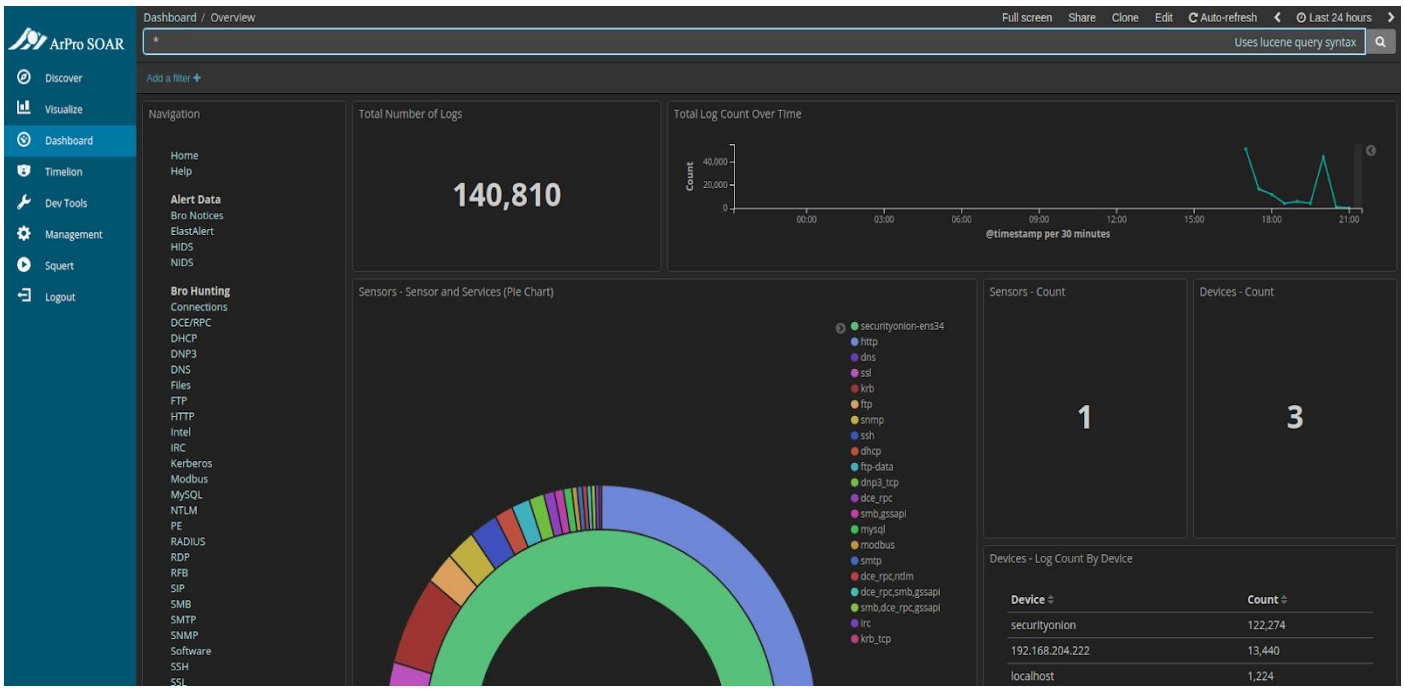
圖形化中文管理介面

監控系統可提供全中文圖形管理介面。
設備或圖形可以中文註解或搜尋。
資安協調、自動化和回應(Security Orchestration, Automation and Response, SOAR)，運作原理是將公司內部、網絡、雲端應用系統等匯集的數據，全部集中在一個儀表板系統顯示介面處理，以宏觀角度分析從各平台發出的警報。



