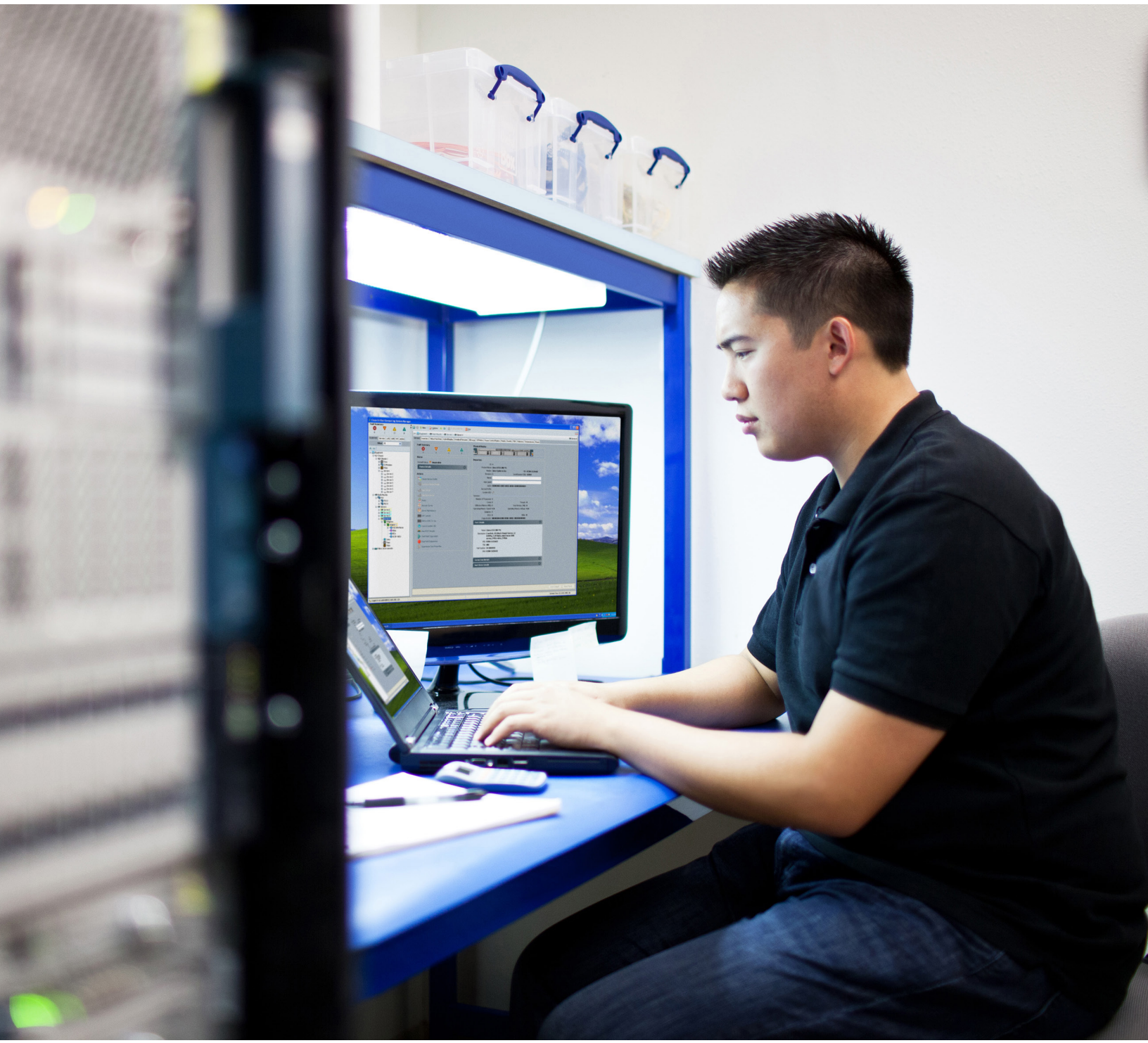
資訊安全分析及其他

建立一個高效的資安事件回應計畫



學習內容

透過此白皮書，IT 及資安團隊人員能夠學習打造高效事件回應計畫的必要元素：

- 瞭解目前的資安事件回應計畫為何無效
- 建立適合的事件回應團隊
- 開發成功的回應程序
- 選擇適當的資安技術
- 利用 NetFlow 及資安分析大幅提升事件回應和鑑識

