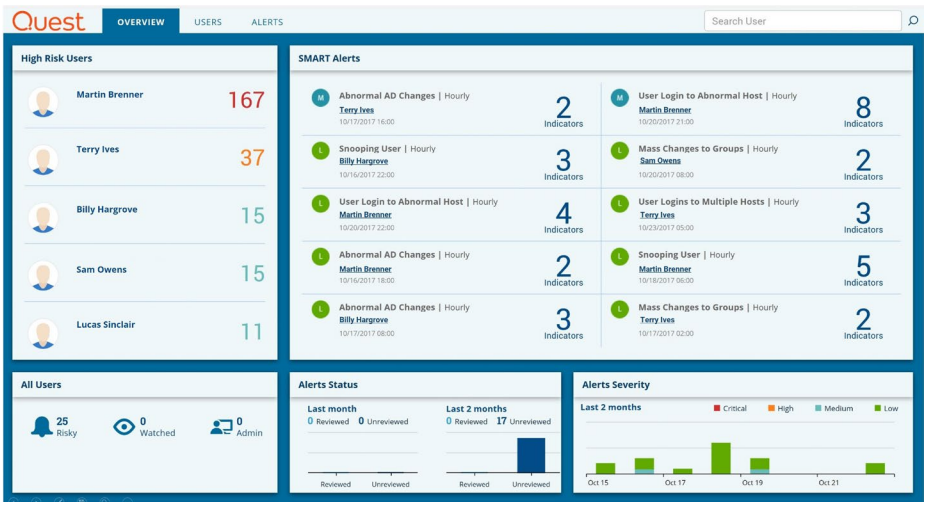


圖 5. Threat Detection 儀表板將隨時標示出環境中風險最高的使用者及最重大的警示，讓優先處理最緊急的使用者威脅變得輕鬆無比。

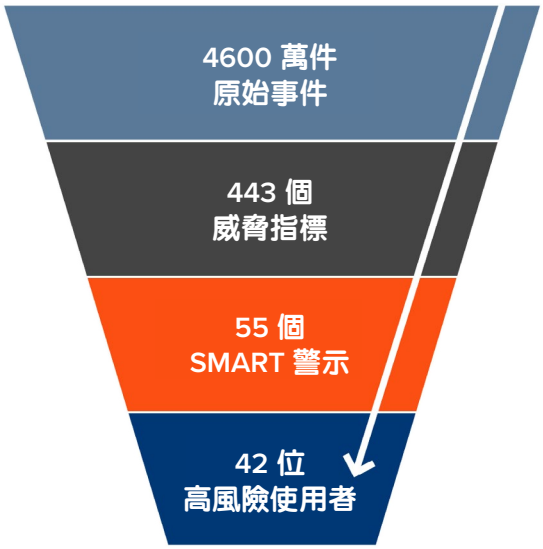


圖 6. Change Auditor Threat Detection 可將大量稽核資料過濾到只剩下風險最高的使用者，讓您專心因應環境中的眞正威脅。以上數據是在含有 7,000 名使用者的環境下於爲期 45 天的分析工作中取得。

爲並迅速回應。儀表板的底部面板會顯示關於高風險使用者的重要統計資料，以及環境中警示長期下來的趨勢。

實際結果

此多步驟威脅偵測程序將過濾環境中上百萬個事件，篩選出少數威脅指標，接著產生更少量的 SMART 警示，最後顯示您眞正需要的安全情報：環境中風險最高的使用者及其可疑行動。

舉例來說，在一個實際包含 7,000 名使用者的環境中，本解決方案在 45 天期間內將 4600 萬件原始事件過濾到只剩下 42 名高風險使用者 (請見圖 6)。

模型種類

說明完威脅偵測程序，讓我們接著探討相關細節，先來談談 Change Auditor Threat Detection 將部署哪些特定模型種類，以建立行爲基準和偵測威脅指標。

