BLACK CAT
INFORMATION 黑貓資訊

黑貓資訊 EDR/XDR 端點與延伸威脅偵測及回應

多層防禦，智慧分析：結合 EDR 與 XDR 的現代資安解決方案

在當今網路威脅日益嚴峻的背景下，傳統的資安防護已無法有效應對新型態的攻擊。為此，EDR (Endpoint Detection and Response，端點偵測與回應)解決方案透過先進的威脅偵測與即時回應機制，提供更精準、高效的端點安全管理，確保資訊資產的完整性與安全性。而XDR (Extended Detection and Response ，延伸偵測與回應) 則進一步透過跨平台資安整合、智慧化威脅分析及自動化應變機制，協助企業全面掌握資安風險，實現更高效的威脅偵測與防禦能力。兩者結合使用，不僅能針對端點提供即時的威脅偵測與回應，還能跨越不同平台，整合並分析多源頭的安全數據，從而提升整體網路安全的智慧化、自動化防禦能力，幫助企業更好地應對複雜多變的資安威脅。

資料來源

- 網路日誌
- 身份日誌
- 終端日誌
- 伺服器日誌
- 應用程式日誌
- 電子郵件日誌

分析技術

- 異常資料移動
- 異常設備存取
- 高風險用戶
- 異常網路活動
- 機器主動回報
- 大量讀寫操作

偵測結果

- 內部橫向攻擊偵測
- 異常登入活動
- 指揮與控制通信
- 未授權資料存取
- 惡意軟體活動
- 特權升級攻擊

中文型錄 黑貓資訊 EDR/XDR 端點與延伸威脅偵測及回應

服務功能與特色

功能	特色	
防護與威脅應變	• 惡意軟體偵測 • 檔案行為分析 • 殭屍網路偵測	• 整合威脅情資 • 記憶體內行為監控 • APT 沙箱進階分析
集中管理與監控	• 自建主控台 • 圖像化關聯圖 • 事件流程進展圖	• AD 目錄服務支援 • 完整的事件紀錄 • 報表功能
進階端點安全管理	• 端點防護安全基線偵測建議 • 端點效能連線狀態監控分析 • 端點軟體資產整合威脅分析 • 資料庫與應用服務日誌威脅分析	• 端點自動化軟體更新修補派送功能 • VANS資通安全弱點通報機制 • 資安院 EDR 偵測回報機制
擴充偵測與回應	• 資安設備日誌分析與端點威脅關聯分析 • 防火牆威脅情資即時聯防機制	• 弱點掃描分析與管理 • 全日誌追蹤與管理

支援作業系統

作業系統	最低支援版本	備註
Windows	7 以上	
Windows Server	2008 R2 以上	
Linux - RHEL 系列	7 以上	支援 Red Hat、CentOS、Oracle Linux、Rocky Linux、AlmaLinux
Linux - Debian 系列	16.04 以上	支援 Debian、Ubuntu、Linux Mint
MacOS	12 以上	
FreeBSD	12 以上	

中文型錄 黑貓資訊 EDR/XDR 端點與延伸威脅偵測及回應