Trellix Insights

可動態強化安全性狀態的首個端點安全性功能，讓您能夠領先對手

網路威脅的進化與步調是組織的持續威脅與壓力點。企業被迫在缺少安全專業經驗的情況下提高安全預算，但還是無法跟上現代對手的步伐，因為他們會持續更新工具庫、策略與技巧。目前的選擇就是在人力與手動介入的情況下獲取支離破碎的情報。這些可能會解決眼前的威脅，但日益增多的網路攻擊以及它們之間的細微差異正迫使安全團隊陷入似乎永無盡頭的回應態勢之中。威脅情報平台 (TIP) 可以提供大型的威脅資料池，但這樣會要求手動整合與分析人員介入，由此導致行動性與修補措施受限。漏洞管理可以針對現有漏洞及其嚴重性提供建議，但對於安全性狀態是否能夠抵禦目前的真實威脅，只能提供有限的威脅深入分析。

解決方案就是採用即時情報來助力主動式行動的 Trellix Insights。人工智慧已經深入鑽研分析全面的情報，而人力則可以對最有可能針對貴組織的威脅與威脅活動排定優先順序。 Trellix Insights 精準預測威脅將如何影響您的整體安全，同時還精準描述您要採取哪些措施來最佳化安全性戰略。

主要優點

- **從十億個感應器中收集風險情報：**在周邊範圍之外主動識別來自可靠來源的的威脅專案。依據垂直行業、地理以及企業的端點安全性狀態，排定威脅專案的優先順序。
- **在攻擊發生之前，從單一主控台識別威脅攻擊活動並排定風險等級：**獲取有關威脅以及您的端點安全性狀態如何抵禦威脅的可採取行動的情報，包括修補建議。
- **縮短偵測到解決威脅的平均時間：**簡化工作流程以加速額外的防護。採用所需的可採取行動的變更來評估您目前的端點安全性狀態，同時加快回應速度(從數月縮短至數小時)。

轉變安全性，從此更為積極主動

Trellix Insights 提供 Trellix 管理平台體驗內建的新功能可與風險和威脅作業保持獨特匹配並將其簡化，在使用更少資源的同時，優先改善防禦對策並加快回應速度。從十億個感應器中收集的風險情報為貴組織提供了深入分析，讓其得以排定防禦措施的優先順序。從單一主控台即可實現偵測、修補、優先加快回應速度以及風險的顯著降低。

回應式網路防禦策略作為網路防禦的重要一環，有其自身的作用，但只是限於趕上他人的水平並消滅已發現的威脅。對手們正在使用新一代的工具來設計用來攻擊傳統防禦的攻擊活動，測試回應式安全產品以瞭解何種技術會打破他們的防護。組織在遭受攻擊前後需要應對整個攻擊循環階段。

攻擊循環階段

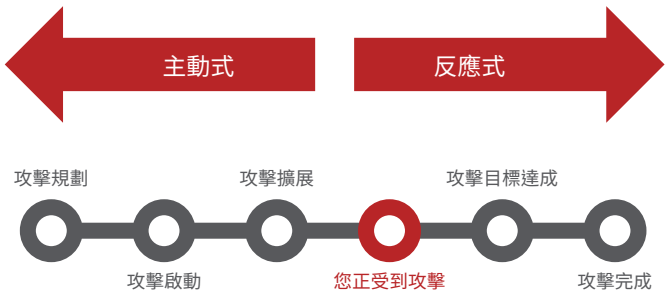

圖 1. 典型的攻擊循環階段。

在每日結束之時，情報以及可採取行動的深入分析能夠針對最有可能的威脅為您提供最佳的可能的網路安全性戰略，並提升您防禦之時的自信。以下是 Trellix Insights 實現此目標的方式：

