Cortex XDR

消除偵測與回應的安全隔閡

安全團隊經常面對令人眼花撩亂的各種威脅，從勒索軟體和網路間諜到無檔案攻擊和破壞性的數據洩露等等。不過，最讓許多安全分析師頭疼的並非是層出不窮地登上媒體頭條新聞的各種風險，而是每天都必須處理許多重複性工作，同時還要進行事件分類並嘗試解決永無止境的待處理警示。

本白皮書介紹安全分析師面對的最為棘手的挑戰，包括蜂擁而至的警示和複雜的調查流程，即使是經驗最豐富的安全作業中心 (SOC) 也難以應付。在本白皮書所提議的框架中，可透過 Cortex XDR 進行偵測與回應以解決每個安全作業階段的問題。隨著惡意軟體、目標攻擊和內部人員濫用等威脅不斷擴大，您可以使用 Cortex XDR 等工具作為消除威脅及簡化作業的祕密武器。

分析師陷入困境

安全團隊現在正面臨兩大艱鉅的挑戰：持續出現的猛烈攻擊和永無止境的大量警示。安全團隊知道攻擊者會不計後果地發動無限次攻擊，直到達到目的為止。為了降低遭到入侵的機率，安全團隊通常會部署多個安全性層級，但這些工具會產生平均每週 11,000 則的大量警示。[1]

為了能夠即時處理所有的警示，分析師經常需要處於緊急救援模式，而每一天都必須儘可能地將所有的警示進行分類。由於這些警示通常缺乏進行調查所需的重要脈絡，分析師只能被迫浪費寶貴的時間來找出其他細節。由於必須忙於應付不正確且不完整的警示，因此有 53% 的安全團隊只能檢視所收到警示的一半，[2] 因而增加數據洩露的風險。

在所有錯誤的地方偵測威脅

層出不窮的攻擊浪潮已讓各種規模的企業都開始採取偵測與回應政策。為了應付這一波的新需求，IT 安全產業引進了許多孤立的工具，例如端點偵測與回應 (EDR)、網路偵測與回應 (NDR)，以及使用者行為分析 (UBA)。然而，這些孤立工具只能提供狹小的活動視野，並且需要具有數年經驗的專家才能操作。而佈建這些工具的安全團隊，因在每個位置部署及維護新的網路感應器和端點代理程式而需負擔大量的成本。

在另一方面，未部署偵測與回應的企業可能會忽略各種隱匿性攻擊，例如高度迴避的惡意軟體、惡意內部人員或針對性攻擊等等。這是因為進階攻擊通常不會使用傳統入侵指標 (IOC)，例如攻擊特徵碼或惡意網域。偵測這些威脅的唯一方法是透過機器學習和分析，隨著時間的推移並跨越所有數據來源檢視整個活動，而不僅僅是警示。

手動調查會增加攻擊者停留時間

偵測攻擊僅獲得一半的成功。分析師還必須調查警示並評估「對象、內容、時間、原因和方式」等詳細資訊來決定要採取的動作。遺憾的是現在許多的安全工具都只能呈現高階警示，但其使用者、端點、網路、應用程式和威脅情報資訊都非常有限。這些高階警示通常無法提供調查和回應所需的所有脈絡。因此，分析師必須在不同主控台之間來回切換並手動整合數據，才能對攻擊有較清楚的瞭解。例如，為了要調查網路警示，分析師可能需要執行仔細的分析和進行關聯性調查，以找出與每個事件有關的端點、網路活動和使用者。現今這些工具不但複雜且各自孤立，因此只有具備專業知識的專家才能利用錯綜複雜的資訊進行調查。

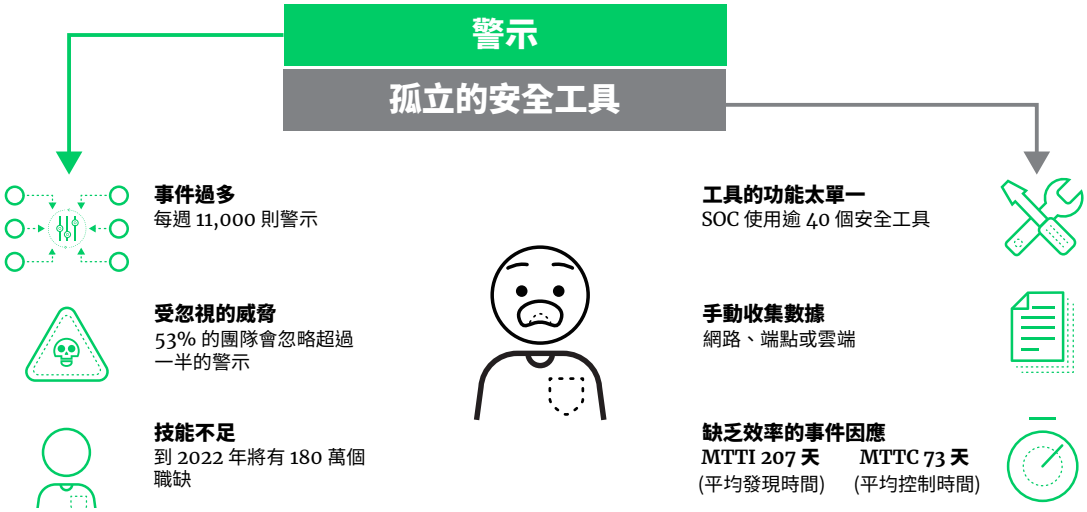

圖 1：安全分析師的許多負擔

1. 「The State of Security Operations Report, 2021」，Forrester，https://www.paloaltonetworks.com/resources/research/state-of-secops-forrester-consulting-study。
2. 同上。

由於這些工具幾乎無法一起運作，讓分析師無法輕易地協調所有執行點的回應。他們並非迅速阻止攻擊，而是必須提交票證或要求其他團隊成員更新安全性政策，這可能需要數天或數週的時間。企業發現入侵和有效控制所需的平均時間已分別增加至 207 天和 73 天，這樣的情況一點也不令人意外。[3] 安全團隊正面臨網路安全專業人員短缺問題，他們必須消除安全隔閡並簡化事件回應，否則將難以阻止網路攻擊得逞。

