Microsoft Security

轉用整合式威脅保護的 3 大理由

內容

前言

一般企業現在使用 30 多種不同的資安工具，通常彼此脫節且採「附帶式」。

資安防護體系正位於轉捩點。隨著組織持續應變從人才短缺和成本平衡到面對混合辦公壓力等挑戰，網路攻擊變得更加複雜。

同時，金融市場比以往更加支離破碎且複雜。一般企業現在使用 30 多種不同的資安防護工具，通常是不一致和「附帶式」，提供給資安作業中心 (SOC) 的可視性有限，洞察力也不不周全。

安全性與合規性領導者希望更瞭解最新的風險和威脅，但他們也需要知道哪些措施可行，哪些功能不完善，落差在何處。

雖然現今安全挑戰的範圍有時令人望塵莫及，但希望提高其安全作業效率和效益的資訊安全長還是抱持著樂觀態度。答案在於採用整合的端對端網路威脅防護方法，有助於組織：

理由 1：事半功倍

整合點式解決方案並降低安全性作業 (SecOps) 超載。

理由 2：讓 SecOps 專注在高價值工作上

使用可提高效率的工具，讓初級分析師比以往更有能力。

理由 3：提高員工生產力

保護組織的方式，讓人員在創造和創新時無所畏懼。

要實現此做法，需將延伸的偵測和應變 (XDR) 解決方案與使用人工智慧 (AI) 和自動化功能的雲端原生安全資訊和事件管理 (SIEM) 系統整合。整合式方案可協助您的 SOC 更預測性、主動性和預防性，以抵禦整個企業的攻擊。

理由 1

事半功倍

使用 Microsoft 整合工具，您也可以只為使用付費來節省成本。

許多組織透過具備單項優勢的點式方案來發展資安工具。不幸的是，這種方法實際上使資安專業人員更難以快速識別與應變威脅。這也最終導致 IT 的開支，並對終端使用者生產力造成負面影響。

由於組織都會尋求以較少成本達成更多成就，像 Microsoft 的 SIEM 和 XDR 等整合式方法可能會有所助益。這樣的方式能整合單一工具來降低複雜性，而且因為是雲端原生，整合式方案也可以改善效能和規模。

使用 Microsoft 整合工具，您也可以只為使用付費來節省成本。您也可以增加自動化和整合，減少管理方案所需的 SecOps 額外負擔。

> 開始接受新資安工具的過程很簡單，因為可預期落差將會不小。從這裡開始發展，您很快就會意識到不同廠商的工具可能會在功能上有所重疊。這種重疊對制衡與平衡來說可能不錯，**但也可能造成昂貴的財務成本。**」
>
> **Jonathan Cassar**
> MITA 技術長

160 萬美元

每年從廠商合併中節省的金額

Microsoft 委託 Forrester Consulting 進行《Total Economic Impact ™ (TEI)》研究，並檢查企業透過部署 Microsoft SIEM 和 XDR 可能實現的潛在投資報酬率 (ROI)。從這間虛構的複合型組織 (擁有 8,000 名員工和 10 名資安專業人員) 中，我們有了重大發現：

- **每年從廠商合併節省將近 160 萬美元**。Microsoft SIEM 和 XDR 投資可讓複合型公司降低之前 SIEM (560,000 美元)、相關現場基礎架構 (超過 360,000 美元)、三個 XDR 點式方案 (192,000 美元) 的成本，以及管理這些架構的持續人力成本 (480,000 美元)。
- **將重大資料外洩風險降低 60%**。此複合投資具備更有效率的安全性調查和回應工作流程、更高的資安應變自動化，以及保護所有運算環境 (包括多雲端保護) 的能力提高，進一步降低了資料外洩風險，每年可節省 160 萬美元。
- **產生 207% 的 ROI**。代表人員訪談和財務分析後發現，複合型組織在三年獲得 1768 萬美元的收益，成本只花了 576 萬美元，加總後淨現值 (NPV) 為 1192 萬美元。

理由 2

讓 SecOps 專注在高價值工作上

因此，重要的是將 SIEM 和 XDR 整合來關聯警示、排定最大威脅的優先順序，以及協調整個企業的行動。

SecOps 團隊因為必須分析的許多訊號而不堪重負，包括許多難以手動偵測 (如果不是測不到) 與緩解的低可信度訊號。隨著威脅增加，負擔過重的 SOC 很難跟上發展，特別是在嘗試分析來自多重點式解決方案的資料時更是如此。分配更多資源來填補缺口並不是解方，因為尋找熟練的安全性專業人員是項持續性的挑戰。

因此，重要的是要整合 SIEM 和 XDR 來關聯警示、決定處理最大威脅的優先次序，以及協調整個企業的行動，並透過先進的 AI 和自動化來主動偵測和修復威脅。

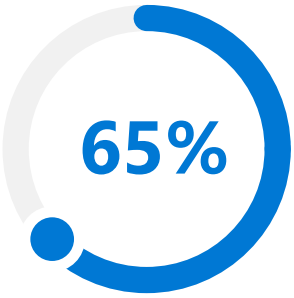
例如，請考慮單一的低層級訊號可能不會引起傳統 SIEM 的太多注意。然而，使用 AI，雲端原生的 SIEM 可以自動將該訊號與整個組織其他來源的訊號進行比較，並跨多個資料集相互關聯以尋找多階段攻擊。

