BLACK CAT
INFORMATION 黑貓資訊

智慧 XDR 防護 | IT 與資安無縫整合

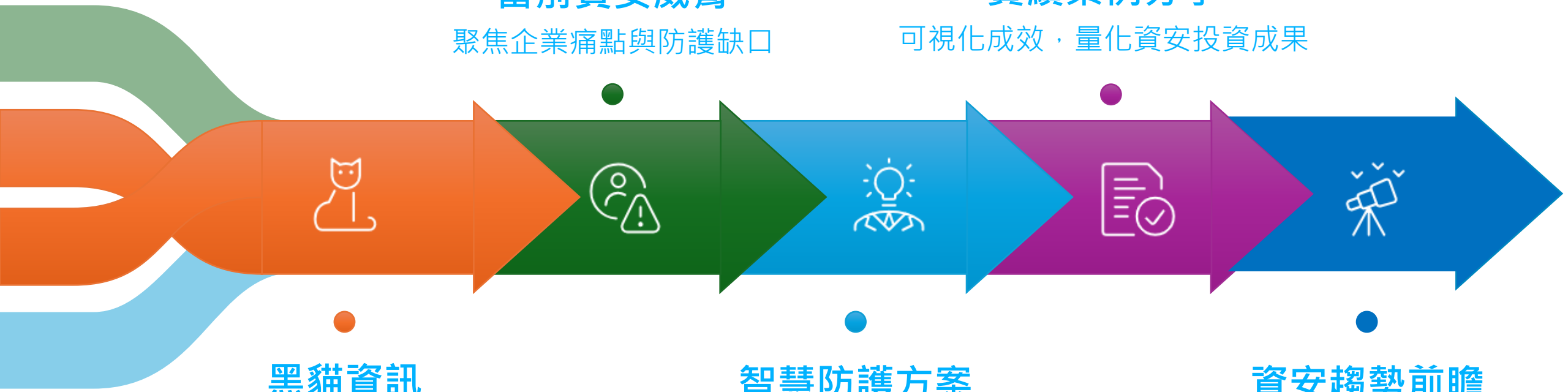
快速偵測 × 精準攔阻，全面掌控資安風險

黑貓資訊 游政卿

2025/4/15

blackcatinfo.com

簡報導覽



黑貓資訊
IT × 資安的整合防護顧問

當前資安威脅
聚焦企業痛點與防護缺口

智慧防護方案
打造全方位威脅偵測與即時應變能力

實績案例分享
可視化成效，量化資安投資成果

資安趨勢前瞻
提前布局，建構永續資安藍圖

黑貓資訊成長歷程

2017年12月 成立

1

整合 IT × 資安

- 於合勤投控體系下成立
- 聚焦企業 IT × 資安整合解決方案

2018-2020年 拓展

2

- 聚焦 EDR / MDR / XDR 技術研發