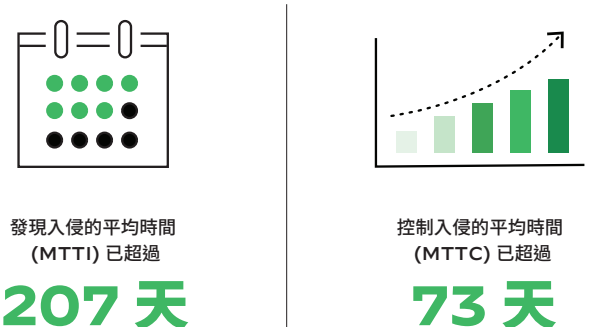

圖 2：MTTI 和 MTTC 增加

必備要件

我們需要新的方法來解決現今的安全作業挑戰，它必須能夠簡化每個階段的安全作業，包括偵測與威脅捕捉、分類、調查和回應。這個新方法需要將三種功能整合在一起以降低風險並簡化作業：

- **有效的威脅防禦措施：**高效的防禦措施讓您不需要任何手動驗證就能阻止所有的攻擊，也就是說您可以即時或者以近乎即時的速度自動阻止 99% 的攻擊。您需要在所有的數位資產中實現協調一致的防禦。
- **AI 和機器學習：**隨著收集的數據不斷增加，您的分析師不應該被迫手動分析或建立數據的關聯性來識別威脅。您需要機器學習和分析以了解企業的唯一特性，並形成預期行為的基準來偵測精密攻擊。
- **自動化：**若要快速確認攻擊，分析師需要可化為行動的警示和豐富的調查詳細資料。他們也應該能夠輕易地了解攻擊的根本原因，而不是需要累積數年的經驗後才能做到。

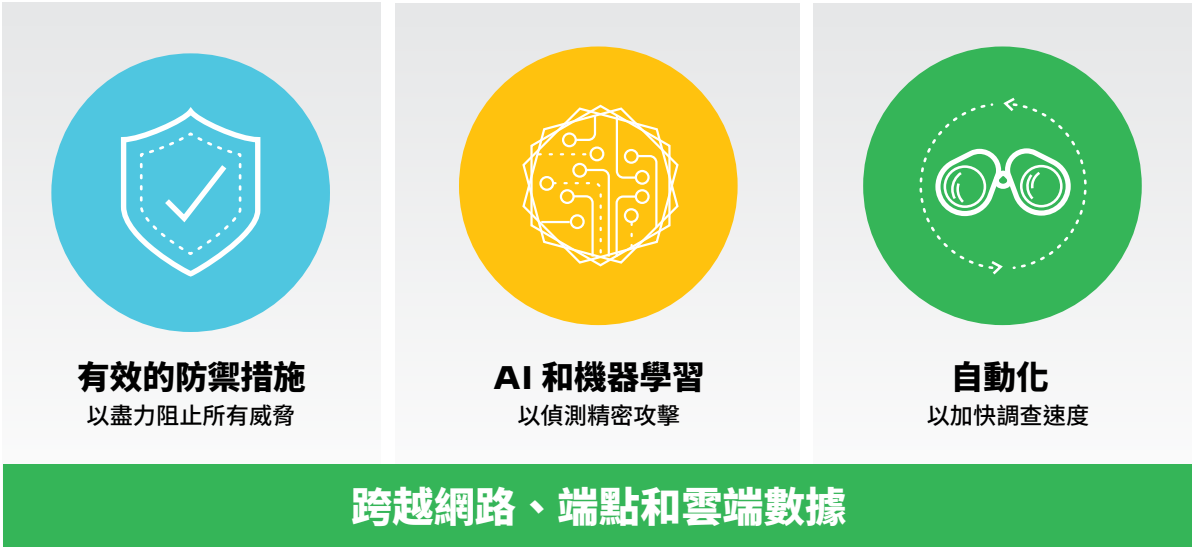

圖 3：重要整合功能

在包括網路、端點和雲端等所有的重要資產上協調這三種整合功能後，您將能夠防禦日益增加的精密威脅。

Cortex XDR 擴展的偵測與回應

Cortex XDR® 是業界第一個整合網路、端點、雲端和第三方數據來阻止精密攻擊的擴展型偵測與回應平台。Cortex XDR 的設計主要是為了協助像貴公司這樣的企業來保護數位資產和使用者，同時簡化所有作業。運用行為

3. 「2020 Cost of a Data Breach Study」，Ponemon Institute，2020 年 7 月，https://www.ibm.com/downloads/cas/861MNWN2。

分析，它可識別出針對網路的未知與高度迴避的威脅。機器學習與 AI 模型會發現包括受管理與未受管理裝置在內所有來源的威脅。

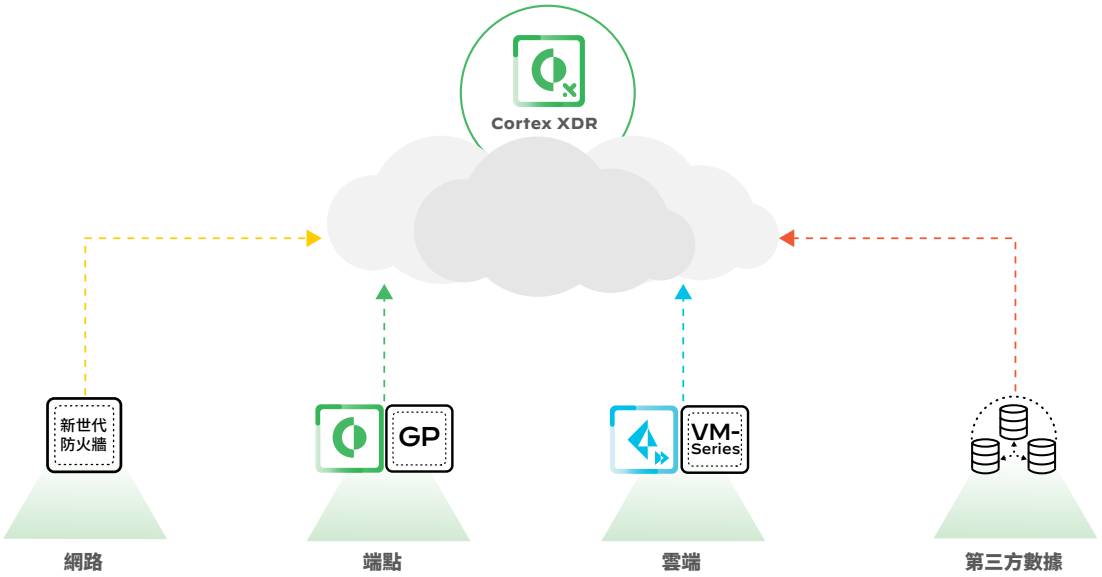

圖 4：使用 Cortex XDR 分析多個來源的數據

Cortex XDR 可提供每則警示的完整狀況以加快調查進度。它可將不同類型的數據整合在一起並揭露警示的根本原因和時間表，讓任何經驗資歷的分析師都能夠執行分類。透過與執行點緊密整合，可讓您回應企業中任何地點發生的威脅或輕鬆地將主機還原到無威脅的狀態。

