傳單

Analytics and Big Data

安全性

使用者與實體行為分析

Micro Focus® Interset 使用者與實體行為分析 (UEBA) 開拓新視野，讓您偵測、調查及應對潛藏在公司的威脅，不再等待資料遭竊才亡羊補牢。

Interset UEBA 利用機器學習技術將數十億個事件整理為實用的安全事務清單，依優先程度高低排序，以專注並加速資安作業中心 (SOC) 的工作。Interset 的機器學習模型結合高度直覺化的使用者介面 (UI)，可將威脅偵測與調查速度從數週時間加速到僅需數分鐘。

為何選用 Interset

許多組織都有重要的資產需要保護，包括客戶資訊、智慧財產和關鍵基礎架構控制等等。然而，企業保護這些資產的現行做法往往有所不足，迫使安全團隊面對僵化的規則式分析工具、零散的安全性共生體系以及永無止境的大量警告，且其中大多為誤報。在此同時，這些團隊還必須完美防範各種重大威脅，如資料竊取和未經授權的網路存取等等。

Interset 擁有獨特優勢能協助需要保護貴重資料卻無充分資安或財務資源的企業，在龐大的監控面積中找出企業應重視的威脅。Interset UEBA 不同於其他解決方案，並不依存於規則和限定值，而是根據數學機率與無人監督的機器學習模型，來評估企業內使用者或實體的潛在風險。這種方式結合 Interset 原生的巨量資料架構，讓安全團隊能夠大規模快速偵測威脅。

偵測、調查、應對。

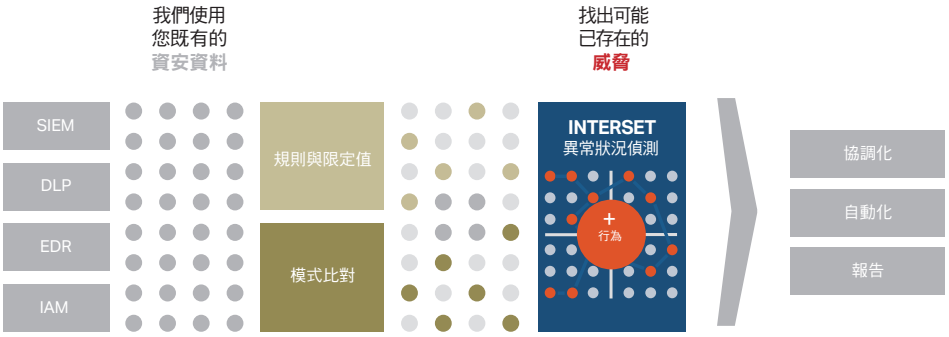


圖 1. Interset UEBA 提供檢視既有資安資料的新觀點，藉由尋找異常行為來識別潛在的威脅。其可提供實用的威脅線索，讓資安團隊能快速有效地應對並矯正問題。

無人監督的機器學習是一種不需要標籤的人工智慧 (AI)。Interset 的演算法會從記錄檔中擷取可用的實體 (如使用者、機器、IP 位址、伺服器、印表機等等) 並觀察涉及這些實體的事件，以判斷應有的行為，此即被稱作「獨特的正常」測量

威脅偵測使用案例

內部威脅
- 具風險員工
- 高風險員工
- 帳戶濫用
- 高權限帳戶濫用
- 離職員工活動

資料外洩
- 資料暫存
- 資料竊取
- 電子郵件竊取
- 列印竊取
- USB 資料竊取
- 異常資料存取
- 異常上傳

進階威脅
- 被入侵的帳戶
- 內部偵察
- 異常流量
- 異常程序
- 異常應用程式
- 受感染的主機
- 惡意通道封裝
- Bot 程式偵測

IP 盜用
- 擅用
- 監聽
- 與閒置的資源/檔案互動
- 高風險的 IP/資料存取
- 橫向移動

圖 2. Interset UEBA 使用先進的數學演算法來持續探勘數十億個資料點，找出內部威脅、資料外洩、進階持續威脅 (APT)、IP 盜用等威脅的跡象。

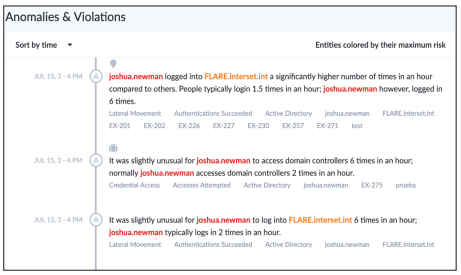
標準。隨著分析過程中出現新資訊，系統即可將事件比對先前觀察的行為，以評估潛在風險。

透過這個建立基線與評分的過程，Interset UEBA 可提高安全團隊偵測、分類、調查及應對威脅的效率與速度。Interset 的輸出風險評估可透過自動化、協調化和警告解決方案來啟動動作，以便在發現風險時比人類更快執行動作。Interset 也提供可下載的報告，摘述組織面臨的立即風險。

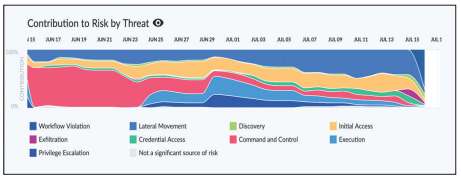
檢視風險實體

身為資安從業人員，您與 Interset 互動的主要機制便是其直覺易用的網頁介面儀表板。Interset 的儀表板讓使用者輕鬆快速地判斷哪些實體具有最大的潛在風險。識別實體後，可使用儀表板向下切入結果，透過產生的警告瞭解潛在風險，並在需要時瞭解產生這些警示的原始事件。下圖的螢幕擷取畫面顯示從最高風險使用者向下切入至原始事件的過程。

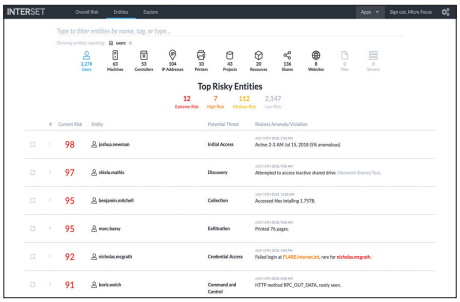
1. 檢視企業內所有實體，顯示分析結果並依實體類型分組。圖中的螢幕擷取畫面顯示使用者清單，依照風險分數由高至低列出使用者。



2. 檢視任何實體時，時間表檢視窗會顯示其風險時間變化。此觀點不僅顯示風險分數的變化，也廣泛地呈現出導致這些風險的行為類型。



3. 檢視實體時，時間表檢視窗下方會顯示與該實體相關的警告。這些警告可依關聯的實體和風險類型進行篩選，且警告是依與時間表檢視窗相關的時間順序顯示，因而可輕易透過揭開之行為與其他事件的關聯，看出其發展過程。



4. 按一下任何警告即可檢視細節，並可透過使用者基線及企業其他相關實體進一步瞭解該事件。畫面會顯示與該警告相關的風險，並詳細說明觸發該警告的模型。請注意系統會將使用者的基線與使用者本身及其他類似實體進行比較。這些相似的實體是依照統計學判定的同儕群組來決定。

5. 觸發警告的原始事件僅需一鍵即可查閱。除了查看分析的記錄檔案的實際內容外，使用者還能於此介面輸入其他查詢。

表 1. Interset 儀表板的螢幕擷取畫面，顯示瀏覽分析結果的過程

Micro Focus Taiwan facebook

網址：https://www.microfocus.com/zh-tw
電話：+886-2-5592-4949
電子信箱：taiwan.sales@microfocus.com