- 成立資安研究中心，整合全球威脅情報與回應機制
- 累積政府及大型企業專案實績

2021-2024年 平台建置

3

- 打造 SIEM + XDR 平台，推動 MDR / SOC 託管防護服務
- 服務拓展至國防、製造、醫療、公運等關鍵產業

2024 年 12 月 進駐竹科

4

- 通過國科會審查，進駐新竹科學園區
- 資安技術實力獲國家級認可

2025 年 ~ 服務進階

5

- 取得 ISO 17025 資通安全檢測實驗室認證
- 導入 AI + SOAR 技術，提升威脅識別與自動化應變效率

合勤資源 × 黑貓技術轉化為可衡量的資安價值

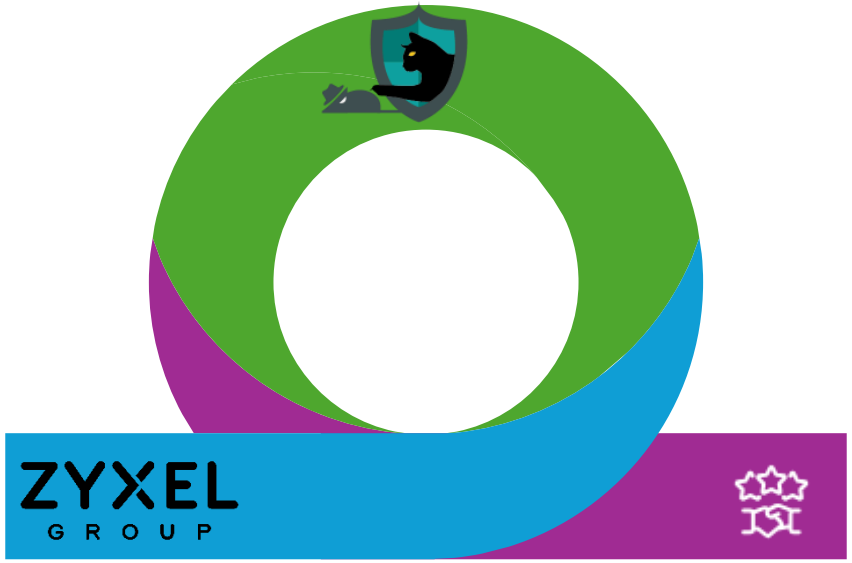
合勤集團全球資源

✅深耕電信、企業、工業及國防，精準掌握全球資安需求

✅全球 150+ 國市場佈局，解決方案符合國際規範