透過 Cortex XDR，您可以使用現有網路、端點和雲端安全作為感應器和執行點，因此不再需要部署新的軟體或硬體。您將只需要一個數據來源即可使用 Cortex XDR，但您可能會需要多個數據來源以瞭解數據整合和分析的優勢。在將所有數據儲存在可擴充且安全的雲端數據儲存庫後，您就不再需要佈建繁瑣的內部部署日誌基礎結構。

Cortex XDR 可在每個安全作業階段提供保護

攻擊者會不斷推陳出新。為了能預先防範攻擊，安全團隊必須實施可重複的程序以透過最佳防禦主動地阻止攻擊，並發現和阻止主動式威脅。Cortex XDR 可提供完成這四個疊代步驟的工具：

1. 自動防禦威脅。
2. 準確偵測。
3. 快速調查。
4. 以智慧方式回應。

此框架可提供您需要的所有功能，無論在現在和未來都能為您的企業提供保護。

實現封閉式的防禦、偵測與回應

防禦已知和未知的威脅，同時獲得完整的可視性

嚴密的安全性始於良好的防禦措施。因此，Cortex XDR 可提供頂級防禦來阻止入侵、惡意軟體、勒索軟體和無檔案攻擊。輕量化 Cortex XDR 代理程式是專為最小端點影響所設計，可在封鎖攻擊的同時收集可提供給 Cortex XDR 的事件數據。

Cortex XDR 代理程式可提供完整的防禦堆疊，並從最廣泛的入侵防護模組開始，可用來阻止導致惡意軟體感染的入侵。每個檔案都由具有適應性的 AI 驅動的本機分析引擎進行檢查，該引擎會一直不斷學習，以因應新的攻擊技術。行為威脅防護引擎會檢查多個相關程序的行為，藉以發現發生的攻擊。

我們的新世代防毒軟體 (NGAV) 結合多種防禦方法，在保護端點的能力方面脫穎而出。其能與惡意軟體防禦服務 Palo Alto Networks WildFire® 進行整合，在雲端中分析可疑的檔案，並在所有的 Palo Alto Networks 安全產品中協調防禦。您可以將統一的雲端交付代理程式快速部署到您的端點，以立即開始阻止進階攻擊，並收集數據以進行偵測與回應。

AV-Comparatives 在 2021 年端點防禦和回應測試中將 Cortex XDR 評為策略領導者

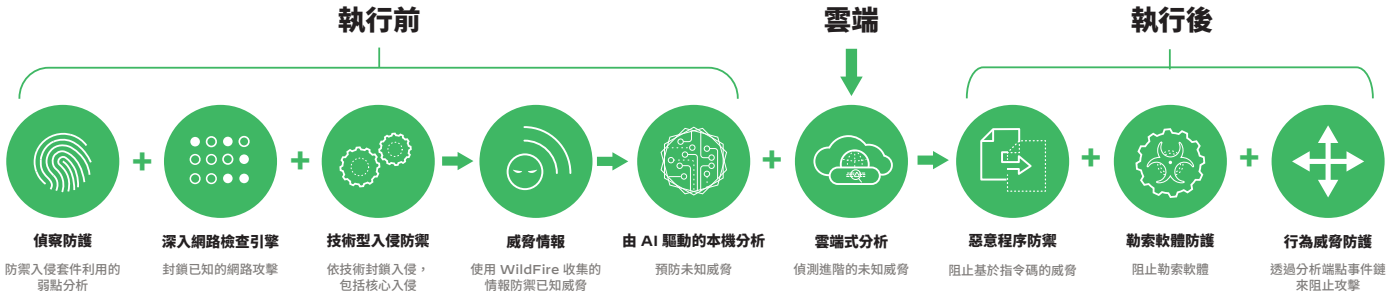

圖 5：自動防禦惡意軟體、入侵和無檔案攻擊

安全地管理 USB 裝置

雖然 USB 裝置可提供從備份儲存到周邊支援的一組廣泛功能，但也會導致風險。當使用者在不經意間將載入惡意軟體的快閃磁碟機、鍵盤或網路攝影機連接到其電腦，或將機密數據複製到備份磁碟機時，就會讓企業遭受攻擊。Cortex XDR 隨附的強大裝置控制模組可讓您保護 USB 存取，而不需要在您所有的主機上安裝另一個端點代理程式。您可以根據 Active Directory® 群組和組織單位指派政策、依裝置類型限制使用，以及依廠商、產品和序號指派唯讀或讀取/寫入政策例外。裝置控制模組可讓您輕鬆地管理 USB 存取，並且能夠放心，因為您已經減輕了 USB 型威脅。

使用主機防火牆和磁碟加密保護端點數據

藉由整合的主機防火牆和磁碟加密功能，您可以降低安全風險並滿足法規需求。Cortex XDR 主機防火牆可讓您控制 Windows® 或 macOS® 端點的傳入和傳出通訊。另外，您可以透過建立磁碟加密規則和政策對於端點套用 BitLocker® 或 FileVault® 加密或解密。對於透過 BitLocker 或 FileVault 加密的端點，Cortex XDR 可提供完整的可視性，並列出所有加密磁碟機。您可以透過主機防火牆和磁碟加密功能從 Cortex XDR 集中管理端點安全政策。

藉由主機見解獲得前所未有的可視性並快速回應

若要保護您的端點，首先您必須清楚掌握所有的端點設定和內容並了解您的風險。一旦發現任何威脅，您必須儘快予以阻止並確認威脅並未擴散到多個端點。

透過主機見解，也就是 Cortex XDR 的附加模組，您將可以取得所有這些功能。主機見解結合了弱點評估、應用程式和系統可視性以及強大的「搜尋和阻絕」功能，有助於識別和遏止威脅。主機見解提供全面的方法來查看端點可視性並遏止攻擊，協助您減少遭受威脅的風險，因此您可以避免未來出現數據洩露。