攻擊事件持續攀升

從大型零售業到醫療保健及政府機構，沒有人能從今日複雜、目標明確的網路攻擊中全身而退。無論攻擊者是要獲取金融資料、商業機密或保密資訊，不斷演化的威脅面貌和迅速成長茁壯的網路環境都讓他們有更多方法入侵我們的系統。

攻擊者早晚會入侵您的網路。他們會使用零時差攻擊、遭竊的存取憑證、被感染的行動裝置、脆弱的事業夥伴或其他戰術。

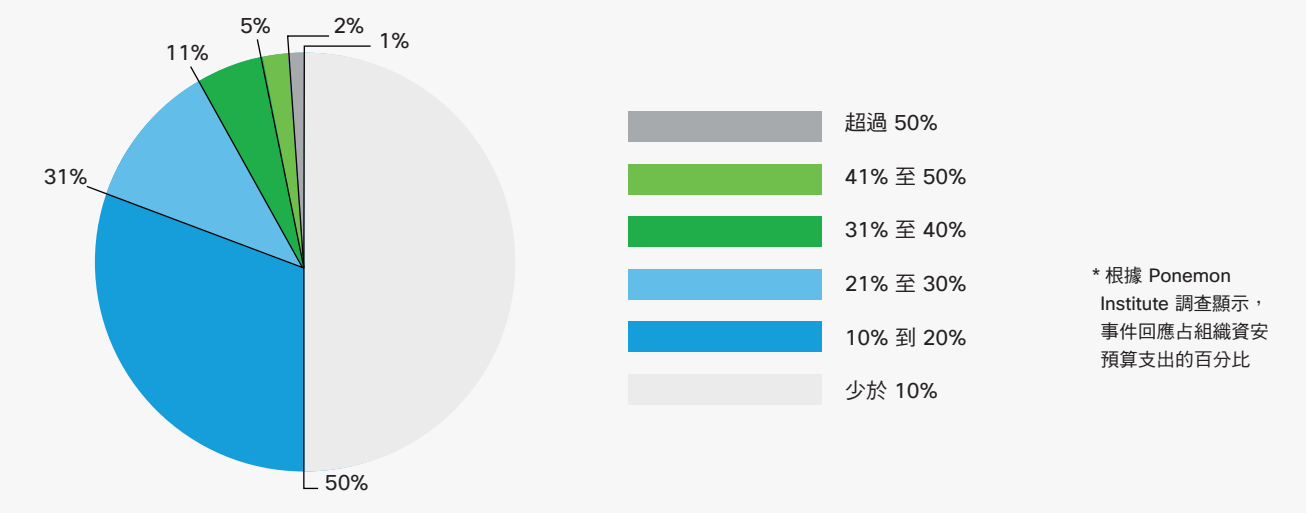
資安的成功不僅僅是將威脅擋在您的網路之外。相反地，應該是在發生攻擊時，快速回應並攔截攻擊。

根據 Gartner 的說法：「組織都無法及早偵測到資安缺口，而且被入侵的組織都未能偵測到超過 92% 的資安缺口。」[1] 顯而易見地，我們都需要更主動積極地保護我們的組織。我們需要持續監控基礎設施的動態，以及採用既定、週期循環的方法在攻擊大肆破壞網路和聲譽之前予以回應。