整合的 SIEM 和 XDR 釋放 SecOps 資源，同時讓初級分析師擁有更多能力和把握。

然後系統會將資料常規化、分析和相互關聯，同時提供網路攻擊進入基礎架構的情境，以及它傳播的時間軸。這讓我們 SOC 團隊從單一主控台將資料外洩視覺化，並有效地處理它。

> 許多 CISO 都發現，**使用 20** 個單一管理平台或點式方案會對團隊造成額外負擔，並產生相關的年度花費 ... 我們透過單一供應商消除了對多種工具的倦怠感。」
>
> **Terence Jackson**
> Thycotic 資訊安全與隱私長

組織不應需要深入的專業技能來發揮資安解決方案的價值。整合的 SIEM 和 XDR 釋放 SecOps 資源，同時讓初級分析師擁有更多能力和把握。



SIEM 和 XDR Microsoft 方法將調查威脅的時間縮短 65%。

在 Microsoft 委託 Forrester Total Economic Impact ™ (TEI) 進行的研究中，顯示了複合型組織對此類 SecOps 的效益：

- **將調查威脅的時間縮短了 65%，並縮短了 88% 應變威脅的時間。**Microsoft SIEM 和 XDR 的整合式安全性威脅調查和應變做法，使複合型組織的資安專業人員更能透過這些工作流程發揮生產力。他們不再需要經過多個工具來找出威脅，而資安自動化功能可進一步強化應變的工作流程。
- **將建立新活頁簿的時間縮短了 90%，新資安專業人員的入門時間縮短了 91%。**Microsoft SIEM 和 XDR 的整合式方法，也使其他資安專業工作流程更有效率。由於 SIEM 資料已整合整個解決方案套件，因此建立活頁簿幾乎採自動化形式，單一登入可讓新的資安專業人員早 16 週上手。

理由 3

提高員工生產力

整合的 SIEM 和 XDR 解決方案可協助您的組織提高最終使用者的生產力。

除了事半功倍且提高 SecOps 效率外，整合的 SIEM 和 XDR 方案還可以協助您的組織提高最終使用者的生產力。

如 SecOps 團隊所知，當您努力確保安全性時，大家都會群起仿效。因此，當最終使用者體驗到的是阻礙而非協助員工發揮生產力時，組織可能會面臨更多的資安風險和更高的成本。密碼不足或遺失、透過個人裝置進行不安全的存取，或自由分享敏感性資料，這些都只是其中一些挑戰。

> 在過去，只要有人懷疑某個問題時，往往會採取大刀闊斧的方式處理。我們會將中止一切運作並關閉存取權限，這對業務帶來負面影響。每個人都很清楚這點，因為事情要暫時停止進行。在 Microsoft Sentinel 中，我們像有一把手術刀，可以對正在發生的事情做出反應。**企業通常甚至不知道**何時應變威脅，而這是衡量成功的重要標準。」
>
> **Rick Gehringer**
> Wedgewood 資訊長

幾乎

68,000

Microsoft SIEM 和 XDR 將其他員工的生產力每年總共提高了將近 68,000 小時。

整合的 SIEM 和 XDR 方法可協助您提供順暢的使用者體驗，讓您的人員在日常體驗的所有層面保持高效且安全。它可以減少對生產力的負面衝擊，例如必須關閉服務或隔離電腦再重新製作映像檔。但是，整合的 SIEM 和 XDR 還可以為終端使用者的工作效率提升創造新的機會，例如擁有更多的自助式安全性支援、更完整的儀表板和報告，以及執行較少的安全性代理程式而提高應變能力及加快開機時間。

在 Microsoft 所負責的 Forrester Total Economic Impact ™ (TEI) 研究中，假設共有 8,000 名員工的複合型組織部署了 SIEM 和 XDR，則 Microsoft 員工的生產力會提高：

- **其他員工的生產力每年總共提高了將近 68,000 小時。** Microsoft SIEM 和 XDR 防止其他員工受到不良資安程序的負面衝擊。例如，由於 IT 專業人員在安全性更新和建議方面自我服務的新能力，複合型組織每年多出了 4,000 小時。它還可在員工電腦上進行遠端安全性型疑難排解，並減少執行安全性代理程式的數量，以在終端使用者工作效率方面每年節省將近 64,000 小時。

安全性已成為技術成功不可或缺的推動者。因此，組織需要安全性措施，盡可能建立抵禦現代攻擊的復原能力，來保護和實現推動成長的生產力和創新。

取得與 SIEM 和 XDR 整合的網路威脅防護

這種領先業界的整合，在單一全面性方案下提供網路威脅預防、偵測和應變。

Microsoft 提供業界首創且唯一的整合式 SIEM 和 XDR 解決方案，在所有雲端和平台提供端對端可視性。這種領先業界的整合，在單一全面性方案下提供網路威脅預防、偵測和應變。