主機見解包括下列功能：

- **搜尋和阻絕**可讓您快速尋找並消除所有端點上的威脅。此一強大的功能會在受管理的 Windows 端點上建立所有檔案的索引，因此您可以探測整個企業以即時找出並移除惡意檔案。精確的設定可讓您排除特定主機上的檔案和目錄。
- **主機清單**可讓您透過重要 Windows 主機設定和檔案的完整可視性，找出安全漏洞並改善防禦態勢。您可以檢視關於使用者、群組、應用程式、服務、驅動程式、自動執行、共用、磁碟和系統設定的資訊。在單一位置中取得所有主機詳細資料後，您就可以快速識別安全問題，並透過額外的主機脈絡加快調查速度。

圖 6：主機見解模組

- **弱點評估**，您可以即時查看所有端點中的弱點暴露和目前修補程式層級，以排定緩解的優先順序。透過 NIST National Vulnerability Database 和 Microsoft Security Response Center 所提供的最新嚴重性資訊，Cortex XDR 揭露了 Linux 和 Windows 端點上的弱點。您也可以查看安裝在端點上的 Microsoft Windows 知識庫 (KB) 更新。

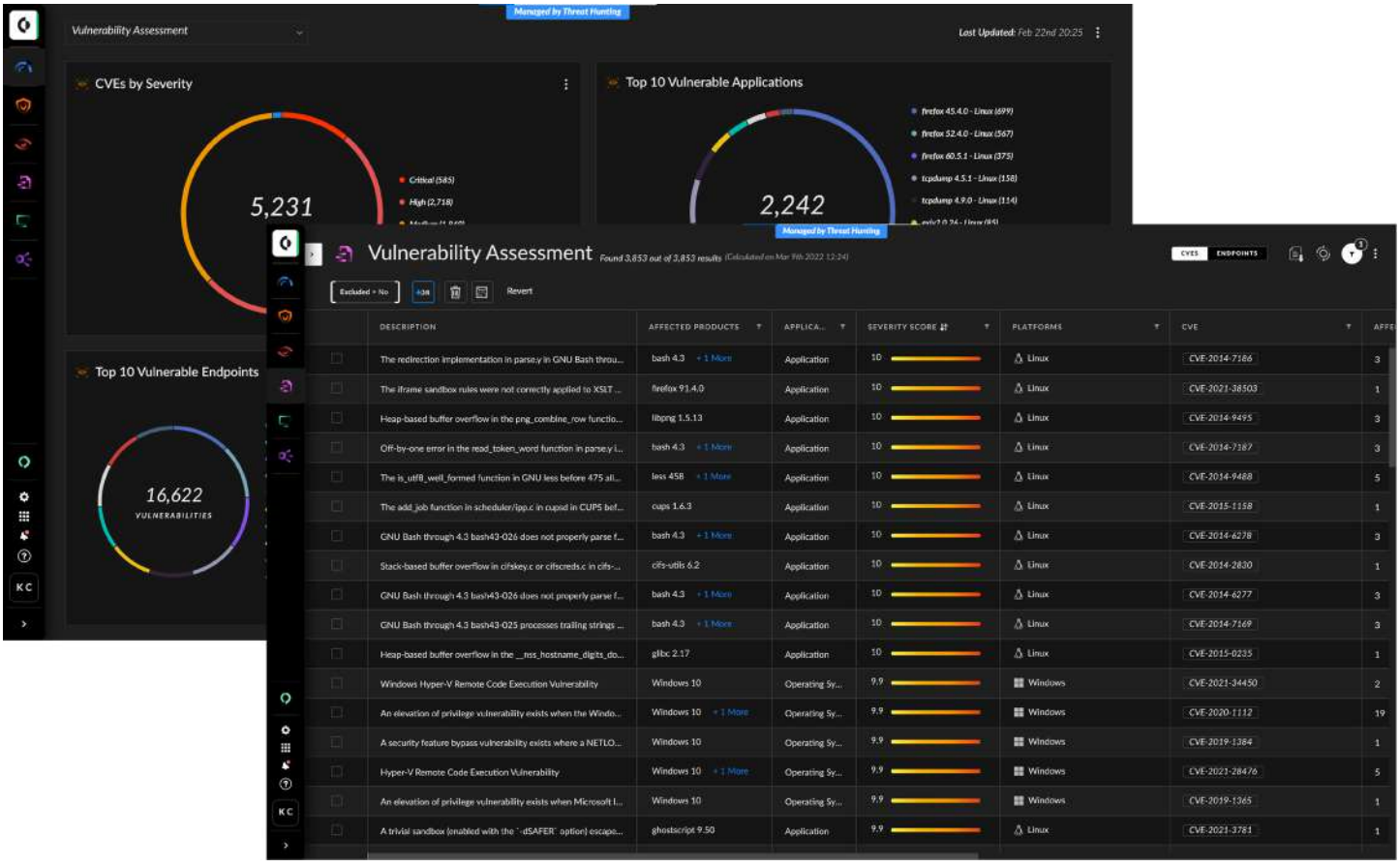

圖 7：弱點表與最新的 CVE 數據

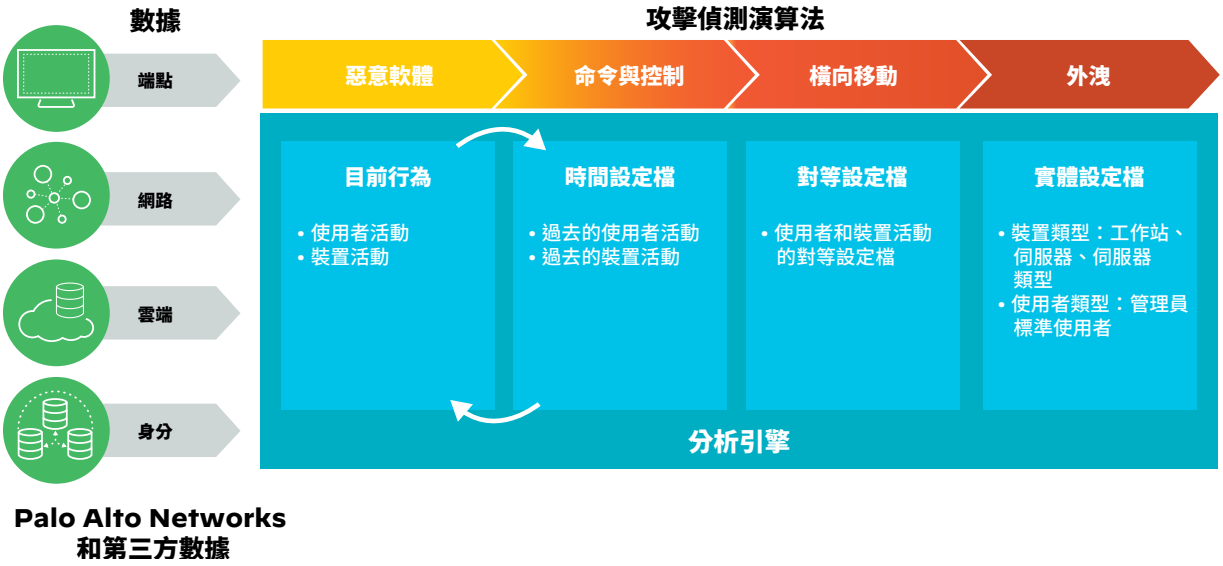

圖 8：Cortex XDR 的行為分析架構

以行為分析和 AI 自動偵測攻擊

Cortex XDR 會使用分析和機器學習找出隱匿性攻擊，使您的團隊能縮短停留時間並迅速遏止威脅。Cortex XDR 首先會分析從任何數據來源收集的豐富數據，為您提供完整的可視性並消除盲點。還將整合從網路、端點和雲端資產收集的所有數據，準確偵測攻擊並簡化調查。

Cortex XDR 可追蹤超過 1,000 種行為層面，包括幾乎無法從傳統威脅日誌中確定的屬性。然後它會利用下列方式分析使用者和裝置行為：

- **無需監管的機器學習：**Cortex XDR 會建構使用者與裝置行為的基準、進行對等群組分析，並將裝置分配到相關的行為群組。根據這些設定檔，Cortex XDR 會與過去行為和對等行為進行比較以偵測出異常狀況，藉此偵測惡意活動，例如惡意軟體行為、命令與控制、橫向移動以及數據外洩。
- **受監管的機器學習：**Cortex XDR 會對網路流量的多種特性進行監控，依裝置類型進行分類，例如 Windows 電腦、Apple iPhone® 或弱點掃描器。Cortex XDR 也會了解哪些使用者是 IT 管理員或一般使用者。透過受監督的機器學習，Cortex XDR 能夠根據使用者或裝置類型來辨識不同於預期行為的情形，以減少誤判發生。

透過身分分析精準掌握基於使用者的威脅

透過 Cortex XDR 的身分分析附加元件，您的團隊可偵測出傳統工具無法察覺的高風險和惡意使用者行為。身分分析會檢驗包括驗證、端點、網路、雲端和威脅日誌在內、隨著時間推移的一組廣泛數據，藉以分析使用者行為。在將目前的使用者行為與已建立的基準進行比較後，它將能夠以無與倫比的精確度找出如憑證竊取、暴力破解和「不可能的旅客」等攻擊。偵測演算法會持續不斷利用雲端式分析和指標進行改善，確保身分分析能夠早一步發現行動迅速的攻擊者。身分分析警示會自動與其他警示進行分組，以顯示攻擊行動的逐步分析。