✅設立資安研究中心，建立全球威脅情報分享機制

✅導入 MITRE ATT&CK 框架，整合最新攻防策略



黑貓技術轉化成果

✅提供 IT × 資安整合服務，涵蓋 EDR / MDR / XDR 全方位防護

✅導入企業級測試驗證流程，確保方案穩定可信

✅符合 NIST SP 800-115 資通安全檢測標準

✅建構一站式資安平台，涵蓋 SOC 監控、威脅獵捕與事件應變

🎯 企業價值

✅ 高效資安防護

✅ 敏捷系統整合

✅ 對齊國際標準

臺灣資安市場地圖

黑貓資訊定位

✅服務領域：EDR / MDR / SOC、

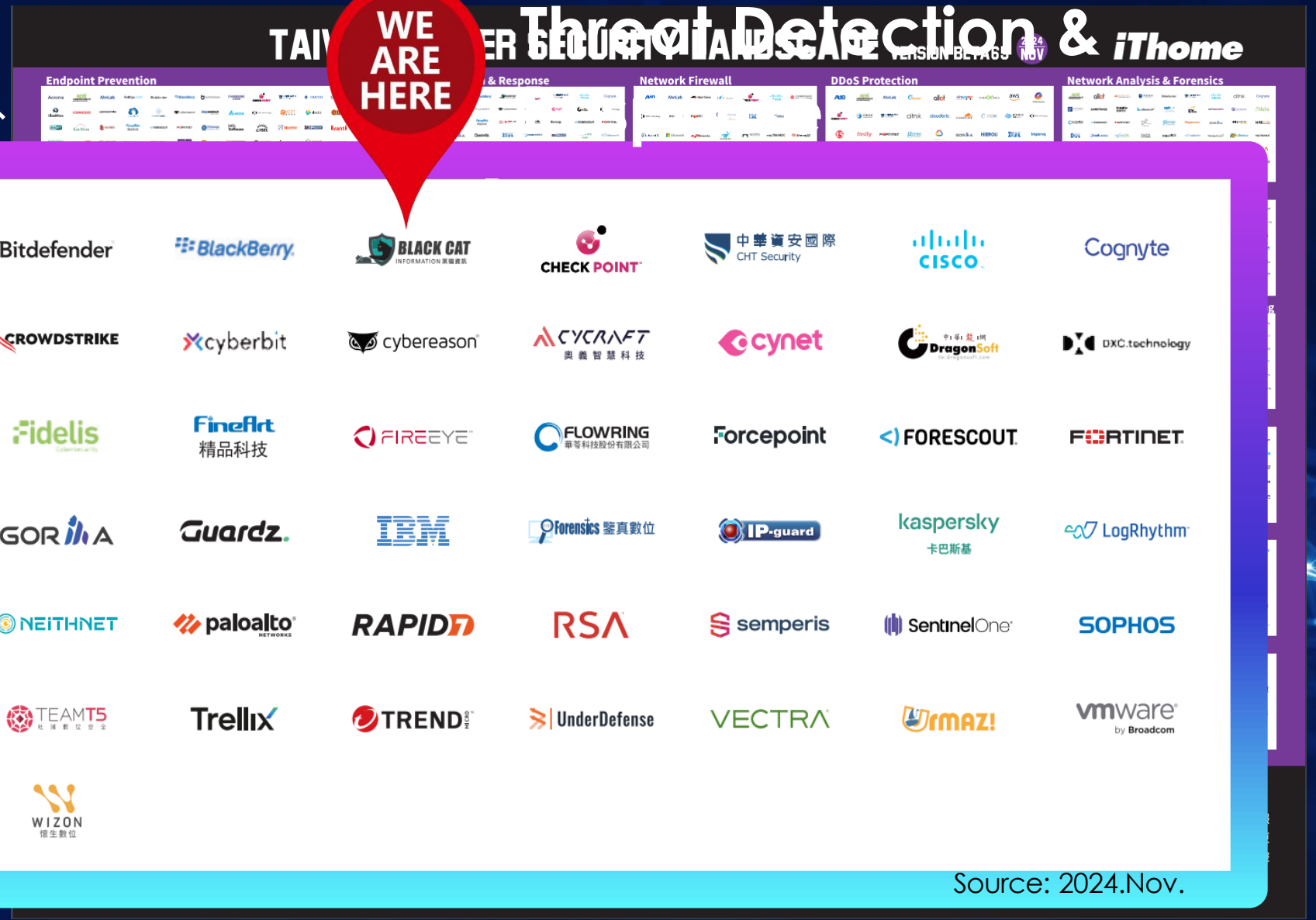
ICT 產品安

✅解決方

置、APT 威

✅競爭優

標準測評能



Source: 2024.Nov.

當前資安威脅及應對重點

進階持續性威脅 (APT)

