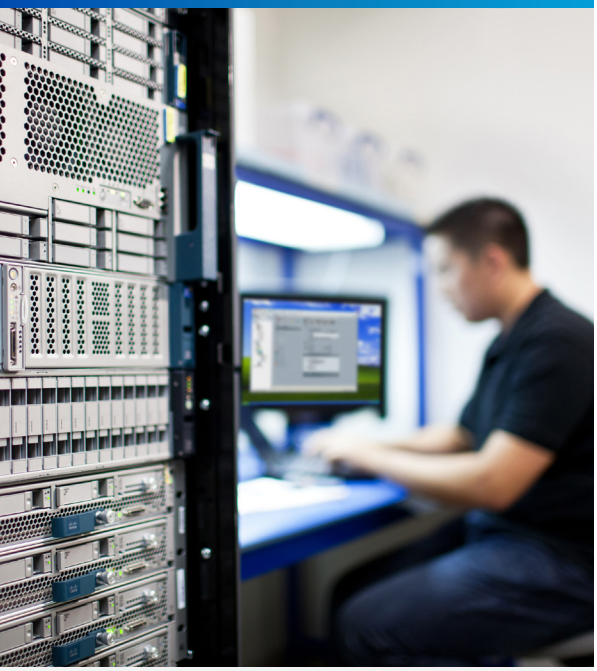
威脅管理



優勢

- 透過可處理整備度和回應的全方位做法，獲得更強健的安全狀態
- 借助經實證的方法、獨特的情報與經驗豐富的團隊之力，對進行中的防護措施更具信心。
- 藉由採用創新技術及專家提供的廣泛持續分析，獲得更高的可視性並對您的作業及基礎架構有更深的瞭解

思科資安顧問諮詢服務
事件回應

組織隨時隨地都可能遭受攻擊。根據 IDC 調查，2014 年的資安缺口問題耗費了近 5000 億美元。同時，思科 2015 年度資安報告指出，全球的資安專業人力資源短缺，估計有一百萬個職缺等候填補。

今日不斷變動的威脅概況

這個人才短缺情形結合事件不斷增加的現況，導致多數組織的資安狀態普遍疲弱。成功的攻擊會造成巨大的金錢損失、智慧財產喪失、客戶資訊與機密危害，以及公司估值降低。

思科®資安事件回應服務可大幅加強您的網路與資訊安全防禦能力，使用最新情報與最佳實務，引入了涵蓋所有防禦層的處理程序，並提供全方位功能，可協助組織快速且有效地針對事件進行準備、管理、回應和復原。

只有 50% 的 CISO 強烈同意「判斷入侵範圍、加以遏止和從惡意攻擊中修復相當容易」

— 2015 思科年度資安報告

透過整備度與回應獲得更強健的安全狀態

思科®資安事件回應服務是包含在思科顧問諮詢資安服務中的解決方案，提供專業知識，有助於採用和設計可促進企業成長、降低成本與減輕風險的安全做法。綜合最佳實務並利用有效的業界安全框架，思科的事件回應團隊提供的全方位功能可為組織提供協助。我們的事件回應團隊由資訊安全專家組成，並結合他們獨特的執業、企業安全和技術安全背景。這支團隊會直接與綜合資安情報 (CSI) 團體合作，攜手識別已知與未知威脅、量化和優先排序風險，以及降低未來風險。

讓我們的專家與您共同制訂新計劃、重新評估現有計劃或在發生攻擊時提供迅速協助。

思科資安顧問諮詢服務：事件回應

整備度：主動式服務

- **基礎架構入侵整備度評估**藉由評估網路設計、安全性控制、作業系統、人員安全性設定、自動修補系統、防火牆、記錄以及其他相關系統，思科得以深入瞭解用戶端環境、預測潛在攻擊媒介，並建議必要的安全控制措施。
- **安全作業整備度評估：**思科根據先前事件和目前的角色與責任來評估安全團隊的整備度，針對貴機構是否具備各類型調查所必要的資源、知識和工具提供建議。
- **作業整備度評估：**評估您的作業模式與活動，進而提供可協助未來事件的建議。
- **缺口通訊評估：**思科會協助您建置具有適當合規性結構的通訊框架，用於董事會層級、整個組織的供應鏈以及與客戶間外部範圍的協調覺察與回應。
- **資安作業與事件回應訓練：**提供領導、協調和支援事件所需的最新技能訓練。此外，也會向資安作業人員提供惡意軟體分析和各種資安工具的技術訓練。

回應：反應式服務

- **評估與調查：**藉由受感染系統的技術回顧，判斷攻擊方法並協力破解惡意程式碼，包括其軌跡、目的地和最終目標。
- **因應對策制訂：**制訂因應對策，用於協助偵測、隔離、追蹤和阻止攻擊者的進一步動作。這些措施可能會產生入侵、資訊洩漏和弱點惡意利用指標。
- **因應對策部署：**部署所有專為偵測和阻止事件制訂的因應對策，且所有過程皆須符合資訊安全和廠商最佳實務。
- **因應對策驗證：**驗證新制訂的因應對策之有效性，並編撰任何設計所需加強事項的效能檢討。產出內容包括要提交給董事會、監管機構和執法機關的文件，其中將詳細說明事件摘要、緩和措施及損失（如適用）。

案例研究

案例研究：零售公司

挑戰
客戶遭入侵，但缺乏可回應進階威脅的資安專家，且基礎架構無法封鎖惡意軟體。

解決方案
在七天的參與期間，思科透過網路鑑識、惡意軟體樣本分析、惡意軟體因應對策制訂、網路異常情況偵測及全方位情報回顧提供了自訂惡意軟體偵測功能。

成果

- 提供有助於建立牢靠安全狀態的資料，且這些資料與端點惡意軟體、傳輸中資料和基礎架構中的整體通訊功能相關。
- 在基礎架構中找到多種商品惡意軟體，而客戶的傳統 AV 解決方案並未捕捉到這些惡意軟體。
- 利用可揭露安全缺陷、錯誤組態和應用程式缺點（與安全有關）的解決方案提高網路可視性。

思科的事件回應可能包括下列任何或全部用於隔離和修復攻擊的措施：

- 記錄來源評估
- 分析與資料挖掘
- 鑑識調查影像分析
- 受感染系統動態檢測
- 惡意軟體反向工程
- 入侵程式分析與重新實作

後續步驟

請立即前往 www.cisco.com/go/securityservices 洽詢我們的顧問，為您的業務提供防護。

DEC14CS4667 07/15