透過自訂規則找出迴避式威脅

自訂規則可讓安全團隊識別您所關切的特定威脅，以及以敏感度最高的資產為目標的攻擊。除了根據惡意軟體雜湊等 IoC 觸發警示以外，Cortex XDR 還可透過一種稱為入侵行為指標 (BIoC) 的自訂規則，揭露特定攻擊者的策略、技術和程序 (TTP)。針對進階偵測，關聯規則可協助您使用 Cortex XDR 的強大 XQL 查詢語言，從單一數據集或多個數據集找出複雜的行為組合。關聯規則可以識別系統和應用程式的濫用，並偵測零時差攻擊來遏止迴避技術，以確保即使在攻擊者操控惡意軟體名稱、雜湊或 IP 位址的情況下也能找出威脅所在。

您的分析師可根據包括程序、檔案、網路或登錄資訊等數十種不同參數來定義規則。超過 500 種預先定義的規則可用來偵測各種即時性威脅，包括持續性、篡改、權限提升和橫向移動。這些偵測功能會整天全天候運作，讓您高枕無憂。

Cortex XDR 檢查的數據

Cortex XDR 會分析 Palo Alto Networks 實體與虛擬新世代防火牆，以及Prisma® Access 所收集的流量日誌、增強型應用程式日誌和威脅日誌之中出現的通訊協定層級中繼數據。它也可以檢測 Cortex XDR 代理程式、第三方警示和日誌數據中的端點數據。透過建構以數百個行為層面為基礎的設定檔，包括連線頻率、流量來源和目的地、使用的通訊協定等等，Cortex XDR 可以了解使用者和裝置的預期行為。Cortex XDR 也會監控內部流量，以及從用戶端和伺服器到網際網路的傳出流量。

工作階段層級數據

防火牆流量日誌可提供分析使用者和裝置行為所需的中繼數據，其中包括：

- 來源 IP、目的地 IP、來源連接埠和目的地連接埠
- 傳送和接收的位元組
- 連線持續時間
- 增強型應用程式日誌，包括 DNS、HTTP、DHCP、RPC、ARP、ICMP 等等的交易層級數據
- App-ID™ 技術提供的應用程式詳細資訊

使用者數據

Cortex XDR 會分析網路流量和端點數據，以擷取使用者脈絡，例如：

- 登入使用者
- 機器的一般使用者
- 建立程序進行通訊的使用者
- Directory Sync 的使用者群組和組織單位
- Okta、Azure Active Directory、PingOne、PingFederate、Kerberos 和 Windows 事件日誌中的驗證事件

雲端數據

Cortex XDR 可從下列來源收集全面的雲端日誌：

- Prisma Access 和 VM-Series
- Google Cloud 平台和 Google Kubernetes Engine (GKE)
- Amazon CloudWatch 和 AWS CloudTrail
- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)

端點數據

Cortex XDR 會分析所有端點活動，包括：

- 檔案建立、刪除和更新
- 檔案雜湊
- 檔案路徑
- 處理程序名稱
- 登錄變更
- CLI 引數、RPC 呼叫和程式碼植入
- 硬體事件，例如 USB
- 事件日誌操縱
- Cortex XDR 代理程式安全警示
- WildFire 惡意軟體裁定

