BLACK CAT
INFORMATION 黑貓資訊

黑貓資訊 MDR/SIEM 資安託管服務

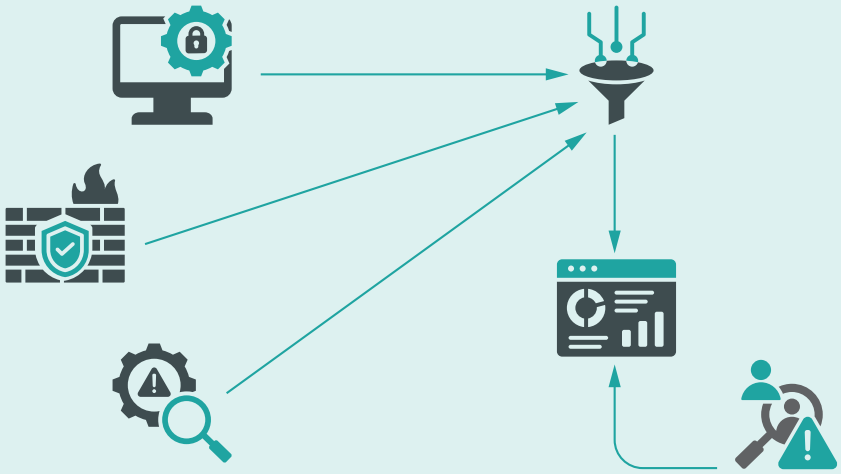
全面掌控資安態勢，強化企業防禦能力

在數位轉型與雲端應用普及的時代，企業面臨的資安挑戰日益升級。MDR（Managed Detection and Response，託管式偵測與回應）與SIEM（Security Information and Event Management，資安資訊與事件管理）服務，透過日誌集中管理、威脅情報整合、即時事件應變，協助企業建立完整的資安監控與應變機制，讓企業能夠即時偵測異常、快速回應威脅，降低營運風險。

服務項目簡介

日誌集中管理與事件溯源

MDR/SIEM透過統一日誌管理，整合端點、網路、防火牆、IDS/IPS等安全日誌，集中監控與分析。透過事件關聯與溯源，能迅速找出攻擊路徑，縮短調查時間，提高應變效率。



中文型錄 黑貓資訊 MDR/SIEM 資安託管服務

威脅情報整合與特徵更新

結合全球資安情報與AI分析，持續更新威脅特徵庫，協助企業即時掌握資安威脅。透過智能風險評估與自動應對，強化防禦機制，降低入侵風險。

定期安全報告與處置建議

定期提供資安健康檢查報告，含事件分析、風險評估與弱點建議，並由專家提供資安策略建議。透過專業監控與即時應變，降低管理負擔，強化企業防禦力。

服務功能與特色

功能	特色
日誌集中管理與事件溯源	• 收集多元安全日誌，實現統一管理與分析 • 持續監測安全事件，快速響應異常行為，有效提升防禦能力 • 透過數據跨關聯分析攻擊行為，提升威脅偵測準確性 • 追蹤攻擊來源與行為模式，加速事件調查與應變 • 分析異常模式，迅速辨識潛在資安威脅 • 快速定位威脅來源，縮短事故處理與復原時間
威脅情報整合與特徵更新	• 收集最新惡意軟體、APT 攻擊與異常行為資訊，強化防禦能力 • 整合蜜罐攻擊情資，提早預警攻擊趨勢 • 持續更新惡意攻擊模式，確保防禦機制能應對最新威脅 • 分析企業資安風險，提供即時應對處置，降低攻擊影響 • 依威脅評估結果，自動觸發應對策略，提升應變效率 • 快速偵測並攔截惡意行為，有效阻擋攻擊與資料外洩
定期安全報告與處置建議	• 評估機關企業資安狀態，優化安全防禦機制 • 解析攻擊事件來源與影響，提供具體風險報告 • 檢測系統漏洞與安全風險，提出強化建議 • 資安顧問提供最佳應對措施，確保防禦機制持續優化 • 透過專家團隊持續監控，快速回應安全威脅 • 提供完整資安報告與處置方案，減少機關企業資安壓力

11/04/25

中文型錄 黑貓資訊 MDR/SIEM 資安託管服務