SOPHOS

Managed Threat Response (MTR)

專家領導的威脅回應

Sophos Managed Threat Response (託管式威脅回應，MTR) 提供全天候的威脅獵捕、偵測，以及回應功能，全部都由專家團隊提供，是一項完全託管式服務。

產品重點

- 進階型威脅獵捕、偵測和回應功能，全都以完全託管的服務方式提供
- 與全天候回應團隊合作採取行動，可遠端遏阻及消除威脅
- 您可決定及控制 MTR 團隊要採取什麼行動及如何管理事件
- 結合評價最高的機器學習技術和訓練有素的專家團隊
- 有兩種等級服務 (Standard 和 Advanced)，為所有成熟度的組織提供全方位功能

威脅通知並非解決之道，只是起點

很少有組織內部擁有能全天候管理安全計畫，同時主動防禦新興威脅的適當工具、人員和程序。Sophos MTR 團隊不僅通知您攻擊或可疑行為，還可為您採取目標性行動，以消除最複雜的威脅。

使用 Sophos MTR，您組織將配備全天候的威脅處理及回應專家團隊，他們會：

- 主動獵捕及驗證可能的威脅與事件
- 使用所有可用資訊，判斷威脅範圍與嚴重程度
- 對有效的威脅使用適當的回應措施
- 啟用動作以從遠端中斷、限制及遏阻威脅
- 提供行動建議以解決重複事件的根本原因

機器加速的人工回應

Sophos MTR 建立在具有 EDR 技術的 Intercept X Advanced 基礎上，融合了機器學習技術和專家分析功能，可改善威脅追捕及偵測、提供更深入的警示調查，以及目標性行動，以快速又精確地消除威脅。Sophos 持續最高評價的端點保護和智慧型 EDR 的這種融合，加上世界級安全專家團隊，成就了我們所謂的「機器加速的人工回應」。

完整的透明度和控制

使用 Sophos MTR，您可決定及控制潛在事件的提報方式和時間、希望我們採取何種回應措施 (如果有的話)，以及通訊對象應包含誰。Sophos MTR 具有三種回應模式，可讓您選擇在事件發生時與我們 MTR 團隊合作的最佳方式：

通知：我們通知您有關偵測的資訊，並提供詳細資訊以協助您設定優先順序及回應。

共同作業：我們與您的內部團隊或外部聯絡窗口合作，以回應偵測結果。

授權：我們負責限制及遏阻行動，並會將所採取的動作通知您。

Sophos MTR 服務等級

Sophos MTR 具有兩種等級的服務 (Standard 和 Advanced)，可為所有規模與成熟度的組織提供全方位功能。不論所選的服務等級為何，組織都能善用這三種回應模式 (通知、共同合作或授權) 以滿足其獨特需求。

Sophos MTR：Standard

全天候負責人推動的威脅追捕

自動阻擋或終止經確認的惡意人為物件或活動 (強訊號)，讓威脅處理專家有時間進行負責人推動的威脅搜尋。此類型的威脅追捕牽涉到因果和相鄰事件 (弱訊號) 的彙總和調查，可發現以往無法偵測的新的攻擊指標 (IoA) 和遭駭指標 (IoC)。

安全狀態檢查

讓您的 Sophos Central 產品 (從 Intercept X Advanced with EDR 開始) 運作效能始終保持最佳，並主動檢查作業條件及建議設定改善的成果。

活動報告

案例活動摘要可做到優先順序設定及溝通，讓您的團隊知道每個報告期間內偵測到哪些威脅及採取哪些回應動作。

對抗性偵測

大多數的成功攻擊都需要執行對監控工具而言看似合法的程序。我們團隊使用專利的調查技術來確定合法行為與攻擊者所使用的策略、技術和程序 (TTP) 之間的差異。

Sophos MTR：Advanced 包含所有 Standard 功能，再加上下列各項：

全天候無負責人推動的威脅追捕

藉由運用資料科學、威脅情報和資深威脅處理專家的直覺，我們會結合您的公司資料、高價值資產和高風險使用者，預測攻擊者的行為並確認新的攻擊指標 (IoA)。

增強遙測功能

來自其他 Sophos Central 產品的遙測功能可補足威脅調查，使調查範圍超出端點以外，可全面了解攻擊活動。

主動狀況改善

透過引導性指引來主動改善您的安全狀況並加強防禦，以解決會降低整體安全功能的設定與架構弱點。

專屬的威脅回應負責人

確認事件之後，會提供專屬的威脅回應負責人，與您的內部預置資源 (內部團隊或外部合作夥伴) 直接合作，直到遏阻主動威脅為止。

直接通話支援

您的團隊可與我們的安全營運中心 (SOC) 直接通話。我們的 MTR 營運團隊提供全天候服務，並擁有全球 26 個地點的支援團隊的支援。

資產探索

從涵蓋了作業系統版本，應用程式和漏洞的資產資訊，到識別託管和非託管資產，我們會提供影響評估、威脅獵捕的寶貴洞見，並作為主動形勢改善建議的一部分。

台灣業務窗口
電話: +886 2 7709 1980
電子郵件：Sales.Taiwan@Sophos.com

2019-09-17 DSZHTW (GH)

SOPHOS