主機數據

Cortex XDR 會透過追蹤下列項目來識別機器：

- 主機名稱
- MAC 位址
- 作業系統

數據保留期間

- 最少 30 天

捕捉威脅並搜尋 IoC

無論分析師是執行獨立的搜尋還是從調查進行擴展，威脅捕捉在安全作業方面都扮演了關鍵角色。透過搜尋查詢，您的團隊可以搜尋特定的主機、檔案、程序、登錄更新、網路連線等，以找出可疑的活動。可以執行精確查詢，例如「主機上的特定程序對於特定檔案進行哪些變更？」，也可以執行開放式查詢，例如「顯示在網域中執行的所有程序」。您的安全團隊不需要學習新的查詢語言就可以搜尋攻擊行為和傳統的 IoC。分析師可篩選結果來減少事件數，以檢視並找出隱密的威脅。進階威脅捕捉專家可透過萬用字元和規則運算式執行複雜查詢、彙總並視覺化其搜尋結果，還可透過 XQL 搜尋功能來找出所有的數據。將威脅情報與完整的網路、端點和雲端數據進行整合之後，您的團隊就能在數秒內找出過去的攻擊或發現進行中的事件。

透過數據整合與自動化以快八倍的速度進行調查

若要加快任何威脅的分類和分析，您的團隊必須能夠隨時取得完整的調查脈絡。Cortex XDR 可提供數種重要功能來加速警示分類和事件回應。此一獨特的事件管理檢視會將相關的警示分組以描述攻擊的所有元素，包括受影響的主機和使用者、威脅情報詳細資料，以及如網域、IP 位址和程序等與事件有關的關鍵構件。警示分組和重複可減少 98% 的個別警示數量，因此可減輕警示麻痺。事件評分可讓您針對高風險的事件進行排名和排定優先順序以專注於真正重要的工作。您的團隊則可以排序、篩選或匯出事件和警示。您只需要按一下就可以調查任何來源的警示，並快速掌握相關事件的根本原因、信譽和序列，從而降低驗證威脅所需的經驗需求。

您的團隊可以使用下列分析檢視得出任何事件引發問題的確定答案：

- **根本原因分析檢視：**獨家獲得專利的分析引擎可連續檢視數十億個事件，以識別出隱藏在每個威脅中的事件鏈。它能夠以視覺方式呈現攻擊過程的根本原因，並提供與序列中每個元素有關的重要細節，使您更容易瞭解複雜的攻擊。您的分析師可迅速找出引發網路或雲端安全警示的端點程序，而不需要手動建立事件的關聯性或在主控台之間不停切換。

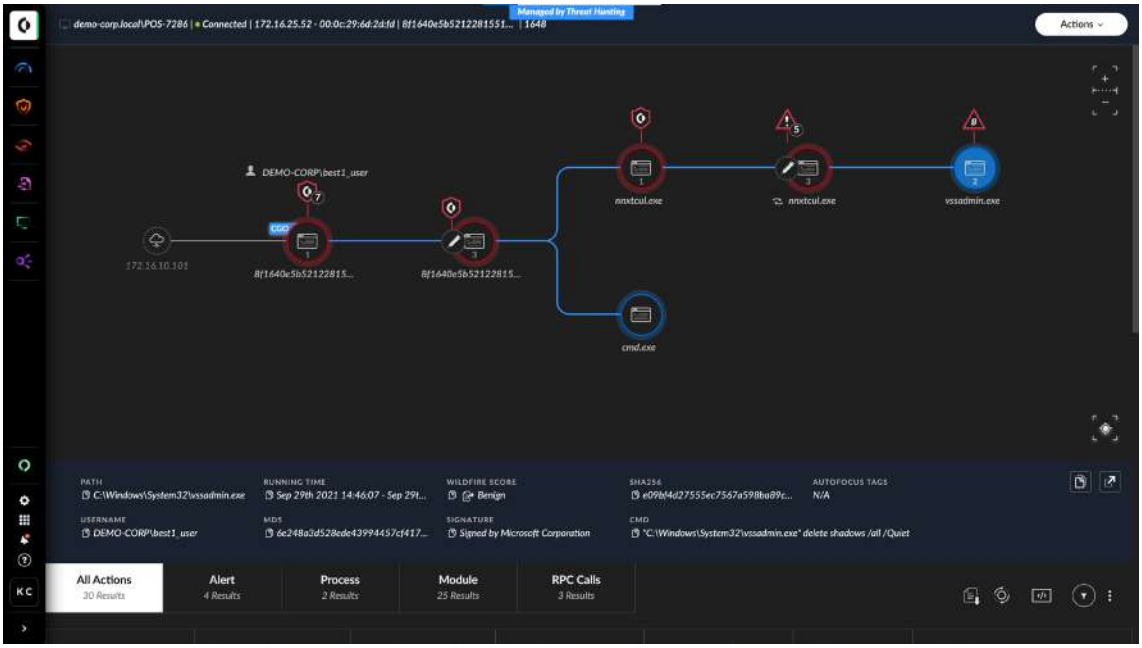

圖 9：Cortex XDR 會顯示警示的根本原因與關鍵構件

- **時間表分析檢視：**所有攻擊活動的鑑識時間表為事件調查提供了可化為行動的細節，使分析師能在幾秒鐘內確定範圍、影響和後續步驟。資訊警示可讓複雜的事件更易於了解，同時 MITRE ATT&CK® 視覺化也會顯示在事件中觀察到的所有攻擊策略和技術。

透過 Cortex XDR，您的團隊不再需要應付各種待處理警示以及棘手且耗時的分析，因此可減輕不少負擔。此外，它還可透過直覺式、視覺化的脈絡驅動工具來簡化警示分類和事件調查。以往需要耗費數小時、數天甚至數週時間的分析，如今都能在數秒或數分鐘內完成，且不需要具備特殊的專業知識即可完成。

以適合的方式回應威脅

當您發現威脅時，必須立即加以處理。Cortex XDR 可讓您的安全團隊立即從單一主控台消除網路、端點和雲端威脅。透過與執行點緊密整合，您的團隊可以快速阻止惡意軟體散播、限制針對裝置發動的網路活動以及更新威脅防禦清單 (例如惡意網域)。