- 多階段滲透，目標鎖定政府、製造、金融與高科技產業
- 關鍵基礎設施成為首要攻擊對象

新興科技威脅

- AI 自動化攻擊搭配深偽與社交工程
- 提升詐騙成功率與隱蔽性

企業風險

- 勒索攻擊與資料外洩頻傳
- 導致營運中斷、品牌受損與鉅額損失

應對重點

- ⚙️ 強化弱點修補與攻擊面管理
- 🔐 建立供應鏈資安治理架構
- 📈 全面提升企業資安韌性與合規能力

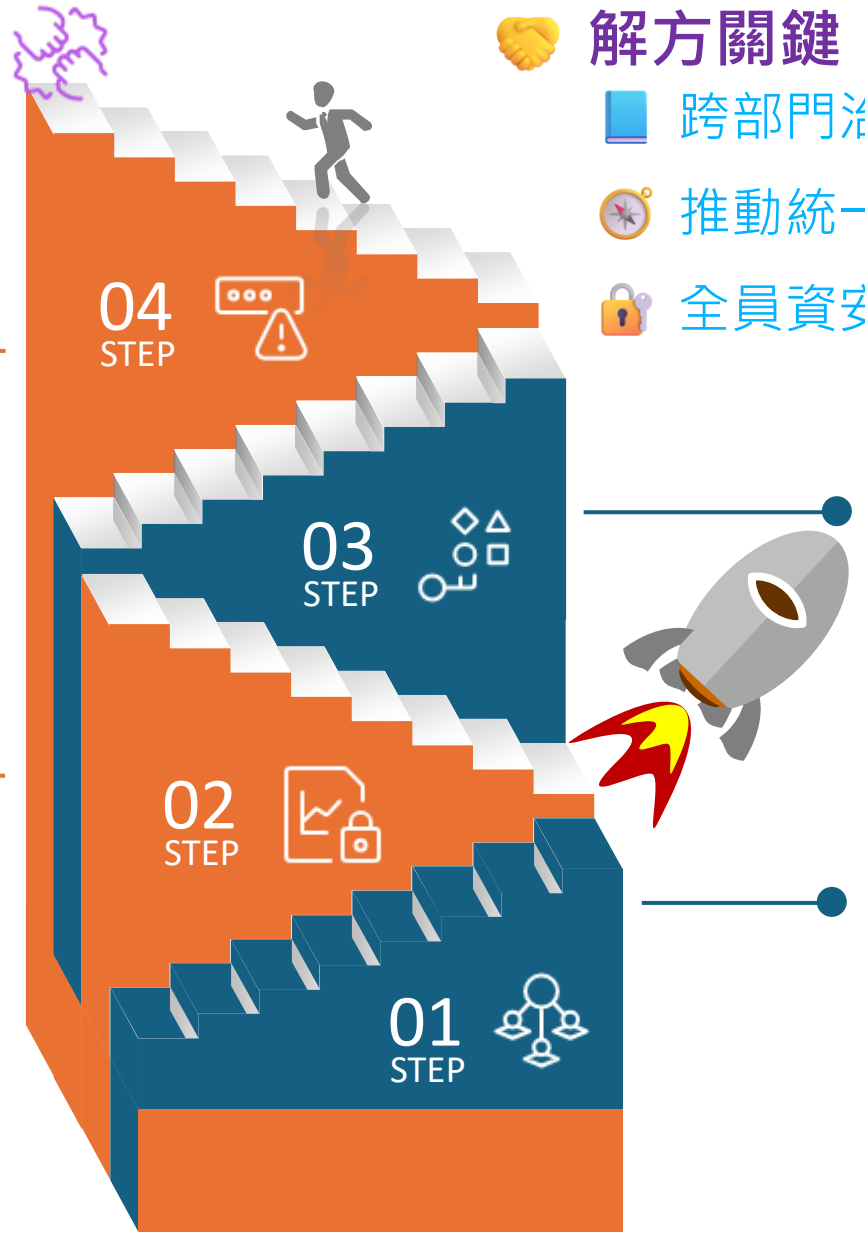
IT × 資安：打破部門隔閡，強化整體防禦效能

解方關鍵：建立共識，落實執行

- 跨部門治理共識
- 推動統一政策與職責分工
- 全員資安意識與行為落實

資安面臨的挑戰

- 告警延遲，回應速度偏慢
- 傳統防禦無法因應持續性攻擊 (APT)



資安需求

- ✅ 建立端點安全基準線防範
- ✅ 管理未授權存取與資料外洩

IT 面臨的挑戰

- 資產盤點與權限設計複雜
- 網路資源難以調校
- 群組政策管理費時費力

IT 需求

- ✅ 系統穩定運作
- ✅ 優化資源效率
- ✅ 快速排除問題

企業資安全面防禦方案

1 端點與橫向防護 (EDR/XDR)

- 主動防堵惡意程式與 APT
- 精準行為分析，辨識威脅
- 阻斷橫向擴散與設備跳躍

2 威脅監控與即時偵測 (MDR/SIEM/SOC)

