BLACK CAT
INFORMATION 黑貓資訊

黑貓資訊資安加值服務

強化資安防禦層級，提升企業安全韌性

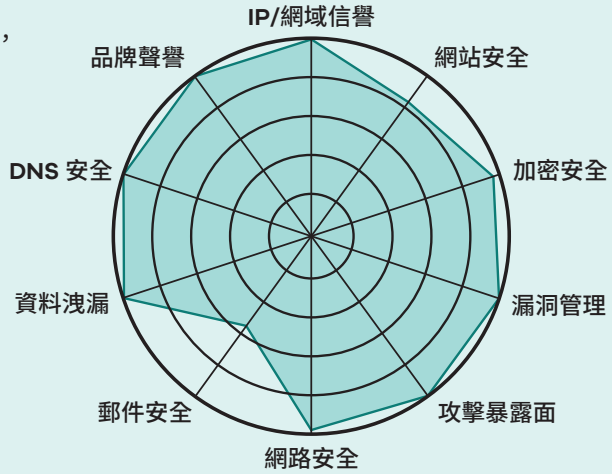
隨著駭客攻擊技術進化，企業面臨**內部資安意識不足**、**AD 網域權限管理缺陷**、**外部資產曝險**等風險，傳統防護已無法有效應對。

黑貓資訊提供**蜜罐建置部署**、**社交工程郵件演練**、**微軟 AD 網域安全強化**、**網際網路資產暨曝險管理**等加值資安服務，透過模擬攻擊誘捕威脅、測試員工資安意識、強化網域存取控管、監測企業外部資產風險，協助企業建立更完整的資安防禦機制。

服務項目簡介

網際網路資產暨曝險管理

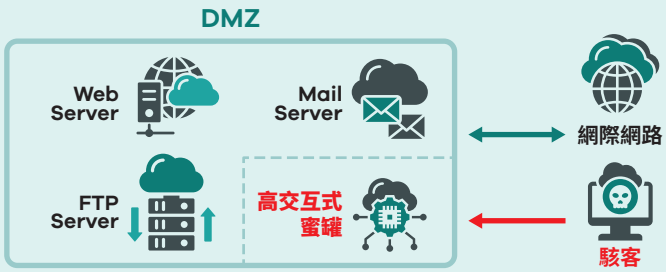
資產可視化、風險評估與安全評分，
快速識別弱點並制定改善計畫



中文型錄 黑貓資訊資安加值服務

蜜罐建置部署

模擬環境吸引駭客，蒐集攻擊行為，提早預警並調整防禦策略降低風險

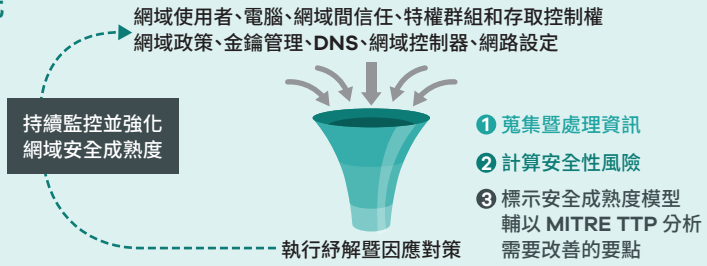


社交工程郵件演練

模擬釣魚攻擊測試應對能力，分析點擊率，強化資安意識降低人為風險

微軟 AD 網域服務安全性強化

強化微軟 AD 安全性，檢測組態、分析權限降低濫權與資料竊取風險



服務功能與特色

功能	特色	
網際網路資產暨曝險管理	• 發掘企業公開資產，從駭客視角分析潛在攻擊點 • 依法規標準評估資安風險，提供修正建議 • 追蹤明網、暗網的外洩憑證，預警與風險處置 • 監控企業外部資產變更，追蹤風險並提供應對策略	• 分析供應商安全狀況，降低供應鏈攻擊風險 • 檢測企業IT資產組成，包括設備、網站或服務風險 • 預防數位資產曝險，維護企業信譽與合規性
社交工程郵件演練	• 提供開信率、點擊率、資料輸入率等視覺化報表 • 支援批次發送與多樣化釣魚郵件設計 • 分析企業內部高風險員工，針對弱點人員強化 • 分析使用者是否輸入帳密等敏感資料	• 多樣化範本或客製化郵件設計，提升演練真實性 • 提供客製整合企業組織(部門)、演練對象資訊(姓名/分機)之服務 • 於系統中回溯每次演練結果，進行比較
微軟 AD 網域服務安全性強化	• 全面分析 Active Directory 配置，提供詳細安全性狀況報告 • 檢查密碼策略是否符合最佳實踐與合規要求 • 檢測 Kerberos 配置弱點，避免認證劫持攻擊 • 識別未使用或過期帳號，減少潛在安全隱患	• 對比 AD 組態與安全基準，找出偏離項目 • 識別高風險帳號與不當權限，降低權限濫用風險 • 提供整體風險評分，並建議改進策略強化安全性
蜜罐建置部署	• 模擬多種協議與互動式服務(HTTP、FTP、SSH等)以誘捕不同類型的攻擊者 • 即時監控並記錄攻擊行為，提供詳細的攻擊來源與方式資訊 • 透過圖表和儀表板展示攻擊數據，便於分析與決策 • 可根據需求增加或減少蜜罐節點，靈活部署在不同網路環境中	• 設計輕量化，對系統資源需求低，適合各種規模的企業使用 • 提供友好的使用者介面和詳細的文件說明，降低部署與維護難度 • 支援多種作業系統，方便在不同環境中部署

11/04/25

中文型錄 黑貓資訊資安加值服務