- **協助減少盲點並提升情境感知：**您完全瞭解如何在威脅展開攻擊之前放置防禦措施。對於預測會攻擊您企業的本機與全球威脅，Trellix Insights 會主動追蹤並排定其優先順序。
- **機器學習分析：**此功能允許您確定特定安全性狀態將如何執行，然後提供優先的規範性防護動作，您可以據此快速輕鬆地實作來阻止這些攻擊。
- **自動識別您未曾瞭解的大多數全球威脅：**此解決方案會利用來自可信來源的安全情報資料池的巨量資料庫，此來源會以統計資料的形式分享重要的遙測資料。

Trellix Insights 提供端點風險相關問題的解答

- 您是否處於風險之中？您的曝光等級為何？
- 您如何排定可能攻擊貴組織的攻擊的優先順序？如何瞭解這些攻擊？您的研究流程為何？
- 您如何瞭解尚未攻擊貴組織的威脅 (但未來可能會)？
- 若您擁有 TIP，則您如何排定 TIP 資料庫內所有攻擊的優先順序？
- 您如何瞭解已攻擊您同事的威脅？
- 這在您行業與地區的流行度如何？
- 您目前的安全性狀態如何應對此威脅？
- 您在完整威脅領域內的信心是什麼？原因為何？

Trellix Insights 儀表板

圖 2. Trellix Insights 儀表板的示例。

風險評估

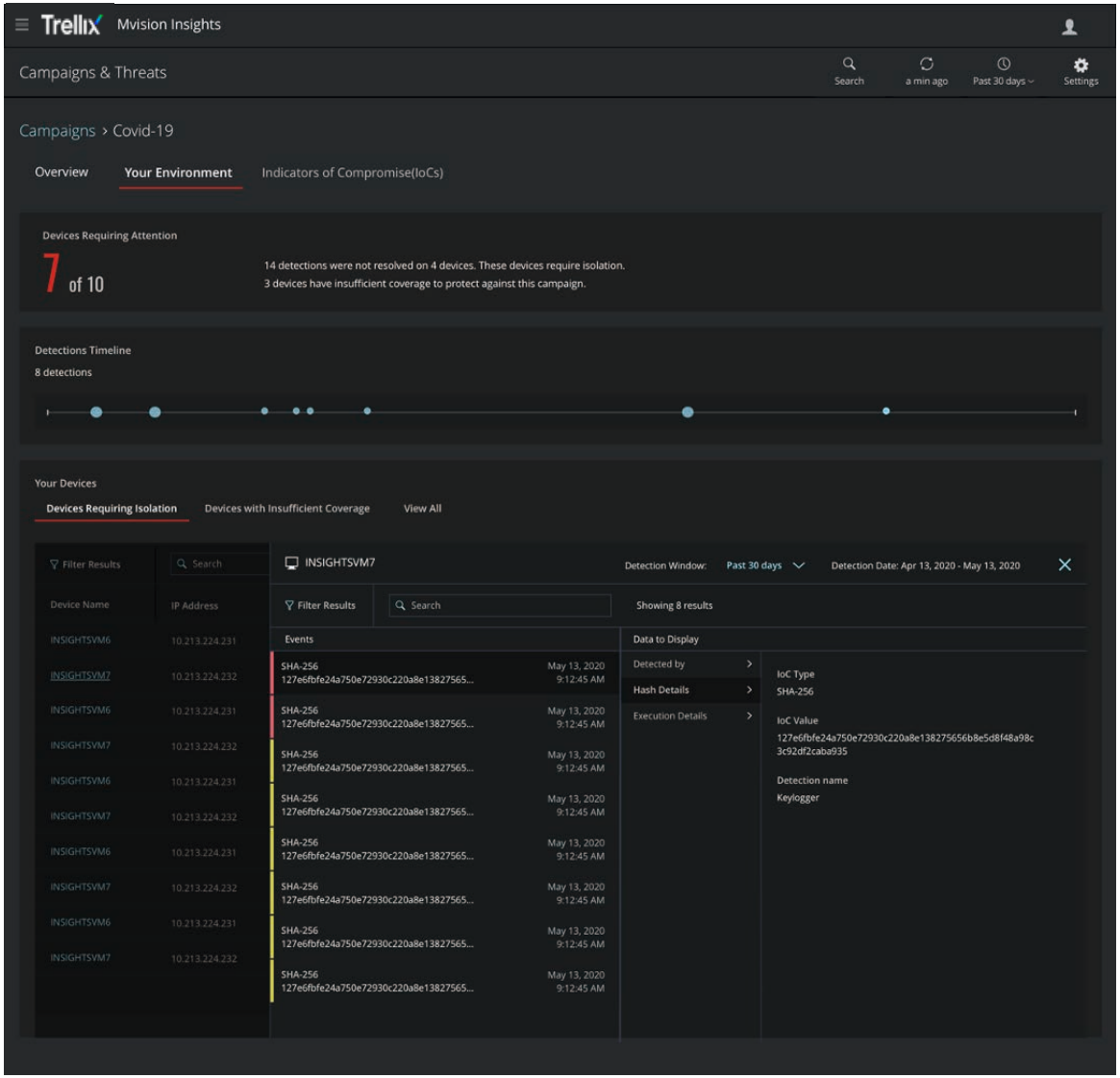

圖 3. 掌握您的環境中需要注意的內容以積極應對威脅。

顯著加快偵測與回應速度

Trellix Insights 提供規範的指引與自動化的行動措施，協助貴企業採取重要的後續主動步驟來變更與修補您的獨特環境。自動化操作可提升應對外部威脅的有效性，自動分析和比較外部威脅，同時在攻擊展開之前主動防禦。

- **將偵測並解決威脅的平均時間從數月縮短至數分鐘：**人機合作（深度學習與機器學習）和進階分析功能可擴充以從大量資料中篩選，並呈現可採取動作的情報。可擴充的偵測功能可優先加快回應速度並顯著降低風險。
