課程名稱：18507_資安事件應對與災難復原 課程摘要

🎯 1. 適合對象與能力門檻

- **適合族群**：企業資安工程師、IT/網管人員、系統管理員、資安主管，以及供應鏈中需要處理資安事件與事故調查的專業人員。
- **能力門檻**：普通。建議具備基礎的網路通訊協定（如 IP、Port、DNS）及作業系統維運常識，課程將帶領學員學習實務事件應變與工具操作。

📚 2. 課程核心大綱與架構圖

- **章節架構**：
  - **章節一：資安事件現況與供應鏈威脅** — 剖析一天數百張事件單的應對機制、旁門左道（供應商/協力廠商）攻擊手法與旁路滲透。
  - **章節二：常見攻擊行為與網路流量剖析** — 利用 Log 視覺化工具分析阻斷服務（DDoS）、SQL 注入攻擊（SQL Injection）與 LocalHost 本機後門繞過機制。
  - **章節三：資安事件應變架構與 MITRE ATT&CK 框架** — 介紹 NIST 事件回應流程與美國 MITRE ATT&CK 駭客戰術矩陣（14 個戰術策略）應用。
  - **章節四：社交工程攻擊與生成式 AI 威脅實例** — 解析生成式 AI 被駭客用以製作極真社交工程郵件（包含洋蔥網路與客製化履歷/合約釣魚）。
  - **章節五：事件調查、採證與日誌/封包分析工具** — 實作 WebCheck 快篩工具、Sysinternals Suite 免安裝工具包、Wireshark/一對二分流器封包側錄 與日誌（Log）分析。
  - **章節六：災害復原（DR）與實務案例復盤** — 剖析 Lockbit 3.0 勒索軟體案件應變、備份計畫設定與 Rookit/核心模式隱藏防範。

🛠️ 3. 必備前置知識清單

- **基礎網路協定與系統概念**：了解基本 TCP/IP 封包、DNS、HTTP/HTTPS 及網路區段（如對外服務區、內網、Internet）劃分。
- **作業系統日誌概念**：對 Windows Event Log 或 Linux Syslog 之基礎讀取與收集有初步概念。

📖 4. 專有名詞與概念辭典

- **IOC (簡失指標 / 威脅指標)**：由大數據分析或情資平臺產出的惡意檔案 Hash 雜湊值、惡意 IP 或域名，用以快速比對系統是否遭入侵。
- **MITRE ATT&CK 框架**：由美國非營利組織產出的駭客攻擊戰術矩陣（包含偵查、初始入侵、執行、橫向移動、衝擊等階段），協助防守方（藍隊）以統一語言歸納攻擊軌跡。
- **Sysinternals Suite**：微軟官方維護且免費的免安裝系統工具包（包含 Process Explorer、AutoRuns 等），適合放入乾淨的隨身碟進行現場資安事件調查與鑑識。
- **EDR (端點偵測與回應)**：相較於傳統防毒軟體僅比對檔案特徵（偵測率常低於 60%），EDR 專注於監控端點電腦的異常行為特徵（如呼叫可疑 Localhost 流量或異常程序）。

💼 5. 課程學習職能對照

- **對應職能名稱**：資安事件應變工程師 / 資訊安全分析師 / 資安鑑識與調查人員
- **主要工作任務/能力指標**：
    - **資安事件識別與應變決策能力**：能判定資安事件影響範圍與優先救援順序，運用 MITRE ATT&CK 框架定位駭客攻擊階段並完成隔離。
    - **事件調查與數位採證能力**：能操作 Wireshark 側錄封包、使用 Sysinternals 提取系統證據，並依據完整的 Log 日誌撰寫事件調查報告。