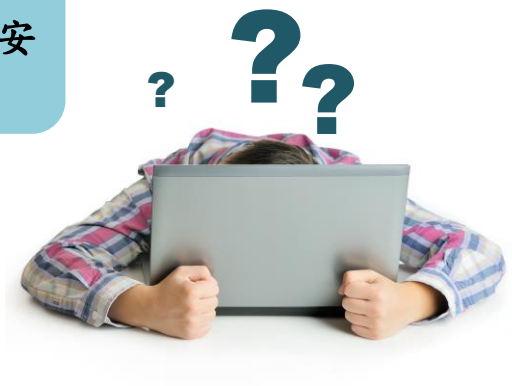
運用人工智能（Artificial Intelligence, A.I.）及機器學習（Machine Learning）技術

判斷及評估威脅的嚴重性，作分流排序，分析整個事件的來龍去脈，並按照預先設定的應變劇本（Playbook）自動回應事件。
定期進行安全審計，從多方面減少安全專才的工作負擔，以執行更重要的工作。

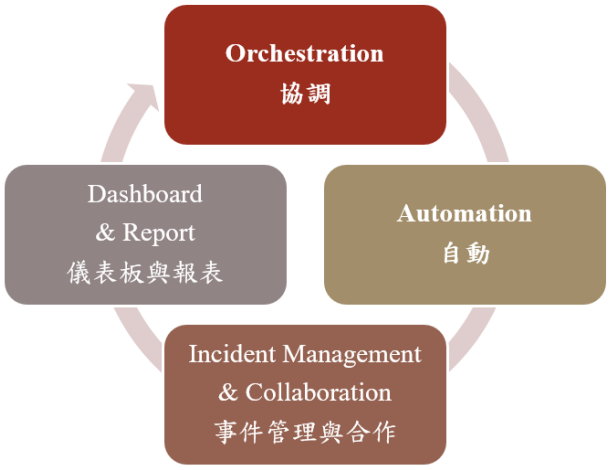
自動化工具更可令整個操作流程變得標準化及可量度，減少專才的技術能力差別及離職，重大影響資安問題。