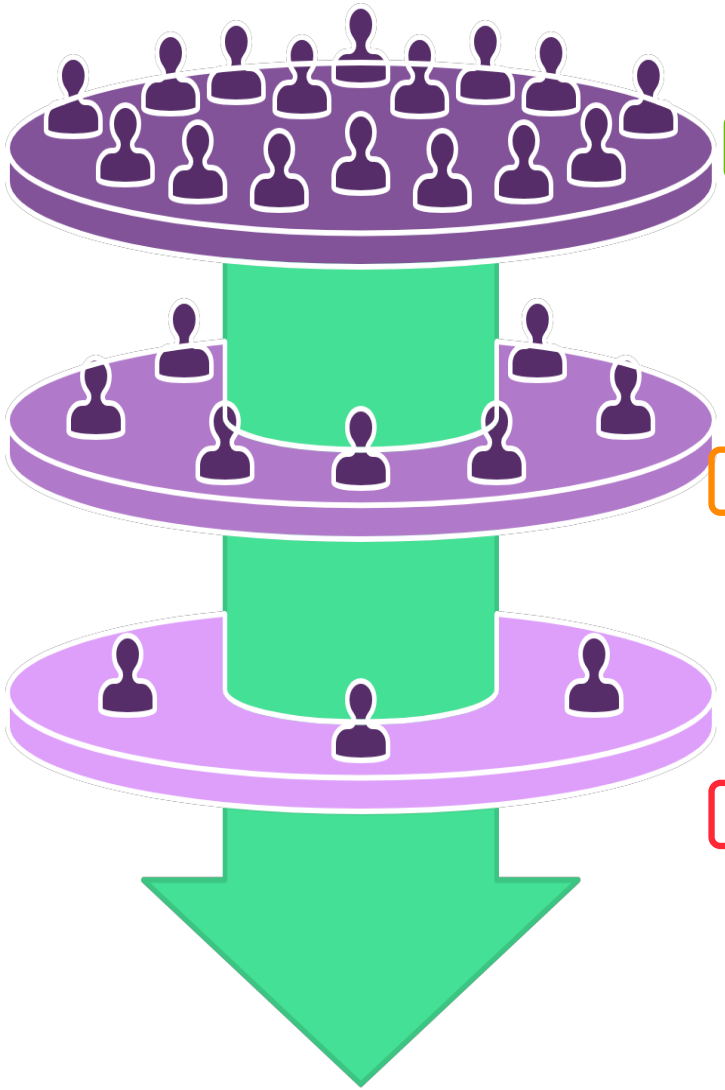
- 24/7 威脅監控與即時告警
- 結合 SIEM + UEBA，掌握異常行為
- 提早發現內部潛藏風險

