進階威脅防護購買者檢查表

下面的檢查表將幫助您從環境覆蓋範圍、資安技術組合及整合能力等面向，評估您目前和預計的安全態勢。其最後結果將可提供一套標緻，以作為您組織選擇最恰當的解決方案之依據。

I. 評估環境涵蓋範圍

- ☐ 決定您要覆蓋的實體位置，如網路入口/出口/內部點、中央電子郵件和檔案系統、行動端點及雲端工作負載。
- ☐ 決定您要在各個點檢查哪些通訊協定（如 http、SMTP、SMB 及其他通訊協定，包括加密版本）。
- ☐ 評估所需的容量（如 1 G、10 G、40 G 埠及/或 1 Gbps、4 Gbps、10Gbps 或以上，加上每個時段的物件數）。
- ☐ 評估或審核近期進行的應用沙箱及相關技術的獨立評比測試，以瞭解其表現。請參閱如 NSS 實驗室、病毒公報（Virus Bulletin）、防毒軟體評比（AV Comparatives）及國際電腦安全協會實驗室（ICSA Labs）等測試機構的評比結果。

這些步驟將幫助您確定所需的部署規模，並快速瞭解導致您走向無以為繼浪費之路的無效（功能有限）產品，以及隱藏效率不足問題的行銷噱頭。

II. 決定您的資安技術組合

- ☐ 瞭解各種位置和通訊協定防護所使用的分析技術，確保您具備更多可有效防禦威脅的進階技術（如簽章、啟發式邏輯、信譽評、模擬及解密）。
- ☐ 瞭解哪些分析技術被用於提供按位置和通訊協定的進階威脅偵測，包括沙箱、行為分析及大數據分析。
- ☐ 識別您已準備好用來回應事件的威脅緩解程序和工具。這可能包括您的反應小組、外部服務、鑑識工具和整合工具，以及產品間的自動反應。
- ☐ 識別用於評估威脅預防、偵測與緩解成效的方法（如定期入侵測試、追蹤生產成效、購買 PoC 的時間及獨立測試報告）。

這些步驟將幫助您集中投資並獲得最大的預防、偵測與緩解成效。請千萬不要疏忽預防的工作，如此才能防止日後進行許多費時又費力的偵測及反應工作。不過，我們也從過去幾年的經驗中發現，若只依賴預防工作，而忽視偵測工作，這也是不對的。同樣地，缺少反應能力的預防及偵測投資也無法有效降低您的資安風險。

III.系統級運作能力

- ☐ 識別哪些預防元件可以與偵測元素相互整合（例如，跨分支、總部、核心、雲端的防火牆整合；電子郵件和網頁安全、端點防護、網路應用程式防火牆、SIEM、記錄檔管理及其它元素）。
- ☐ 定義進階威脅防護元件如何提供反應用的資訊（例如，儀表板與報告、透過 API 匯出資料、傳送資料的整合元件及自動簽章）。
- ☐ 瞭解內部元件可採取哪些輔助或自動反應措施（例如，隔離裝置、封鎖來源或移除檔案）。
- ☐ 識別需要多少個中央情報樞紐、本機威脅交換及/或全域研究實驗室。

這將決定您所有預防、偵測與緩解元素（無論分開運作時表現再好）能夠整合在一起有效運作的能力。

評估進階威脅防護的強度

評估您組織在防禦當前複雜威脅方面的整體強度時，需要瞭解已到位預防技術、會跳過的偵測及緩解進階威脅的措施，以及所有這些元件間的整合點的數目。

預防功能很多，但進階威脅偵測或緩解功能很少的解決方案將使組織異常容易遭受攻擊。即使個別功能加起來很多，但整體上仍有漏洞。洞悉您當前的處境，並依據充分而完整的資訊，選擇能有效整合預防、偵測與緩解威脅的解決方案。

預防元件

- ☐ 分支防火牆
- ☐ 總部防火牆
- ☐ 核心防火牆
- ☐ 雲端防火牆
- ☐ 安全電子郵件閘道
- ☐ 安全網頁閘道
- ☐ 網路應用程式防火牆
- ☐ 端點防護
- ☐ 其他

偵測元件

- ☐ 網路行為
- ☐ 網路鑑識
- ☐ 端點行為
- ☐ 沙箱
- ☐ 大數據
- ☐ 其他

反應元件

- ☐ 反應服務
- ☐ 端點鑑識
- ☐ 自動化

整合點

- ☐ 防火牆與進階威脅偵測
- ☐ 安全電子郵件閘道與進階威脅偵測
- ☐ 安全網頁閘道與進階威脅偵測
- ☐ 網路應用程式防火牆與進階威脅偵測
- ☐ 端點防護與進階威脅偵測