Sophos XDR

Intercept X Advanced with XDR、Intercept X Advanced for Server with XDR

Intercept X 將功能強大的擴充式偵測和保護 (XDR) 與無與倫比的端點保護整合在一起。威脅捕獵可偵測主動式攻擊者，或應用在 IT 營運上以保持 IT 健康。發現問題時，可從遠端精準回應。透過豐富的資料來源 (包括端點、伺服器、防火牆和電子郵件) 將可見度擴展到端點之外。

回答 IT 營運和威脅捕獵問題

快速獲得關鍵業務問題的答案。IT 系統管理員和網路安全專業人員在執行日常 IT 操作和威脅捕獵時都能看到它帶來的價值。

從最佳保護開始

Intercept X 在攻擊開始之前就能加以阻擋。這意味著您可以獲得更好的保護，花費更少時間在調查已被自動阻擋的事件上。您還可以取得詳細的威脅情報，藉由獲得必要的資訊以採取迅速而明智的行動。

深入研究詳細資訊並快速回應

當您需要進一步調查時，可從 Sophos Data Lake 深入研究以取得豐富的即時資訊，直接從裝置取得多達 90 天的歷史資料。確認問題後，可以遠端存取裝置並採取任何必要的措施，例如解除安裝應用程式並重新啟動。

跨產品可見度

Sophos XDR 不僅只於端點和伺服器，讓 Sophos Firewall、Sophos Email 和其他資料來源* 都可以將關鍵資料發送到 Sophos Data Lake，使您對組織的環境擁有難以置信的寬廣視野。

即使裝置離線也能獲得資訊

Sophos Data Lake 是 XDR 功能的關鍵元件，是一個雲端資料儲存庫。它使您能夠儲存和使用來自端點、伺服器、防火牆和電子郵件的關鍵資訊，以及即使裝置離線也可使用裝置資訊。

幾秒鐘即可上手

使用預先編寫的 SQL 查詢庫，詢問各種各樣的 IT 和安全性問題。若您願意，也可以加以自訂或自行編寫。您也可以參考會定期共用查詢的 Sophos 社群。

產品重點

- 回答關鍵的業務 IT 營運和威脅捕獵問題
- 專為 IT 管理員和安全分析人員設計
- 從遠端對目標裝置採取補救措施
- 全面了解組織的 IT 環境，並在需要時深入研究詳細資訊
- 利用端點、伺服器、防火牆、電子郵件和其他資料來源*
- 立即可用、完全可自訂的 SQL 查詢
- 適用於 Windows、macOS* 和 Linux

*Cloud Optix 和 Sophos Mobile即將推出

*XDR 功能即將出現在 macOS 中

SOPHOS

使用案例

IT 營運

- 電腦為什麼執行緩慢？
- 哪些裝置有已知弱點、未知服務或未經授權的瀏覽器擴充功能？
- 執行的程式有沒有應該移除的？
- 識別未受管理的訪客和物聯網裝置
- 為什麼辦公室網路連線速度緩慢？哪個應用程式造成這個問題？
- 可回溯 30 天以查看遺失或損毀裝置上的異常活動

威脅捕獵

- 哪些處理程序嘗試在非標準連接埠上建立網路連線？
- 顯示最近修改了檔案或登錄機碼的處理程序
- 列出偵測到且對應到 MITRE ATT&CK 架構的 IoC
- 無需裝置回復上線即可擴大調查達 30 天的資料
- 使用防火牆中的 ATP 和 IPS 偵測來調查可疑主機
- 比較電子郵件標題資訊、SHA 和其他入侵指標，以找出惡意網域的流量

包含哪些功能？

	擴充式偵測和回應 (Extended Detection and Response, XDR)
跨產品資料來源	✓
跨產品查詢	✓
端點和伺服器查詢	✓
Sophos Data Lake	✓
資料湖保留期間	30 天
磁碟上資料保留期間	✓
SQL 查詢庫	✓
Intercept X 保護功能	✓

如需授權的更多詳細資訊，請參見 Intercept X 和 Intercept X for Server 授權指南。

立即免費試用

註冊取得 30 天免費試用版本
www.sophos.com/intercept-x

台灣業務窗口
電子郵件：Saales.Taiwan@Sophos.com

21-07-08 DS-ZHTW (PS)