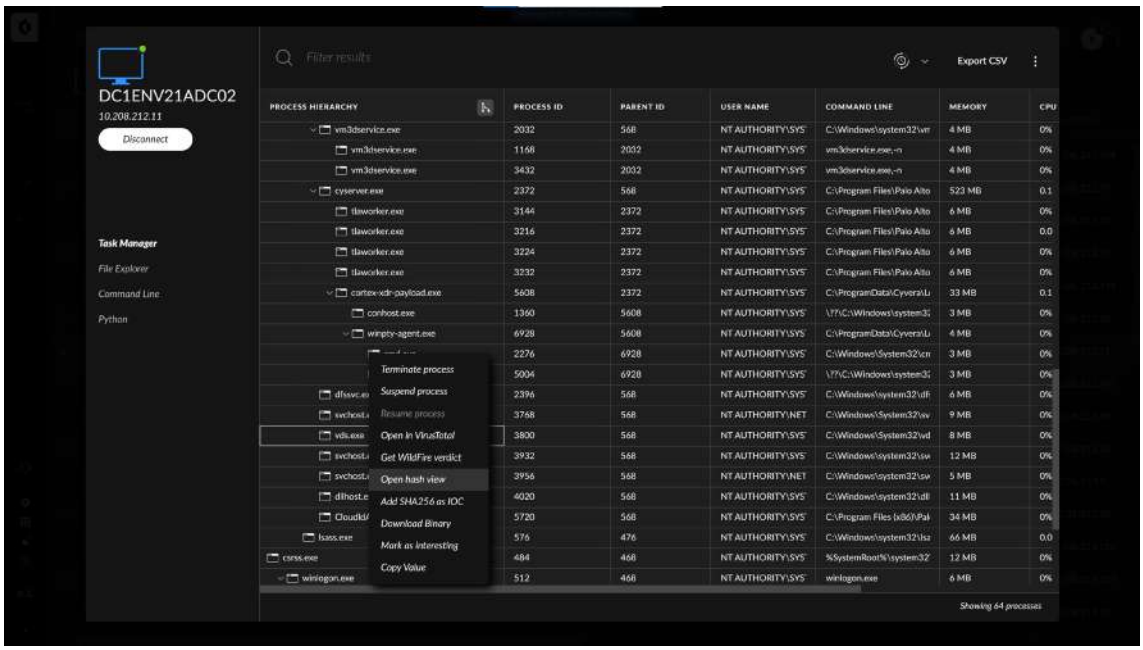

圖 10：Cortex XDR Live Terminal 工作管理員

您可以透過具有彈性的回應選項來消除威脅並實現：

- **隔離端點**，除了到 Cortex XDR 管理主控台的流量之外，停用遭入侵端點上的所有網路存取、防止這些端點與其他端點通訊，藉以避免感染其他端點。
- **終止程序**，阻止任何正在執行的惡意軟體繼續在端點上執行惡意活動。
- **阻止再次執行**特定檔案，方法是將該檔案列入政策中的封鎖清單。
- **隔離惡意檔案**，如果 Cortex XDR 代理程式還未隔離檔案，則將這些檔案從其工作目錄中移除。
- **擷取特定檔案** (從正在調查的端點中) 以進行進一步分析。
- **使用 Live Terminal 直接存取端點**，從而獲得業界最有彈性的回應動作，以執行 Python®、PowerShell® 或系統命令或指令碼；審視並管理主動程序；以及檢視、刪除、移動或下載檔案。您的團隊也可以在實施完整稽核時，在任何主機的實際環境中終止及刪除程序。在消除威脅期間，最終使用者隨時都可以繼續工作而不會遭遇干擾或停機。
- **使用開放式 API** 整合第三方管理工具、執行政策，並從任何位置收集代理程式資訊。
- **與 Cortex XSOAR 整合，**可進行安全協調、自動化和回應。您的團隊能夠與 Cortex XSOAR 共用事件數據，以實現自動化、由劇本驅動的回應並跨越超過 450 種第三方工具。Cortex XSOAR 劇本可以作為劇本任務自動提取 Cortex XDR 事件、擷取相關警示，並更新 Cortex XDR 中的事件欄位。
- **執行任何 Python 式指令碼**，並從 Cortex XDR 管理主控台或使用 Cortex XSOAR 等協調工具執行。立即可用的指令碼可讓您的團隊輕鬆地利用這個強大的功能。
- **迅速找到並刪除檔案**，您可以使用「搜尋和阻絕」功能建立端點檔案的索引以在企業中執行此動作。
- **將主機還原到無威脅的狀態**，並以補救建議為根據。補救建議會提供您執行下一個步驟的建議，並可讓您解決在事件中發現的所有活動。您可以透過移除惡意檔案和登錄機碼並還原損壞的檔案和登錄機碼來快速從攻擊中復原 — 不需要重新映像或建立自訂指令碼。

整合管理、報告、分類和回應

Cortex XDR 可在單一 Web 式管理主控台中結合端點政策管理、偵測、調查和回應，以提供順暢的平台體驗。您可以透過可自訂的儀表板快速評估安全狀態，並且可以根據隨需排定或產生的圖形化報告來彙總事件和追蹤安全趨勢。您也可以從集中位置輕鬆地部署及升級 Cortex XDR 代理程式。

Cortex XDR 會不斷進化以提早發現威脅並反制攻擊者。也可以將 Cortex XDR 與業界最全面的惡意軟體分析服務 WildFire 進行整合以識別惡意軟體。作為一種雲端原生應用程式，Cortex XDR 可運用社區提供的結果來識別攻擊者的最新手法並提高偵測準確性。

MITRE | ATT&CK®

在 MITRE ATT&CK® 第 3 輪的測試中，Cortex XDR 透過 100% 的威脅防禦和 97% 的可視性，獲得最佳的整合防護和偵測評分。

透過鑑識加快事件回應速度

Cortex XDR 鑑識是一種強大的分類和調查解決方案，可讓您在單一主控台上檢閱證據、捕捉威脅和執行入侵評估。Cortex XDR 鑑識的附加模組可透過深入的數據收集，使您能快速存取豐富的鑑識構件，並讓您判斷攻擊的來源和範圍，以及已在事件發生期間存取哪些數據 (如果有的話)。作為一種點對點解決方案，它可協助您進行事件回應的每一個步驟，包括數據收集、分析、威脅捕捉和補救。它是由事件回應者針對事件回應者所設計，可簡化調查程序以追蹤攻擊者的每個動作，並從 Cortex XDR 主控台迅速遏止威脅而不需要在安全工具之間切換。

