

## August, 2005

### Cell Technology公司提供資安事件管理平台

首先是收集各個防火牆與入侵偵測/防禦系統的事件，經由正規化的過程後加以分析處理，基本上可以產生統計報告，一覽使用狀況，這個管理平台的重點在於可以將收集到的事件做聚集 (Aggregation) 處理，將同類型的事件簡化，還有就是做相關聯分析，這個功能對於企業來說是非常有幫助的，企業可以將平常處理資安事件的流程標準化後制定規則，由這

套系統自動產生所要看到的事件分析或報表，也可將公司重要伺服器加入事件分析中，更嚴緊的區分出事件的嚴重性。

Cell Technology所發展的CMC平台就是這樣的一套系統，可支援多個廠牌的防火牆與入侵偵測/防禦的事件記錄檔，我們採用先進的AI (Artificial Intelligent) 技術，將收集到的記錄檔做聚集 (Aggregation) 處理，有效的減少

事件的數量，透過關聯性分析，找出真正嚴重需要立即處理的事件，有效的協助IT人員做好資安事件管理工作。具備延展性架構，支援2-Tier與3-Tier管理架構，可以應用在企業環境或是電信服務供應商。面對IP網路的安全威脅，提供一個及時監視與回應的系統。

<http://www.cell-technology.net/>