時間式模型

本模型將鎖定於不正常時間發生的活動，例如以下狀況：

- 使用者在異常時間登入 Active Directory。
- 使用者在異常時間存取檔案。

類別式模型

本模型將針對使用者互動的特定類別或物件搜尋相關活動 (如電腦、地點或資料夾)，例如以下狀況：

- 使用者在異常地點登入 Active Directory。
- 使用者存取過去未曾存取過的伺服器。
- 使用者從過去未曾存取過的資料夾開啓檔案。

持續式模型

本模型將觀察特定時間範圍內發生的事件模式。範例：

- 異常大量的檔案在一小時內遭到刪除。
- Active Directory 在一小時內遭進行大量變更。

Change Auditor 不僅可偵測異常事件，更鎖定長期以來使用者行爲的風險模式。

圖 7. Change Auditor Threat Detection 會在四個不同階段使用風險評分，以鎖定組織內的最大風險。

Change Auditor Threat Detection 可準確識別出環境中風險最高的使用者。

風險評分

Change Auditor Threat Detection 會在四個不同階段使用風險評分，確保僅標示高度可疑的活動模式，並抑制更多無害警示，藉此降低整體誤報機率 (請見圖 7)：

- **第 1 階段：事件評分 —** 系統將對每個原始事件計算初始風險分數，以評定參數 (例如電腦、時間或檔案位置) 的異常性。
- **第 2 階段：威脅指標評分 —** 系統會將類似事件歸類成威脅指標，並再次評分以識別一段時間 (例如一小時或一週) 內的異常模式。
- **第 3 階段：警示評分 —** SMART 警示會將事件及威脅指標相互關聯以形成彙總警示，系統接著將根據彙總警示的組成獨特性及涉及活動的嚴重性進行第三次評分。系統會將分數不夠高、或與其他指標在同一期間不構成關聯的指標消除並認定爲誤判，避免在使用者介面造成過多的警示誤報。唯有經系統評定的嚴重 SMART 警示才會顯示在儀表板上。
- **第 4 階段：使用者風險評分 —** 使用者風險分數即針對特定使用者發出之所有 SMART 警示的彙總。系統會在 Change Auditor Threat Detection 動態儀表板上標示出風險分數最高的使用者。

但系統究竟是如何計算風險分數？系統在各階段指派的分數會將事件的整體稀有性及風險量化爲一筆特殊的標準化分數。這筆分數是根據以下三方面計算而成：

- **參數層級見解 —** Change Auditor Threat Detection 會透過一組參數 (例如：伺服器名稱、地點和時間戳記) 將行爲模型化，並將根據這些參數來區別使用者基準行爲，以及根據歷史資料瞭解其行爲模式。舉例來說，系統會將每位使用者經常存取的裝置設爲基準，任何異常裝置存取行爲皆將運算爲風險評分事件。如果此一行爲對特定使用者而言實屬高度異常 (舉例來說，該名使用者從不存取個人工作站以外的裝置)，風險分數就會提高。如果此行爲不應視爲異常 (舉例來說，該名使用者是正當存取所屬工作站以外裝置的管理員)，風險分數就會降低。

- **群組層級見解 —** 透過資料叢集技術，Change Auditor Threat Detection 會把與整體組織活動相關的使用者活動稀有性因素納入考量。舉例來說，若新型企業裝置突然遭數十名使用者存取，上述情況不應視爲獨特或可疑活動，風險分數相對較低。
- **統計見解 —** 統計見解可協助排除預期的正常行爲，以確認事件異常數量。整體風險分數將反映上述面各向的異常程度，提供可反映實際威脅層級的單一最終分數。透過結合多層次評分和多媒介見解，可免除進行過多調整的需要，確保 Change Auditor Threat Detection 可使用最小設定安裝完成並開始分析稽核資料，以鎖定使用者威脅。

結論

Change Auditor Threat Detection 不會觸發排山倒海的警示讓您應接不暇，而是透過部署進階技術 (包含機器學習和 SMART 關聯)，識別出資料和業務中眞正的重大威脅。其行爲基準、威脅模型化和多層次評分功能可對您 IT 生態系統每日產生的上百萬個事件進行系統性過濾，找出可疑行爲模式並識別風險最高的使用者。因此不論何時，需要展開調查的警示數量皆落在可應付範圍內，讓您有效並有效率地保護您的組織資料和聲譽。如需詳細資訊，請造訪 quest.com/change-auditor。

Change Auditor Threat Detection 僅需使用最小設定，即可對使用者資料展開分析以鎖定威脅。

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，讓您和貴公司可以減少管理 IT 工作的時間，進而投入更多時間發展業務創新。

專利

Quest Software 對於擁有先進的技術感到自豪。此產品可能含有已登記與申請中的專利。如需此產品適用之專利的最新資訊，請造訪我們的網站：www.quest.com/legal

商標

如果您對使用這份資料有任何疑問，請連絡：

Quest Software Inc.
收件者：LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

請參閱我們的網站 (www.quest.com)，以取得各地區及各國的辦公室資訊。