FORESCOUT

★ 由Forescout其他解決方案所支援

EXTENDED DETECTION RESPONSE

X D R

OPEN (跨廠牌支援)

- 支援超過 180種資源來源:
  - 12 EDRs
  - Security 資安工具
  - Infrastructure
  - Enrichment
  - Applications
  - Cloud
- 超過1500條威脅檢測規則
- 持續增加新的資料來源及規則

★設備狀態 & 組態數據

≦1 真實威脅/每小時*

- 高於傳統SOC 450倍偵測率
- 2階段偵測引擎(應用5種偵測技術) :
  - Cyber intel
  - Signatures
  - UEBA
  - Stats/outliers
  - Algorithms (context-aware AI/ML)
- 整合MITRE ATT&CK®識別攻擊鏈

★設備狀態 & 組態數據

*平均值，基於每小時約5000萬條日誌的攝取量

全範圍威脅響應

- **強大的威脅調查功能**
- 整合事件案例管理 & SIEM

★觸及每一個連線設備 (已納管 & 未納管)

★網路及主機響應包含:

- 限制流氓資產/基礎架構
- 隔離資產
- 關閉埠口
- 限制訪問權限
- 啟動強制性的應用程式和程序
- 更新代理/套用修補程式
- 終止未經授權的應用程式
- 停用外圍裝置

MANAGED & UNMANAGED

CLOUD / CONTAINERS | IT | IoT | IoMT | OT / ICS

- **高度整合功能提升SOC效率及成效:**
  - 先進數據管道
  - 威脅偵測引擎
  - SOAR
  - UEBA(使用者與實體行為分析)
  - 威脅情報平台: 70 種來源
  - Custom rules
  - 整合事件案例管理 & SIEM
  - 管理者角色客製化儀表板
- **雲端資料湖:** 高成本效益，分層的日誌存儲 (Hot, Warm, Cold):
  - 31天
  - 365天
  - 自定義
- **企業級:**
  - 雲端服務
  - 多用戶架構
  - 跨國際部署
- **價格策略:** 價格親民且計價方式簡易。基於端點數量，而非日誌檔案大小
- **效益量化:** 確保價值快速顯現(只需幾天而非耗時數月)
- **★主動降低風險:** 透過與Forescout模組連動有效減少攻擊面，降低受到威脅或未合規設備首次連線到您網路的風險

若需更多資訊請至Forescout TW粉絲專頁或來信洽詢

郵件信箱:
vian.chen@forescout.com
粉絲專頁:
https://www.facebook.com/FORESCOUTtw/