3 產品與供應鏈資安檢測

- 遵循 ISO 17025、NIST SP 800-115 標準
- 建立 SBOM 與弱點掃描機制
- Web 滲透測試揭露攻擊面風險

UEBA 行為分析：從日誌中挖掘威脅線索

- UEBA 引擎處理三步驟



1 資料整合來源

2 行為建模與異常識別

3 威脅分類與風險評級

資料來源 10 +

彙整超過 10+ 類型日誌（AD、EDR、VPN、Proxy、DNS、Firewall...）

建立全方位使用者與設備行為視角

異常類型 150 +

分析超過 150+ 種異常行為類型

可疑登入 / 橫向移動非預期檔案存取 / 權限濫用等

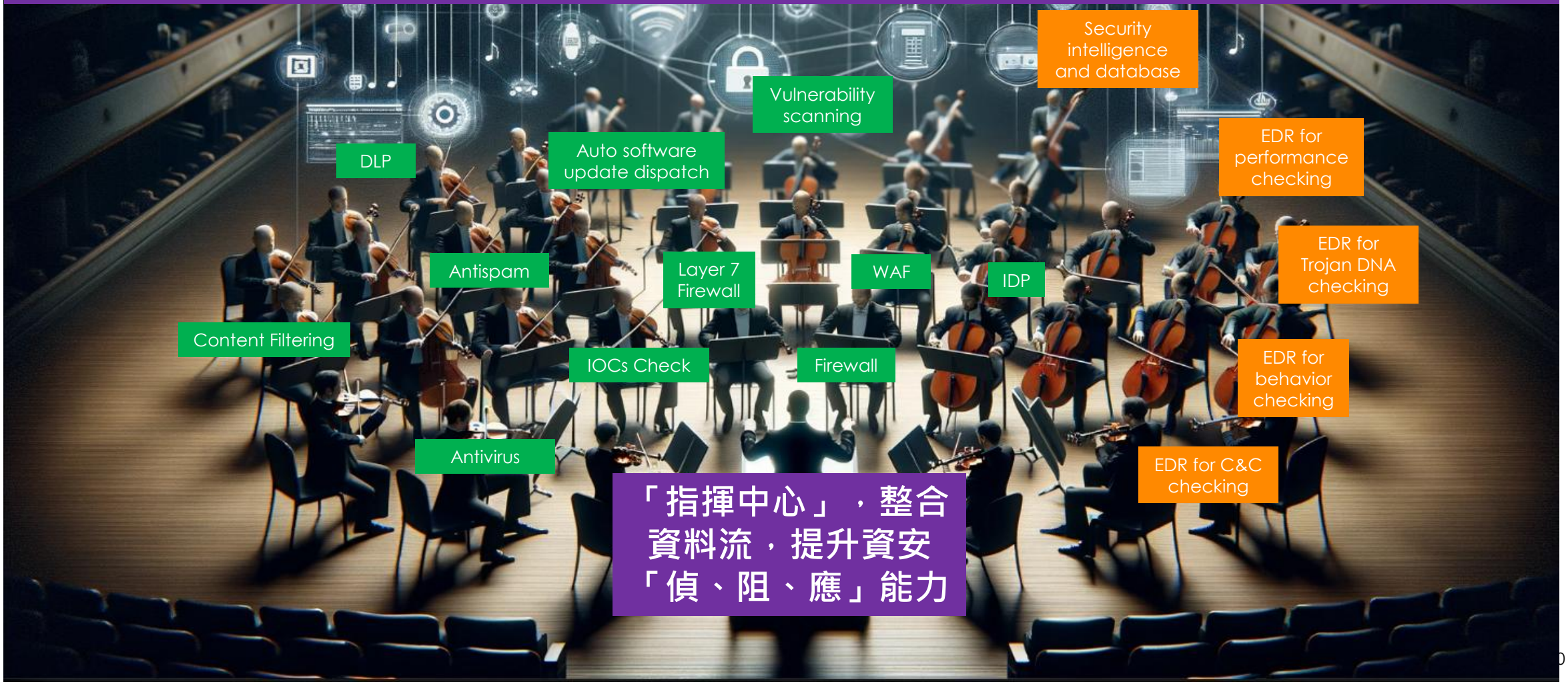
威脅分類 25 +

參照 MITRE ATT&CK 框架，分類 25+ 種威脅行為

自動標記風險等級，觸發後續回應

XDR 策略：如交響樂團協奏般的資安聯防

XDR 如同資安交響樂的指揮，透過統一平台協調防火牆、EDR、WAF 等多種資安工具，讓防護機制各司其職、協同運作，有效提升整體防禦力與威脅偵測效率



資通訊產品安全檢測

ISO 17025 ACCREDITED LABORATORY