各式的資料型式
不同的查詢方法
複雜的人工比對

冰冷的比對內容
費時的位置搜尋
令人抓狂的錯誤結果？

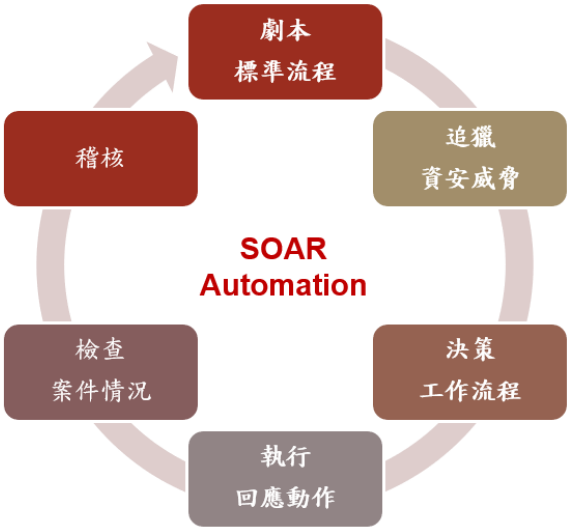


四大功能模組

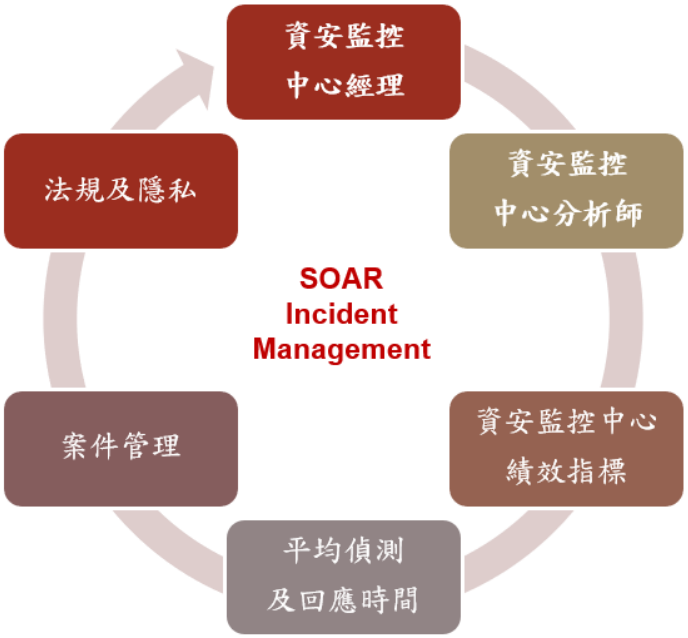


Orchestration 模組 Orchestration 基礎架構

Automation 模組事件管理與合作模組



Dashboard & Reporting 模組

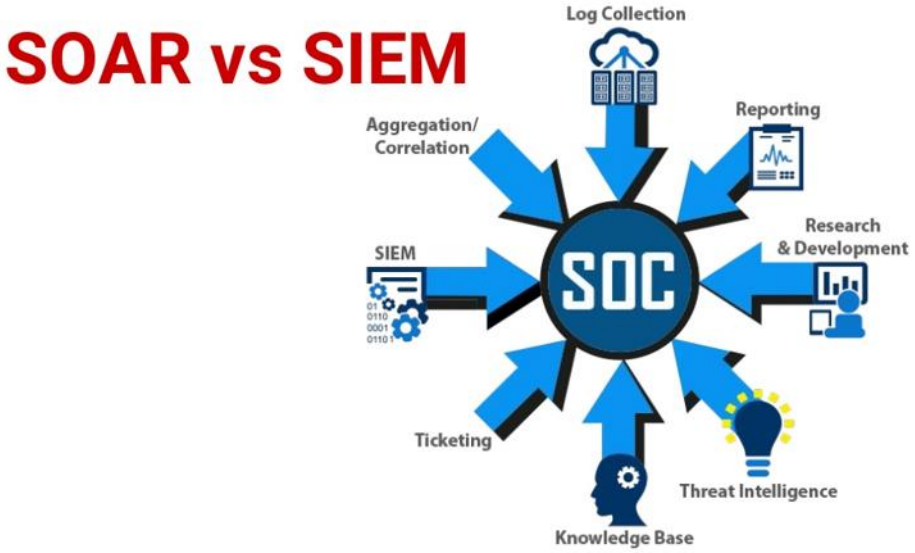


不再顯示給電腦看的資料，而是呈現給人看的資訊

- ✓資訊團隊同步了解即時事件動態
- ✓各式事件整合一站式服務
- ✓減低不必要的人工負擔與錯誤
- ✓提高事件相關資訊取得的時效性

SOAR 與 SIEM 的區別

企業需要在入侵事件的蒐證上，以過去入侵案例之應變劇本(Playbook)來進行自動化操作。管理及追蹤所有資安事件的生命週期。
擴大取得可疑資安事件資料的範圍，從多種設備及資安系統(包含 SIEM)的警示及資料。
判斷及評估威脅的嚴重性，作分流排序，分析整個事件的來龍去脈，並按照預先設定的應變劇本（Playbook）自動回應事件。



項目	SIEM	SOAR
資料來源	彙整日誌(Logs)	整併案例之入侵指標(IoC)
資料類別	Syslog為主要收集對象	警示與入侵指標(IoC)
入侵確認操作法	指令自動化操作法	劇本自動化
搜尋目標法	真實與原來事件搜尋效能優化	搜尋可疑的行為及活動
威脅標的取得法	整合弱點掃描功能	整合其他防毒系統的警示與資料
重要結果	警示(Alerts)	入侵確認與阻擋
特點	內建使用者行為分析功能	測試假陽性流程自動化

如有任何疑問歡迎隨時與我們聯絡，
專業團隊竭誠為您服務！

飛幕科技有限公司
台北市中正區北平東路 28 號 7 樓之 1
Tel：(02)2391-2961　Fax：(02)2395-6275
Web：www.maxpower.com.tw