- **提高威脅指標的訊噪比：**進階分析功能可擴大偵測範圍並改善警示狀況。Trellix Insights威脅分析可輕鬆轉向 Trellix EDR 來研究傳統的情境 (例如入侵指標(IoC)) 並縮短調查週期。
- **系統將以您可理解的方式呈現威脅，同時提供優先順序與行動性：**依據經分析且排定優先順序的情報和深入分析的指引式回應，甚至可提升新手分析人員的能力。透過變更

  配置、隔離受影響的裝置、更新原則或專注於端點偵測與回應 (EDR)，從整合式主控台快速輕鬆地回應。

助力 SOC 資源

安全團隊有大量情報需要處理，必須篩選以保護環境。有限的資源與時間壓制了威脅和防禦分析。藉由人機合作，分析功能可擴充（無論分析人員的技能等級如何）以耙梳大量資料，並將其作為可採取動作的情報呈現。MVISION Insights 可讓貴企業彌補其技能缺陷並助力 SOC 業務部門。安全團隊的消息更為靈通，如此就能做出更明智的決策。

- 使用提供的資料情報獲取的人工深入分析讓安全團隊可以自訂並最大化企業的防禦，從而獲得最優防護，無需擴大員工規模或仰賴更高層級的專業經驗。Trellix Insights 可提供有關 Trellix EDR 的更多目標性深入分析，以縮短調查週期的長度，同時提供執行調查所需的專業經驗與資源。分析人員可以更快的速度和效率驗證事件的風險以及根本原因。

- 透過讓安全分析人員脫離繁瑣的日常工作並協助提升初級團隊成員的工作成效，協助首席安全官 (CSO)從員工與產品中獲取最大效益。組織可以實現安全管理相關工作的時間縮短 (以小時為單位) 。工作流程得以簡化，可加速額外的防護。
- 針對排定優先順序的威脅，從單一主控台優先自動化偵測、回應與防禦，從而減輕分析人員在不同工作之間切換的需求。Trellix Insights會在單一位置使用可採取行動的指引來累積與分析相關資料元素，並在需要時將其放在安全分析人員的掌控之下。