NIST Special Publication 800-115

✅ 符合國際標準，協助企業發現潛藏風險，提升信任與資安成熟度

（符合 ISO 17025、NIST SP 800-115）

組態風險

開放服務掃描，找出不當設定

實戰驗證

滲透測試與弱點管理，驗證防護力

開源風險

SBOM 分析

檢查開源元件漏洞與授權風險

應用漏洞

Web 應用程式安全檢測

程式風險

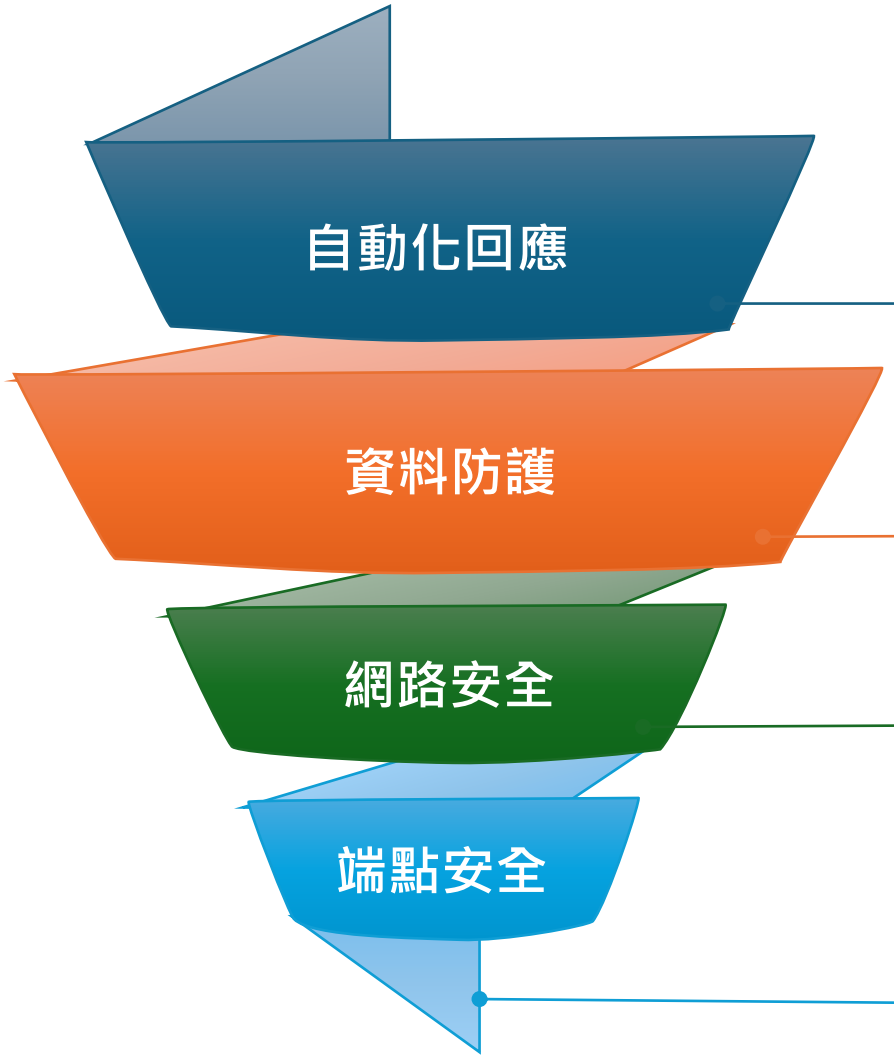
韌體靜態分析，挖掘潛在弱點

裝置通訊

設備防護能力評估與協議安全

面對 APT 攻擊，打造多層次防禦架構

🔒 從端點強化到自動化回應，全面提升滲透攻擊防護力



	基本對策	進階對策
自動化回應	事件通報（CSIRT）	導入 SOAR：加速應變流程
	日誌監控（SIEM）	定期演練：模擬攻擊、紅隊滲透測試
資料防護	郵件防詐	DLP 防外洩
	敏感資料加密	動態授權控管
網路安全	防火牆、IDS/IPS 部署	AI 異常行為分析
	網段隔離	C2 通訊阻斷
端點安全	MFA 多因子認證	UEBA 行為分析
	ZTA 零信任架構	微分段隔離攻擊
	定期漏洞修補	