資安事件回應缺點

在 Ponemon Institute 進行的研究調查中指出，大多數的受訪者都同意組織能減少未來資安缺口的最佳作法是提升其資安事件回應能力。但在當時，有一半的受訪者表示花費在資安事件回應上的支出低於整體資訊安全預算（圖 1）的 10%。[2] 根據另一項調查顯示，90% 的大型企業表示他們一整年都會發生重大 IT 事件，但只有約一半的企業設有事件回應團隊來處理此類事件。[3]

圖 1. 資安事件回應支出



從世界最知名品牌和機構所持續遭受的大量攻擊看來，資安事件回應仍然有漫漫長路要走。今日的駭客在網路上沒有被偵測到的時間仍然是一個讓人無法接受的天數：平均達 100 到 200 天。[4]

[1] Gartner「安全資訊及事件管理的魔術象限」(Magic Quadrant for Security Information and Event Management)，2013 年 5 月
[2] Ponemon Institute「網路安全事件回應 - 我們是否自以為準備妥當了？」(Are we as prepared as we think?) 2014 年 1 月
[3] Dimensional Research「2016 年主要資安事件管理趨勢」(Major Incident Management Trends 2016)，2015 年 12 月
[4] 思科 2015 年年中資訊安全報告

「組織都無法及早偵測到資安缺口，而且被入侵的組織都未能偵測到超過 92% 的資安缺口。」

– Gartner

支援資安事件回應計畫

事件回應包括用於偵測和回應資安事件的人員、流程和技術。其中每個部分（人員、流程及技術）對於建立和實施有效的資安回應計畫而言同樣重要。

人員

哪些人應該參與組織的資安事件回應計畫？所有人。

CSIRT

首先最重要的是，企業組織需要設立全功能「電腦資訊安全事件回應團隊」(CSIRT)，其中包括受過訓練、專屬的資安專業人員。每個組織（無論大小規模為何）都應該有至少一名指定人員負責電腦資訊安全事件回應。作為資安專家並不代表就一定是資安事件回應方面的專家。資安事件回應專家必須具備處理高壓回應情況的特定背景知識，或是受過訓練而可處理高壓回應情況。有一位專職的事件回應人員，不同時負責其他 IT 和資安職能也很重要。

資安事件回應團隊應該對於網路及其資產有深度瞭解。在今日的許多情況下，攻擊者會進行徹底勘察及深入瞭解其目標網路，比受害組織自己的 IT 或資安團隊更瞭解。適當技術可以協助資安事件回應人員探索網路上的資產、決定哪些資產最重要而需要保護，以及基準正常行為而可快速識別異常情況，進而找到攻擊所在。

IT 以外範圍

對於資安事件回應，不僅僅是需要設立適當技術團隊。除了 IT 團隊以外，法律、管理、人資、公關和其他部門的主要利害關係人都應該在組織的資安事件回應計畫中扮演不可或缺的角色。組織需要瞭解這些團隊在發生事件時應採取的行動。他們需要在事件發生之前建立角色和職責，然後將這些人員引進早前的規劃中。讓高階管理層知道資安事件回應程序、成功和挑戰也很重要，如此才能確定這些作為都獲得適當程度的關注和資金，而能發揮成效。

最後，在理想的世界中，所有員工甚至是與組織合作的第三方都應該協助支援資安事件回應團隊。訓練員工，讓他們瞭解在發生社交工程事件時要留意的事項。仔細篩選、進行背景檢查並查詢可存取您的網路或甚至是貴公司相關機密資訊的任何第三方的安全性。還有，別忘了內部威脅。訓練經理以留意並向人資回報可疑的員工行為，然後訓練人資以便和 IT 溝通這些疑慮。