Microsoft SIEM 和 XDR 利用 AI 和自動化的力量，以及持續在網路威脅偵測和分析方面的深入投資：擁有專家洞察力和每天對 43 兆筆訊號的可視度。SOC 團隊整合了所有這些商品，其背景比以往都還要多，以更快的速度尋找和解析關鍵網路威脅：

Microsoft Sentinel

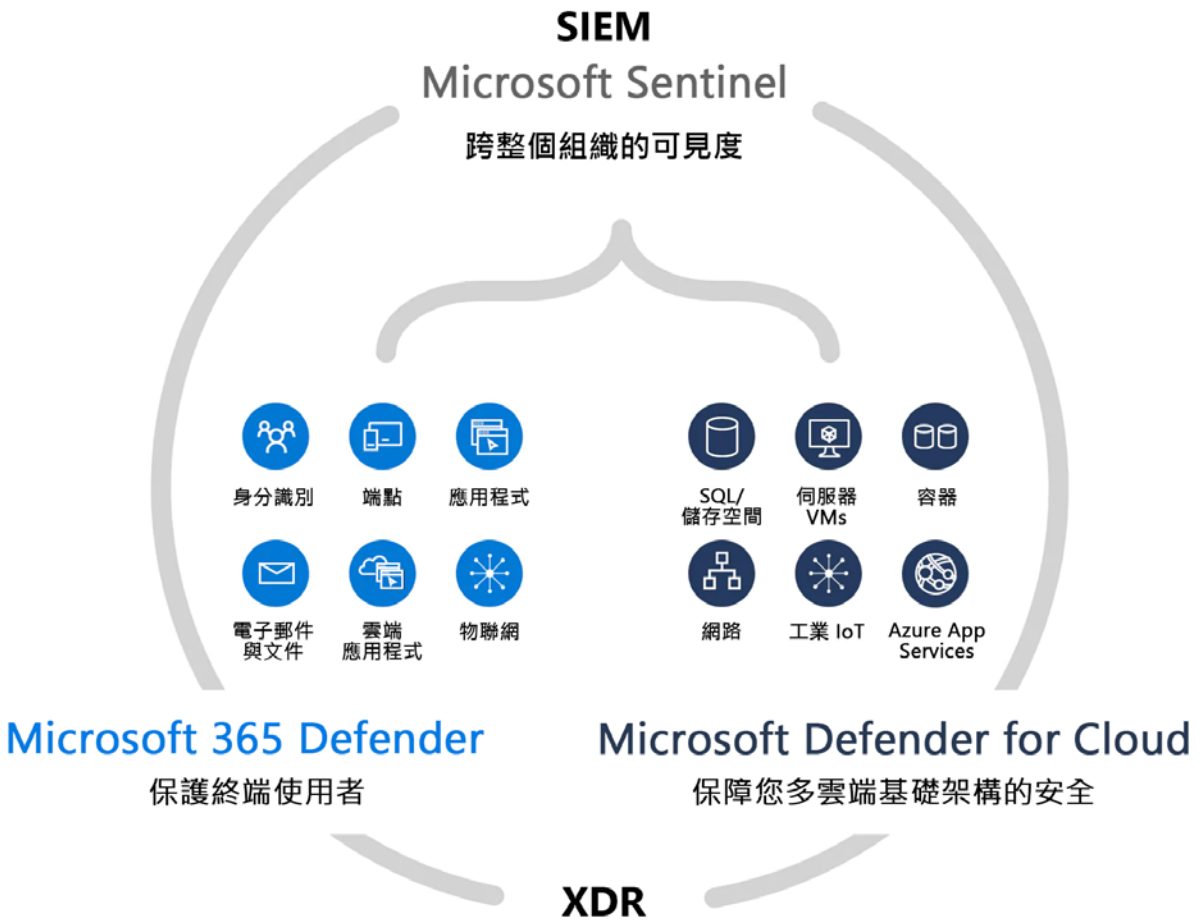
透過 Microsoft 雲端原生 SIEM，企業得以掌握全局。彙總幾乎任何來源的安全性資料，並採用 AI 來區隔虛實，在複雜網路攻擊鏈中建立警示關聯，同時借助內建的協調和自動化加快網路威脅應變。

Microsoft Defender XDR

使用 XDR 功能，防止並偵測跨身分、端點、應用程式、電子郵件、資料和雲端應用程式的網路攻擊。透過開箱即用且同級最佳的現成保護來調查和應變網路攻擊。尋找威脅，並輕鬆地從單一儀表板協調您的應變方式。

Microsoft Defender for Cloud

使用內建 XDR 功能保護您的多雲端環境和混合雲工作負載。保護您的伺服器、儲存設備、資料庫、容器等。透過區分輕重緩急的警示功能，將心力專注在最重要的事上。



別把資安防護當成附帶機制，而應由內而外構築而起。

將適當的工具和智慧掌握在合適的人手中。使用端對端、雲端原生的整合式方案來抵禦現代攻擊。

進一步瞭解如何過 SIEM 和 XDR 解決方案實現整合式網路威脅防護 >

Microsoft Security