

# 針對威脅獵捕之資料最佳化與效率提升技術研發計畫

## 啄木科技股份有限公司

創立日期 110年06月23日

負責人 邵逸青

經營項目 資訊安全套裝軟體、資安可視性解決方案

### 創新動機

後疫情時代的全球經濟衰退對各產業帶來了控制資安防護預算的壓力。然而，這也為資安產業提供了機會，進一步展示其價值和報酬率。透過強調投資回報、優先確定關鍵風險領域、提供整合性解決方案以及合作整合的策略，資安產業可以在這一環境中找到成功的機會，為企業提供卓越的資安保護。本公司的產品屬於 XDR 類型，可以跨網路、端點與其他資料源分析，解決企業資安防護的核心需求，這也與近年來推廣的資安營運中心 (Security Operation Center, SOC) 之核心概念不謀而合。然而，各資料源的蒐集與處理在實務上卻是一大挑戰，在不影響 AI 分析與威脅獵捕的前提下，如何精確地減少或過濾原始資料、提升資料蒐集效率與資料使用效率成為非常困難、但迫切需要改善的問題。因此，我們申請了新竹市地方型 SBIR 計畫，

希望藉由研發新技術來克服這些困難，並進一步提升產品價值。

我們非常感謝新竹市政府對創新的重視與鼓勵。此計畫有效緩解了新創公司在研發資金上的困境。在政府的支持下，我們將加速創新技術的產品化與商業化過程，並藉此提升產品的商業價值，為新竹市的資安與科技發展做出貢獻。

### 重點成果

本計畫產出的研發成果，在不影響威脅分析偵測率與事後案件調查的前提下，大幅降低原始資料數量並提升資料使用效率。其中程序執行相關系統日誌與裝置資訊相關系統日誌分別降低 89.86% 與 99.96%，成果卓越超乎預期；而網路流量蒐集方面亦開發彈性的多元網路流蒐集架構並新增一種蒐集方法，以因應複雜的企業網路環境；後續的跨源資料利用，透過新

研發之威脅獵捕資料處理演算法，調查資安事件所需的查詢等待時間減少約 72.7%，有效提升資安人員調查與回應的時間。以上的計畫成果，讓整合性跨源資安威脅分析與獵捕能成為實際可行之解決方案，大幅增加本公司 Woodpecker XVR 的商業價值。

### 未來創新

本公司目前全力發展 Woodpecker XVR 資安可視性解決方案，未來規劃研發更多具有吸引力的資安產品，以創造更全面的產品線，滿足市場需求。

### 在地回饋

我們是一家新竹在地新創公司，雖然資源有限，但對資訊安全的熱情驅使我們積極回饋社會。我們希望利用資安專業，透過免費研討會幫助企業提升資安防護相關觀念，並促進同業 / 異業交流與合作。目前市場上大多數研討會在台北舉行，但我們相信地方活動能促進新竹的產業發展，計畫執行期間我們在新竹協辦了兩場實體研討會，提升地方廠商的資安技術與經驗交流，協助地方經濟與技術進步。身為新竹資安廠商，除了提供最即時的資安諮詢與服務，亦能為新竹資安人才提供就業機會，致力於研發更優

質與完善的解決方案，並活絡在地資安產業發展創造正向循環。

### 執行過程中得到的協助

新創公司對於市場常常過於樂觀，容易錯估市場的現實性，故在撰寫申請計畫書時容易掌握不到方向，很感謝計畫辦公室與審查委員的協助，提出非常犀利且精準的建議，讓我們修正產品研發方向與市場定位，更有機會在市場上博得一席之地。

#### 量化效益

- + 增加產值 5000 仟元
- + 衍生商品或服務數 1 項
- + 額外投入研發費用 300 仟元
- + 增加就業人數 1 人