「Stealthwatch 可讓資安及事件回應團隊比以往更快速地補救事件、縮短停機時間和降低管理網路及網路服務的整體成本。」

– Telenor Norway

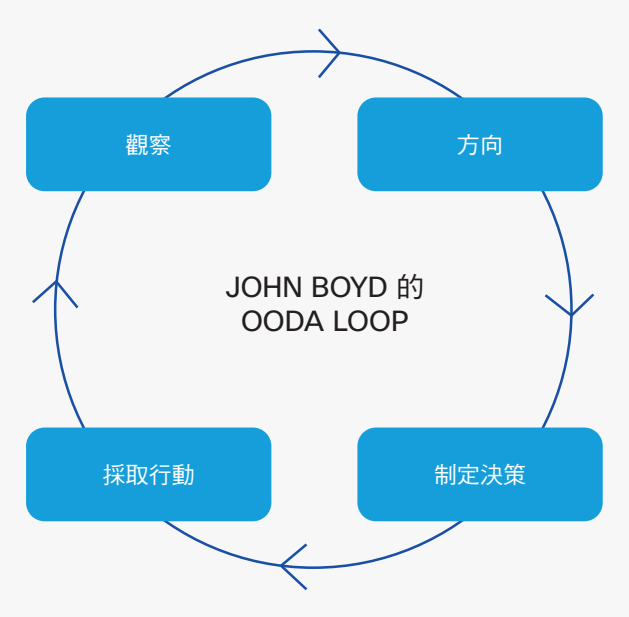
程序

事件回應不能是事後聰明。企業組織需要有明確建立、考慮周全的資安回應計畫，其中會整合整個企業中的重要人員和團體。

為了確實發揮成效，資安事件回應計畫應包含：

1. **為所有參與人員設定非常明確的角色、職責和核准程序**，同時制訂規則，明確定義可以採取及不可採取的行動與時間。例如，事件回應團隊是否可讓機器離線，而不需要獲得額外核准，以便阻斷攻擊？清除電腦或阻斷特定服務的存取權限如何呢？這些行為在必要情況下是被允許的嗎？此外，發生資安漏洞時，公司的法律、法規和合約義務為何？重要的是在發生事件之前，以書面方式準備好這類問題的回答。理想情況是您的資安事件回應計畫應該在制定政策（以確保在危機中制定適當決策）但不要有許多層核准程序（因而妨礙技能熟練之回應人員的成效）之間取得完美平衡。
2. **定期訓練和評估練習**。公司的資安事件之間可能間隔一段時間。在那段時間內，重要的是不斷訓練所有相關員工並進行練習以評估他們在事件發生時的準備程度。此外，真正發生資安事件時，請別忘了將事件作為衡量您團隊成效的機會。運用一些指標，例如識別資安問題的平均時間 (MTTI)、瞭解根本原因的平均時間 (MTTK)，以及修正資安問題的平均時間 (MTTF) 等基準，可大幅協助您改善回應流程，以及向高階管理層展現投資報酬率。
3. **與公司高階管理層定期溝通資安事件回應規劃工作的努力和成功**，以確保此工作流程獲得適當的關注及投資，並使管理層瞭解其對業務持續性的關鍵作用。
4. **對於組織基礎設施和關鍵重點的徹底瞭解**。檢視網路內部的典型活動，以及來自外部世界的可靠威脅情報都是事件回應的關鍵部分。
5. **意見反應迴圈可確保事件不只是被清除**，同時也是被調查。必須以鑑識方式，擷取關於攻擊者及其所用方式的重要詳細資料，以便預防類似攻擊。軍事戰略家 John Boyd 發明 OODA Loop 作為在對抗作業中制定決策的架構(圖 2)。今日，OODA Loop 已經應用於許多其他領域，而且可作為有效事件回應所需之持續程序的優異範例。

圖 2. OODA Loop



技術

同樣重要的是讓適當人員和既有程序在事件發生之前預先部署適當技術。

來自外部的威脅情報對於掌握已知攻擊而言非常重要，但如果沒有協助資安事件回應團隊取得關於網路活動的關鍵見解的工具，回應努力將無效。畢竟，您無法保護自己看不見的部分。