更為深入的分析

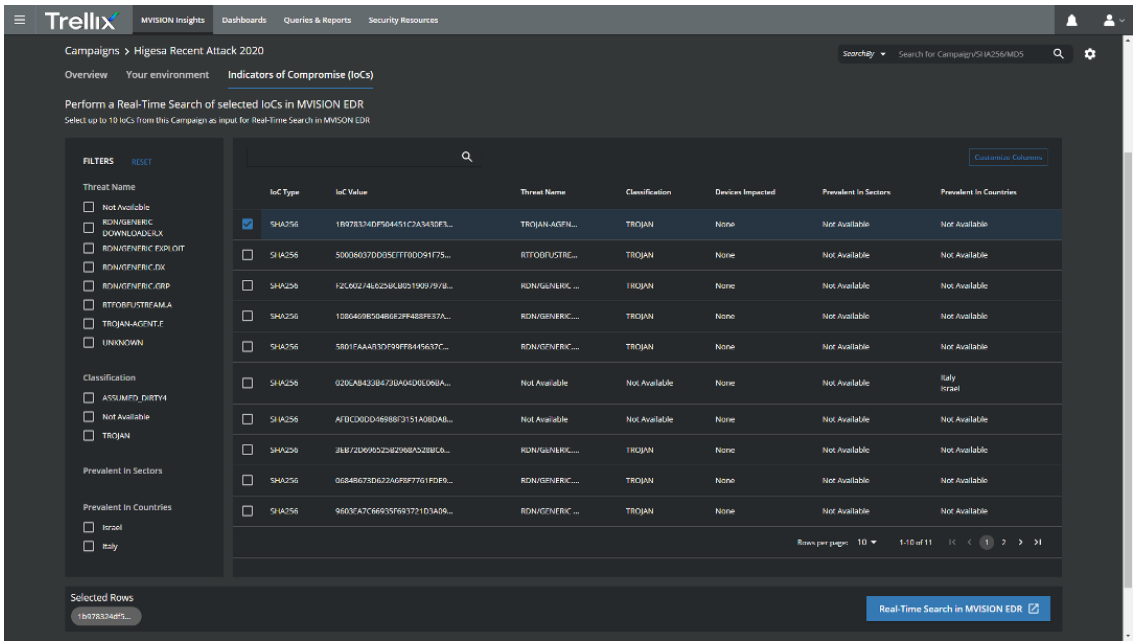

圖 4. 深入瞭解威脅事件並確定保護組織的能力。

Trellix Insights 需求

Trellix Insights 由 Trellix ePolicy Orchestrator (Trellix ePO) 軟體 5.10 (內部部署與 IaaS) 以及 Trellix ePO (SaaS) 管理。已進行最佳化，可與最新的端點防護技術搭配使用：Trellix Endpoint Security 與 Trellix Agent。 Trellix Insights 需要您選擇加入 Trellix Endpoint Security 遙測技術才能有效運作。

使用案例示例

問題	解決方案	結果
我是否就是攻擊目標？	▪ 已知攻擊活動威脅評估	回答問題：我是否處於風險當中？
這是否是新的攻擊活動變體？	▪ 選定的追溯攻擊分析 ▪ 可比較的防護功效報告 ▪ 使用者 IoC 追溯攻擊分析	
我目前的防護設定是否可保護我的安全？	▪ 本機防護狀態檢查	評估我目前的安全性狀態
我需要特別變更什麼來受到防護？	▪ 本機防護狀態檢查	有關應採取措施的規範指引
可以隔離其他安全功能嗎？	▪ 將隔離或包含發布到其他安全功能	向其他安全功能發送包含操作以進一步降低風險 (透過 DXL)

深入了解

如需詳細資訊，請造訪 www.trellix.com。

Trellix