SafeCove SOAR 資安事件自動回應包(每年訂閱)

產品簡介

頻繁的針對式資安攻擊事件，對於企業與政府機關的資安防護維運作業形成巨大的質量上的衝擊。如何利用 SafeCove SOAR 自動化回應機制來提升資安事件的處理能量，將大量重複性的資安事件處理工作，以 SOAR 平台的流程引擎及資安設備整合能力來將人力作業轉變為自動化作業，提升資安事件處理效能與增進事件回應能力，已經為各企業與政府單位資安長在構思新世代資安治理與防護架構中的重要一環。

現代的資安防護思維觀念，已經由事後的被動防禦觀念轉變為事前的主動防禦戰略，才能抵擋先進的駭客刺探與勒索軟體攻擊。SOAR 的流程引擎可將工作流程標準化，以自動化流程系統性處理資安事件，減低人力處理出錯的機會與過度的人力投資，從而增進資安事件的處理能量。SOAR 可整合多樣化的資安設備、事件管理系統與 SIEM 平台等，同時 SOAR 系統內建的事件自動化回應腳本，透過系統流程整合規劃與設定，則可擴大資安事件處理自動化與整合能力，提升自動化腳本的工作含蓋範圍，加大自動化事件回應的完整性。

SafeCove SOAR 資安事件自動回應包，秉持安碁資訊多年資安維運經驗，可將常見資安事件處理流程、資安設備維運流程等高度重複性與可流程化的作業，透過 SOAR 自動化資安協作平台，進行自動化腳本的開發與導入。整合 SOC 監控平台的事件通報機制，自動觸發 SOAR 系統上對應的自動化腳本，進行事件回應自動化的整合。透過 SOAR 平台可導入以下常見的自動化 Playbook，相關範例說明如下：

1.強化設備防護能量

SOAR 定期自動至安碁資安威脅情資平台取得中繼站清單（IP 位址、網域名稱），並將清單處理為可供防火牆介接之格式，貴司之防火牆便可即時根據此清單進行阻擋，可避免防火牆設定未同步之問題、大幅減少週期性反覆作業之人力負擔，並有效起到防護與偵測之作用。

2.半自動情資整合至資安設備

以往額外獲得的重要 IoC 情資需要透過層層關卡溝通，才可以將情資設定到資安

設備進行防護與偵測，此一過程費時費力。在導入半自動情資整合至資安設備 Playbook 的輔助下，透過電子郵件整合至 SOAR 平台，維運人員只要將 IoC（如：網域名稱、IP 位址、檔案 Hash 等）寄送至貴司特定電子郵件信箱，SOAR 平台即會取得與解析內容，並自動地將 IoC 情資導入各式資安設備，這樣便可起到防護與偵測之作用。

3.整合 SOC 通報自動化阻擋威脅

為加快事件處理速度，縮短作業人員手動將威脅來源匯入至資安設備進行阻擋的時間，本情境與 SOC 通報單進行整合，由 SOC 將必定要執行阻擋的通報單，寄送至貴司特定電子郵件信箱，SOAR 平台收到信件後即解析內容，並將威脅來源（IP 位址）自動化導入各式資安設備，達到防護與偵測之作用。

產品功能說明

項目	內容說明
產品功能	
SafeCove SOAR 系統功能	●SOAR 重點功能： – 整合 1000 多種第三方系統，如資安設備、事件管理平台、SIEM 等。 – 內建自動化流程引擎。 – 原廠提供各設備自動化腳本與第三方整合介面。 ●提供 2 個自動化腳本，包含防火牆黑名單自動新增、IPS 黑名單自動新增。
技術支援	

產品授權

產品名稱	授權內容
SafeCove SOAR 資安事件自動回應包(每年訂閱)	● SafeCove SOAR 授權 ● 2 個自動化腳本，FW、IPS 黑名單自動更新

產品售價

- NT$190 萬(含稅)

交付項目

- SafeCove SOAR 資安事件自動回應包授權(每年訂閱)

SOAR 系統安裝硬體需求

- CPU ： Intel 8 核心 2.0 GHz 以上
- 記 憶 體： 64 GB
- 硬碟空間： 500 GB 以上
- 作業系統： Linux

預期效益

- 系統支援廣泛之資安設備，可透過 API 與內建腳本自動協調各式資安系統，建立資安與 IT 維運之自動化腳本。
- 流程引擎可 提升自動化應變能力，從而達到縮短事件應變時間、降低維運人力之目的，並建立標準化之威脅處理流程。
- 改善、補強傳統資安維運工作所難以達成的部分，建立高敏捷之全網整體安全維運防禦體系。