事件回應不只是清除惡意程式並讓受感染的電腦回復連線狀態。需要完成進一步調查，才能判定完整範圍的攻擊、其他機器是否受到感染，以及攻擊者使用的戰略類型。如此您就能確定完全從環境中根除攻擊，而且相同確切的攻擊不會再次發生。

> 「Stealthwatch 可將解決問題的時間從數日縮短為數分鐘。有了 Stealthwatch，我們可以在潛在攻擊和資安缺口之前提前得知並預做準備。」
>
> – Edge Web Hosting

網路稽核軌跡

查看今日大型、複雜網路動態的最佳方式是收集和分析網路稽核軌跡。事實上，Ponemon 調查的 80% 受訪者表示從 NetFlow 此類來源的稽核軌跡分析和封包擷取是偵測安全性事件和資安缺口最有效的方法。[5]

使用網路活動記錄，組織可以更輕鬆地得知和阻斷攻擊嘗試行為。尤其，NetFlow 是高度有效的技術，因為其可在整個網路中進行收集，而不需要安裝專屬的探測器。而且能以經濟實惠的費用儲存長期資料。

NetFlow 的威力

思科首創且現在固定應用於廣泛網路基礎設施裝置的 NetFlow（連同其他類型的網路遙感勘測）可從現有路由器、交換器和防火牆提供寶貴中繼資料，以提升可視性和情境感知。其提供透過網路進行之每個連線的記錄，包含「目的地」(to) 和「出發地」(from) 位址、連接埠號碼、所傳輸資料數量和其他資訊。

NetFlow 可能會揭露關於您網路資產和行為的無數寶貴詳細資料：對話對象、正在使用的應用程式等等。

大多數組織都已經能夠存取環境中的 NetFlow。他們只是必須開始收集和分析 NetFlow，才能獲得對網路更高程度的新見解。但並非所有 NetFlow 監控技術都能創造相同效果。

隨著我們今日經歷的持續網路演化，網路會產生巨量的大數據。存取該數據是理想的第一步，但令人遺憾的是，如果事件回應團隊無法瞭解其中意涵且無法用這些資料來提升感知和制定更理想的決策，那一切都沒有意義。這就是我們為何需要 Cisco® Stealthwatch 這類進階、以流程為基礎之監控解決方案的原因。

