IBM Security Resilient 進階安全性協調、自動化與應變功能

運用進階安全性協調與自動化功能提升事故應變效率。

IBM Security Resilient

重點特色

- 協助事件應變團隊快速決策與行動
- 整合 100 多種安全性工具
- 自動處理重複性的低階任務
- 充分運用 OODA Loops 作法
- 迅速應變錯綜複雜的攻擊

概覽

隨著網路攻擊能夠運用與收集越來越多的情報資料，許多企業組織疲於應對這類型攻擊。但目前技術環境亦趨複雜且相關人員缺乏技術能力，因此企業組織苦於無法有效應變相關事故。

資安團隊若要積極應變層出不窮的威脅，必須透過安全性、自動化與應變 (SOAR) 平台，才能獲得相關分析情報以利迅速決策與行動。進階事故應變協調功能可協調企業內部安全營運中心 (SOC) 的相關人員與技術。

身經百戰的 IBM Resilient® SOAR 平台可簡化應變流程，將事故應變時間從數小時縮短至幾分鐘。

打造應變團隊的決戰武器

IBM Resilient SOAR 平台能提供進階協調功能，強化團隊彈性與迅速應變的能力。

應變平台可自動處理重複性與繁瑣的任務並將正確的資訊在適切時間傳遞給合適的分析團隊，並運用協調能力降低平均應變時間，能夠讓分析人員更有效率與更具戰略性。

一間大型製藥公司運用此協調與自動化的平台因應威脅，能夠將將獲取鑑識取證的時間從 84 分鐘縮短為不到 2 分鐘。

「我們透過應變平台將處理緊急事故的時間從 84 分鐘縮短為不到 2 分鐘。」

– 跨國製藥公司的網路安全處長

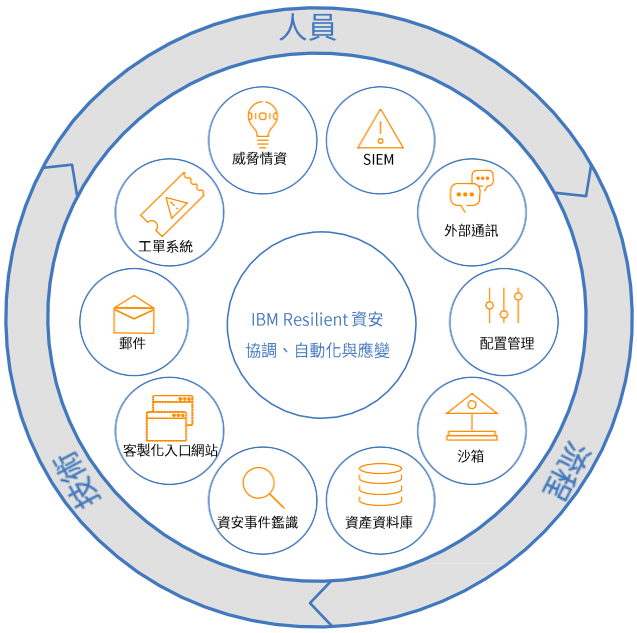

圖 1：IBM Resilient SOAR 在事故應變協調流程擔任中央樞紐的角色。

協調平台功能

企業組織可運用 IBM Resilient SOAR 平台的最新技術打造協作、彈性與迅速事故應變流程所需的工具。Resilient SOAR 平台的概念源至於美軍的 OODA 循環理論 (Observe、Orient、Decide 與 Act)，讓企業組織得以透過此循環流程迅速準確地取得相關分析資料。

Resilient 平台還可以整合 100 多種安全性工具，協助您串聯現有安全性環境與 IR 流程，打造一個事故應變協調的中心樞紐。

Resilient SOAR 平台的最新協調功能包含：

- **彈性戰略計畫**：提供您敏捷與精細的計畫以對抗錯綜複雜的攻擊。彈性戰略計畫會自動依據即時事故條件進行調整，並在分析人員開啟事故資料前，就能完成重複性的初步分類作業。
- **視覺化工作流程**：協助分析人員運用整合任務與技術的視覺化複雜工作流程，進行協調事故應變。
- **視覺化事故資訊**：以圖像顯示事故工具或入侵指標 (IOCs) 與企業組織與企業組織環境內事故之間的關聯。
- **分秒必爭**：在工作流程中設定時間管理規則，確保團隊能及時應變、找出瓶頸並遵循企業 SLA。
- **工具工作流程**：提供工具之間的自動化工作流程，和以人為本的任務與核准流程。
- **任務與指令碼**：您可以為工作流程新增平台內指令碼功能，以啟用平台內自動化功能。

效益：

CIO 與其資安團隊可以運用 SOAR 平台獲得以下效益：

加速應變錯綜複雜的攻擊

透過整合 100 多種不同技術，協助安全性組織應變錯綜復雜的攻擊、展現安全性成本的商務價值，以及提升整個安全性堆疊的 ROI。

提升與測量 SOC 生產力

透過整合現有安全工具，及根據攻擊手動與自動化調整應變流程的功能，協助 SOC 主管提升與衡量其生產力。嚴格執行 SLA 並確保合適的分析師可以使用適切的工具正確的執行任務。

消弭技能落差

加倍提升生產力，能夠協助資安分析師管理精心策劃的複雜威脅，並透過自動化分類與強化任務品質，將精力著重在威脅的偵測與應變，而不是疲於使用不同的工具。

提升資料外洩通知流程

提供全球法規與應變計畫知識庫，協助使用者找到對應的最新法規，遵循隱私權外洩法規的同時化繁為簡，進一步簡化隱私權應變管理。

協作您的應變流程，讓您的資安團隊能夠更快速及更有智慧地行動。

更多資訊

立即造訪 IBM 官網 Resilient Incident Response Platform：

ibm.com/tw-zh/marketplace/resilient-soar-platform

2020 年 5 月

BUD03063-USEN-00