導入標準驗證，強化資安合規與信任

🎯 轉化技術實力為市場競爭優勢通過國內外驗證，提升信賴度與採用率

✅ 符合資安規範，提升防護品質與競爭力

驗證項目	驗證內容	帶給企業的價值
國科會審查（竹科進駐）	通過國科會核準進駐新竹科學園區	強化技術可信度與曝光
VANS 通報機制	符合資安院要求，支援政府資產管理	強化資安合規體系，提升政府採用機率
EDR 偵測通報	符合資安院要求，與中華資安、安碁資訊完成端點安全監測與通報	增強端點防護力，滿足多方監管需求
ISO 17025 實驗室	通過國際資通訊產品安全檢測標準	符合國際市場進入門檻，提升供應鏈信任度

整合 IT 與資安，一站式解決三大痛點

從合規驗證到偵測應變，一站式提升資安韌性

- **資安防護三大痛點**

1. 資安商不熟 IT 環境
2. 設備難驗證資安性
3. SOC/SIEM 無法偵測未知威脅

- **黑貓的獨特優勢**

跨域整合

懂 IT，更懂資安管理

合規驗證

通過測試驗證

強化供應鏈信任

智慧偵測

縮短反應時間

掌握異常威脅

導入實績：攻防可見，成果量化

協助客戶從攻擊可視化、行為辨識到即時防禦，大幅降低資安風險

案例一

高科技製造業

資安議題	APT 年攻擊逾 500 次，難以有效偵測並防禦
黑貓解法	透過 XDR 行為分析，建立 24/7 全時偵測
實際成效	成功偵測並攔截 **98%** 進階攻擊 風險降低 **80%**

98%

案例一

學術研究機構

資安議題	內網異常存取問題嚴重，機敏資料存在外洩風險
黑貓解法	導入 MDR 全面監控方案 建立異常行為辨識機制
實際成效	橫向移動攻擊減少 **70%** 內網路可視性大幅提升

70%

應對挑戰的策略 – 資安挑戰與企業價值

合規與監管趨嚴 降低法規風險、守住營運底線	IT 與資安整合 強化內外防線、提升資安韌性	智慧驅動防禦 提升偵測精準度、加速應變效率
挑戰 ✅法規要求日益嚴格，企業面臨合規壓力	**挑戰** ✅遠距工作 + 混合雲環境，風險升高	**挑戰** ✅AI 假訊息、深偽攻擊難以即時偵測
黑貓解決方案 ✓ 通過 ISO 17025 安檢，強化供應鏈安全 ✓ 整合 SIEM + XDR，掌握弱點與通報機制	**黑貓解決方案** ✓ 推出 XDR 跨域防禦，保護端點、雲端、內網 ✓ 建立資產盤點與攻擊面監控	**黑貓解決方案** ✓ 導入 XDR 行為分析，降低誤判 ✓ 提供 24/7 MDR 託管服務
企業價值 ◆ 降低法規罰責與營運中斷風險 ◆ 降低供應鏈攻擊機會	**企業價值** ◆ 提升企業 IT 系統防禦力 ◆ 降低內部威脅風險	**企業價值** ◆ 提高威脅辨識效率 60% ◆ 縮短應變時間，避免業務中斷

立即行動，強化企業資安！

🟥 限時免費
企業資安風險評估

✓ 掌握 IT 設備與供應鏈風險

✓ 獲得專業安全建議

🔔 **限額 20 名免費名額！**

🟩 即刻體驗
外部資產風險掃描

✓ 掃描企業外部資產，預防潛在攻擊

✓ 發現暴露風險與漏洞

🔔 **限額 20 名免費名額！**

🟦 預約體驗
整體資安解決方案

✓ 學會如何透過行為分析預警威脅

✓ 體驗 SIEM/SOC 即時監控與回應

🎁 **首 3 個月免費體驗！**

📍 展覽地點：1F | 合勤集團 C118 攤位

🔗 更多資訊：https://www.blackcatinfo.com

BLACK CAT
INFORMATION 黑貓資訊

謝謝您的聆聽

📍展覽地點：1F | 合勤集團 C118 攤位

🔗 更多資訊：https://www.blackcatinfo.com