Cisco Stealthwatch

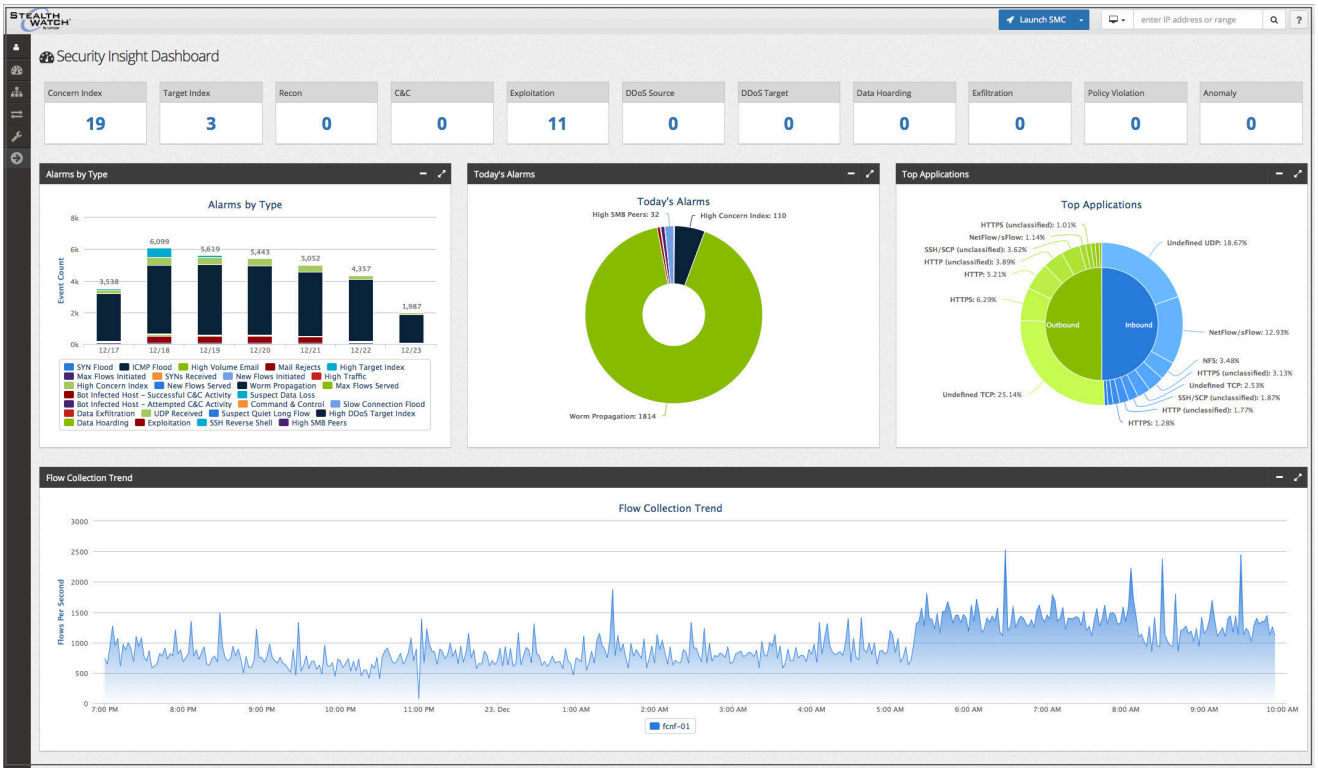
Cisco Stealthwatch 可作為網路的耳目。其可迅速收集和分析大量 NetFlow 資料，以便為安全性及回應團隊提供深度可視性和可行情報。其可提供早前討論的深度網路瞭解和網路活動基準線，而這對於建立穩健資安事件回應程序而言至為關鍵。

此外，與思科其他安全性技術整合時，Stealthwatch 可協助組織以具成本效益的方式使用其現有基礎設施，將其網路轉化為持續運作的安全性感測器，而可更順暢無縫地偵測威脅。透過精密的行為分析，Stealthwatch 可自動偵測會導致廣泛攻擊（從零時差惡意程式和分散式拒絕服務 (DDoS) 攻擊到進階持續威脅 (APT) 和內部威脅）的可疑行為。

Stealthwatch 可大幅降低與資安事件調查相關聯的手動分析。其通常可將疑難排解時間從數日或甚至數月時間縮短為數分鐘。直觀的儀錶板和報告可讓資安及事件回應專業人員按幾下滑鼠，就能快速取得所需資訊，無論是網路活動的整體情況、潛在問題的清單，或是特定主機的檢視（圖 3）。此資訊也能與其他利害關係人（例如，高階管理層）輕鬆分享。

[5] Ponemon Institute「網路安全性事件回應 – 我們是否自以為準備妥當了？」(Are we as prepared as we think?) 2014 年 1 月

圖 3. Stealthwatch 儀錶板



Cisco Stealthwatch 提供進階網路可視性和安全性情報，以加速事件回應。

也許內部人員會反覆嘗試存取網路受限制區域。或許會從網路傳出異常大量的資料，或是內部主機與外國的可疑 IP 位址通訊。有效的網路可視性及安全性分析工具可挑選這些行為並警告管理員進行進一步的調查。

「80% 的受訪者表示從 NetFlow 此類來源的稽核軌跡分析和封包擷取是偵測資安事件和資安缺口的最有效方法。」

– Ponemon Institute

Stealthwatch 差異

與只會監控進出網路的流量的許多其他技術不同之處在於，Stealthwatch 也會監控橫向（東 - 西）流量以偵測散布在網路內部的攻擊並識別內部威脅。透過持續監控異常行為的網路，以及使用進階安全性分析、警報和報告以警告管理員處理潛在問題，Stealthwatch 能夠更快速且更有效率地回應事件。

