Splunk SOAR

現代安全營運中心 (SOC) 的安全協調、自動化和回應 (SOAR)

- 自動化警示分類和重複的安全工作，使您能夠更聰明地工作，並專注於關鍵性的目標。
- 在幾秒鐘內調查和回應安全事件，而無須耗時數小時。
- 跨工具和團隊協調工作流程，提高 SOC 的效率和生產力。

採用自動化技術增強 SOC 的生產力，並能夠快速應對威脅

安全營運中心 (SOC) 其實已經不堪負荷了，因為分析人員已經被安全警示淹沒。每天需要進行全面調查和解決的警示實在太多，而且安全營運的工作單調、固定又重複，尤其是在一級分析師的層級。當今全球缺少超過一百萬個具備足夠知識和專業技能的資安專業人才，才能充分滿足安全營運中心的人員需求，而且現在我們發現、分類和回應威脅的平均時間仍然太慢。

不要再被壓垮了，掌控全局才是正解。Splunk SOAR 提供了安全協調、自動化和回應能力，能增強您的 SOC。Splunk SOAR 可以讓安全分析人員更聰明地工作，而不是疲於奔命。它可以自動化重複性的工作，加快安全事件的分類，透過自動偵測、調查和回應來提高生產力、效率和準確性。此外，它還可以透過協調團隊和工具之間的複雜工作流程來加強防禦能力。Splunk SOAR 還支援了各種安全功能，包括事件和案件管理、整合威脅情報、協作工具和報告等。

大部分的警示和重複性工作都可以在不需人力介入的情況下解決

Splunk SOAR 可以在幾秒鐘內自動處理警示分類、回應和過去手動重複性的工作，若以人工處理，可能需要幾分鐘甚至幾小時的時間。透過使用自動化劇本不同的單點產品之間協調和執行操作，安全團隊可以免除分析師繁重的工作，提高效率，同時也可以讓他們有更多時間專注於更重要的工作。告別警示疲勞。現在，您的團隊可以從不堪負荷轉換成可以掌控一切。

使團隊的產能倍增

SOC 人力其實嚴重不足。現在業界非常缺乏專業的網路安全人才。但有了 Splunk SOAR，您可以讓三人小組的工作效能達到十人的效果。Splunk SOAR 可以自動化重複性的工作、調查和進行回應，讓您的安全團隊提高生產力，發揮現有人員的最大價值。

讓您的工具更好地協作

Splunk SOAR 可以協調您 IT 和安全堆疊中的工作流程和回應，讓每個產品都能積極參與防禦，讓這些工具更好地協同作業。透過整合現有的安全基礎架構，可以強化防禦，創造一個保護網，讓攻擊更難以得逞。

Splunk SOAR 支援超過 350 個第三方工具和 2,400 多個動作，因此您可以跨團隊和工具連接和協調工作流程。這不僅能加快了您調查和回應的速度，還能發揮先前投資的價值。

從 30 分鐘縮短成 30 秒

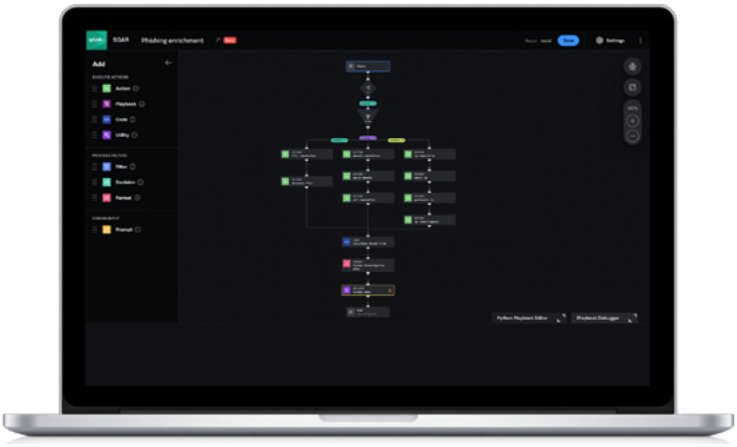
平均偵測、分類和回應威脅的時間太慢了。使用 Splunk SOAR，您可以在幾秒鐘內回應威脅，而不是幾分鐘或幾小時。使用 Splunk SOAR，您可以利用自動化劇本來跨多工具自動執行安全工作，以機器的速度降低縮短威脅的平均時間 (MTTD) 和回應威脅的平均時間 (MTTR)。

按照自己的方式使用 SOAR

您可以根據業務需求、簡化安全營運和促進數位轉型的需要，選擇以最適合的方式部署 SOAR。Splunk SOAR 支援本地部署、雲端部署或混合部署。

自動化變得更簡單

我們的視覺化劇本編輯器讓建立、編輯和實施自動化劇本變得更加容易。您無需編寫程式碼，只要使用拖放式介面即可，如此一來任何人都可以進行自動化。藉此，您的團隊能夠擴展自動化以滿足您的業務需求。



了解更多 Splunk SOAR 的特色和功能。

21-19335-Splunk-Splunk SOAR-PB-113