透過受管理威脅捕捉讓您高枕無憂

Cortex XDR 受管理威脅捕捉可提供世界級威脅捕捉專家的全天候監控，也是業界第一個針對整合式端點、網路和雲端數據運作的威脅捕捉服務。我們的 Unit 42 專家會為您發現進階威脅，例如國家資助的攻擊者、網路罪犯、惡意內部人員和惡意軟體。為了偵測隱藏在企業中的攻擊者，我們的捕捉專家將仔細檢查來自 Palo Networks 和第三方安全解決方案的完善數據。

詳細的威脅報告會揭露攻擊的工具、步驟和範圍，因此您可以快速清除攻擊者，影響報告有助於您領先掌握新興威脅。

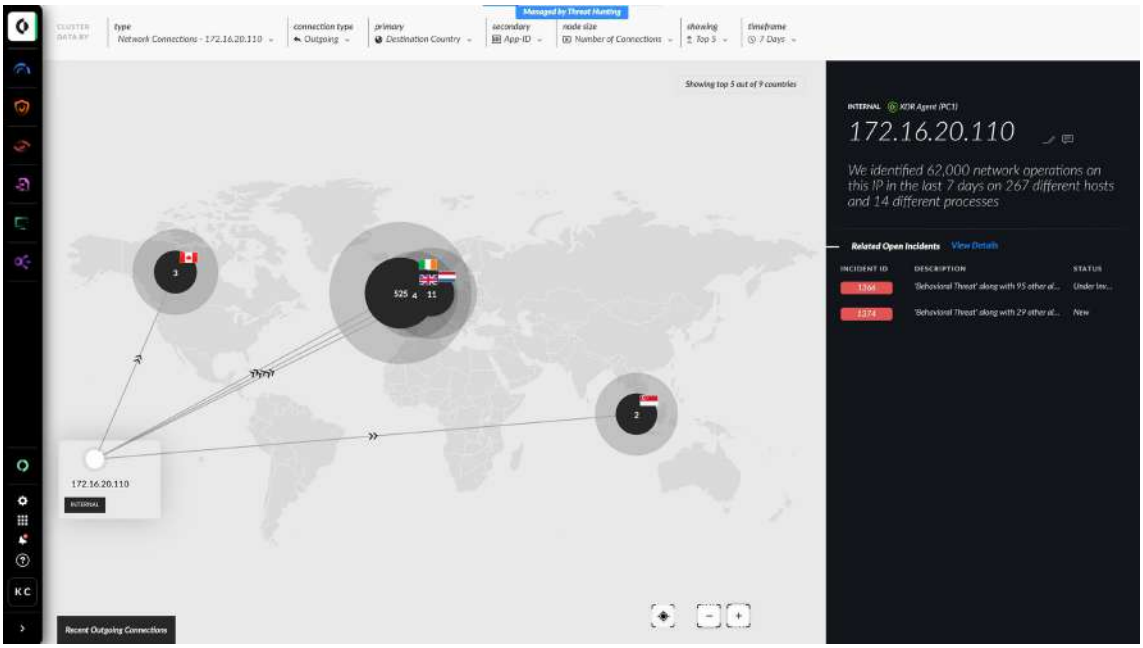

圖 11：IP 檢視 — 可化為行動的詳細資料以及與 IP 位址有關的調查脈絡

雲端部署的一道曙光

Cortex XDR 是一種雲端應用程式，不再需要部署額外的內部部署軟體或硬體。它會使用包括 Cortex XDR 代理程式在內的現有 Palo Alto Networks 產品作為感應器和執行點，進而簡化安全作業。從 Palo Alto Networks 基礎結構收集的數據儲存在 Cortex XDR 平台中，能夠提供高效率的日誌儲存，以便處理偵測與回應所需的大量數據。您可以快速部署 Cortex XDR，並避免設定新設備所需的費時流程。

Cortex XDR 代理程式可輕鬆部署到所有端點中，包括您的 Windows、macOS、Linux、Chrome® OS 和 Android® 系統而不需要重新啟動。Cortex XDR 代理程式可完美地搭配各種實體伺服器、虛擬機器 (VM) 和容器，可保護您所有的數位資產，包括行動裝置以及私有雲、公有雲、混合雲和多雲端環境。Cortex XDR 支援無障礙的 Kubernetes 部署，確保您的安全性能隨著雲端工作負載不斷擴展。

您可以從 Palo Alto Networks 新世代防火牆、Prisma Access、Prisma Cloud、Cortex Xpanse 以及其餘的 Cortex XDR 安全基礎結構儲存日誌數據，並減少您的日誌管理和 SIEM 成本。Cortex XDR 不再需要內部部署日誌儲存以及額外的感應器和執行點，相較於各自孤立的工具，平均可降低 44% 的整體擁有成本。Cortex XDR 能準確偵測攻擊並加快調查速度，可大幅提升安全作業團隊的生產力。

運用 Cortex XDR 提升安全性

現今的分析師正面臨巨大的挑戰。為了因應不斷增加的威脅，企業部署了越來越多的孤立工具，因而產生大量不完整且不正確的警示。傳統安全性資訊和事件管理 (SIEM) 產品並非使用雲端式機器學習來減少雜訊並找出難以偵測的攻擊，而是不斷累積安全基礎結構所識別並加以阻止的威脅相關警示。另一方面，孤立的偵測與回應工具迫使 IT 人員部署額外的硬體和軟體，但能提供的威脅相關資訊卻非常有限，這樣的盲點迫使分析師必須從多個工具收集線索並建立它們之間的關聯性。

Cortex XDR 會整合及分析所有的網路、端點和雲端數據，為分析師提供秘密武器來根絕隱匿在環境中任何地方的威脅。透過 Cortex XDR，您可以：

- 透過 Cortex XDR 代理程式防禦進階的惡意軟體、入侵和無檔案攻擊。
- 利用機器學習和分析自動偵測隱匿性攻擊。
- 揭露任何警示的根本原因，加快警示的分類和調查，進而提升所有安全分析師的生產力。
- 協調增強點之間的回應，快速控制威脅。
- 透過雲端原生部署簡化作業並提升規模和敏捷性。

透過 Cortex XDR，您將能在網路、端點和雲端資產中取得完整的可視性，確保所有的使用者和數據都能獲得妥善保護。

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號台北南山廣場 34 樓