一般而言，處理 NetFlow 比完整封包擷取等資源密集型替代方案需要的資源更少。但全球企業的普遍記錄可能還是會產生超過每秒 100 萬個流程的記錄數量。有效的解決方案必須要能夠適當地進行擴充，以減少儲存量和能耗量。Stealthwatch 的大量可擴充性以及對單向流程記錄進行重複資料刪除和拼接的能力，甚至可為最大型、最複雜的企業網路實現具成本效益的流程監控和儲存。

除了提升即時威脅偵測以外，Stealthwatch 也會協助您更快速且更徹底地進行鑑識調查。其可儲存數月或甚至數年的流程資料並使用進階查詢功能，快速擷取關於之前攻擊的適當資訊。這項歷史回顧對於微調事件回應程序以改善威脅抵禦效果而言至為關鍵。隨著網路持續擴充且隨雲端、軟體定義網路 (SDN) 和物聯網 (IoT) 架構演化，有效率地收集、分析和解讀大量網路及資安資料愈趨重要。

> 「在 Stealthwatch 之前，我們是手動分析並將網路活動資料產生關聯。Stealthwatch 會透過單一且易於使用的介面，自動為我們提供詳細的網路見解，從而協助提升資訊安全、網路作業和法規遵循成效。」
>
> – BlueCross BlueShield of Tennessee

增強型資安內容及整合

研究顯示，69% 的組織表示他們的資安工具並未為他們提供足夠內容，因而使得他們無法瞭解自己面臨的風險。[6]

透過組織自己的技術和產業合作（包含與其他思科技術的緊密整合），Stealthwatch 還可引進其他資安訊息內容，以進一步加速和提升事件回應和鑑識效果。

這些增值情報層的範例包含：

- 使用者和裝置感知
- 雲端可視性
- 應用程式感知
- 威脅回饋資料
- 端點資安整合
- 代理伺服器可視性
- 封包擷取

從單一主控台存取所有這些資訊，可大幅簡化威脅調查及補救。事實上，根據 Enterprise Strategy Group 所述，80% 的組織相信他們的事件偵測和回應程序都因為缺少資安技術整合而受到阻礙。令人遺憾的是，不連貫的解決方案會降低威脅緩解的速度，而且會留下讓攻擊者能更輕鬆利用入侵的資安漏洞。增強型資安內容和深度整合可讓組織更自動、順暢且有效地回應組織今日面臨的所有威脅。

結論

令人遺憾的是，目前還沒有任何技術可將駭客完全阻擋在企業網路以外。但是，如果組織透過適當的人員、程序和技術配置定期監控自己的環境，即使攻擊仍在進行中，資安團隊也能具備更多能力而可精準找到並停止攻擊，因此可避免災難性結果以及與資料漏洞相關聯的成本。

[6] Ponemon Institute「特權使用者濫用及內部威脅」(Privileged User Abuse & The Insider Threat)，2014 年 5 月
[7] Enterprise Strategy Group,「處理攻擊偵測及事件回應」(Tackling Attack Detection and Incident Response)，2015 年 4 月

更多相關資訊

Stealthwatch 整合了思科廣泛的資安產品組合，而可從邊緣提供全方位保護和簡化的事件回應以進行存取：跨網路、數據中心、端點、行動裝置及雲端。

按一下此處以閱讀思科自己的 CSIRT 如何使用 Stealthwatch 來偵測和分析惡意流量，以提升事件回應和鑑識成效。

深入瞭解。要求產品演示。
stealthwatch@cisco.com

「80% 的組織相信他們的事件偵測 / 回應程序都因為缺少資安技術整合而受到阻礙。」

– Enterprise Strategy Group

C11-737531-00　2016 年 7 月