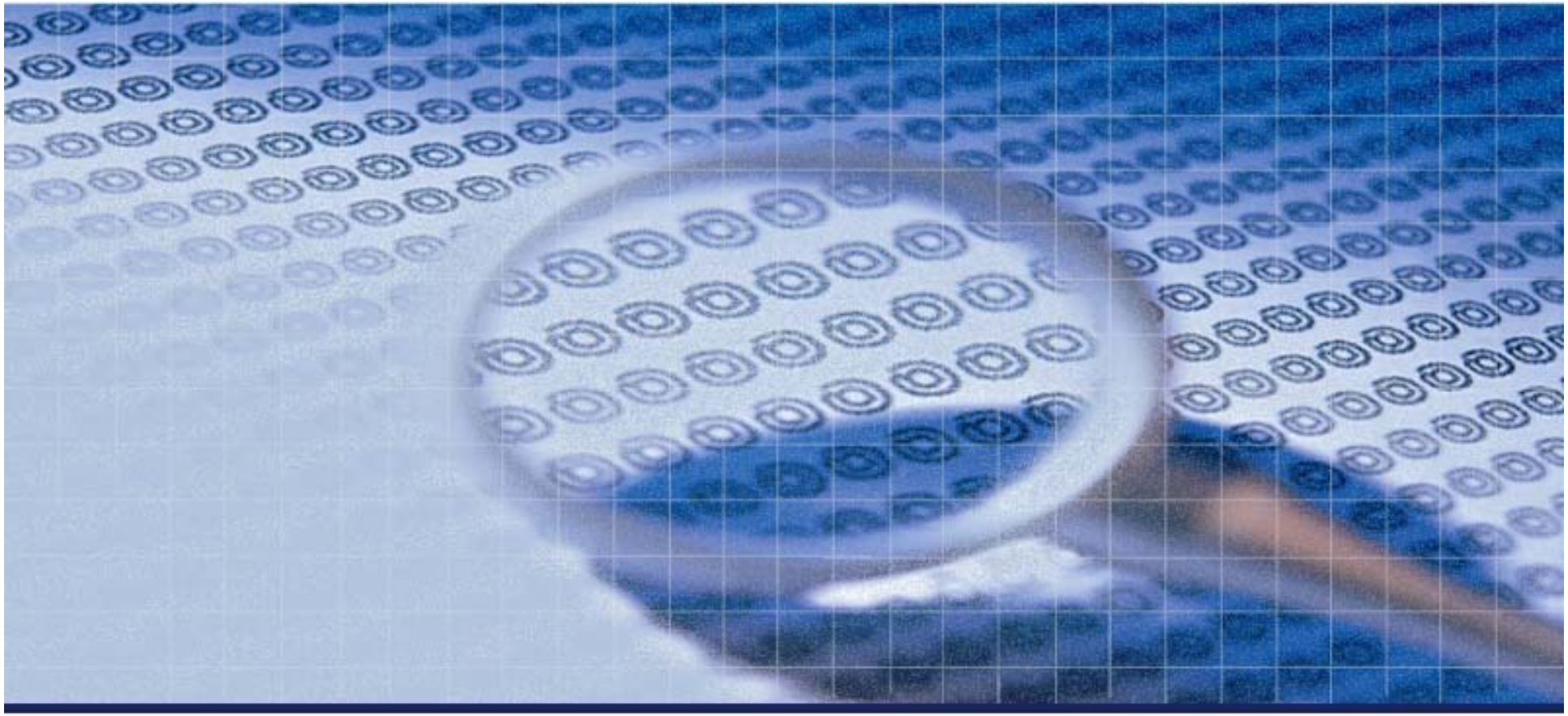


惡意程式解析訓練課程

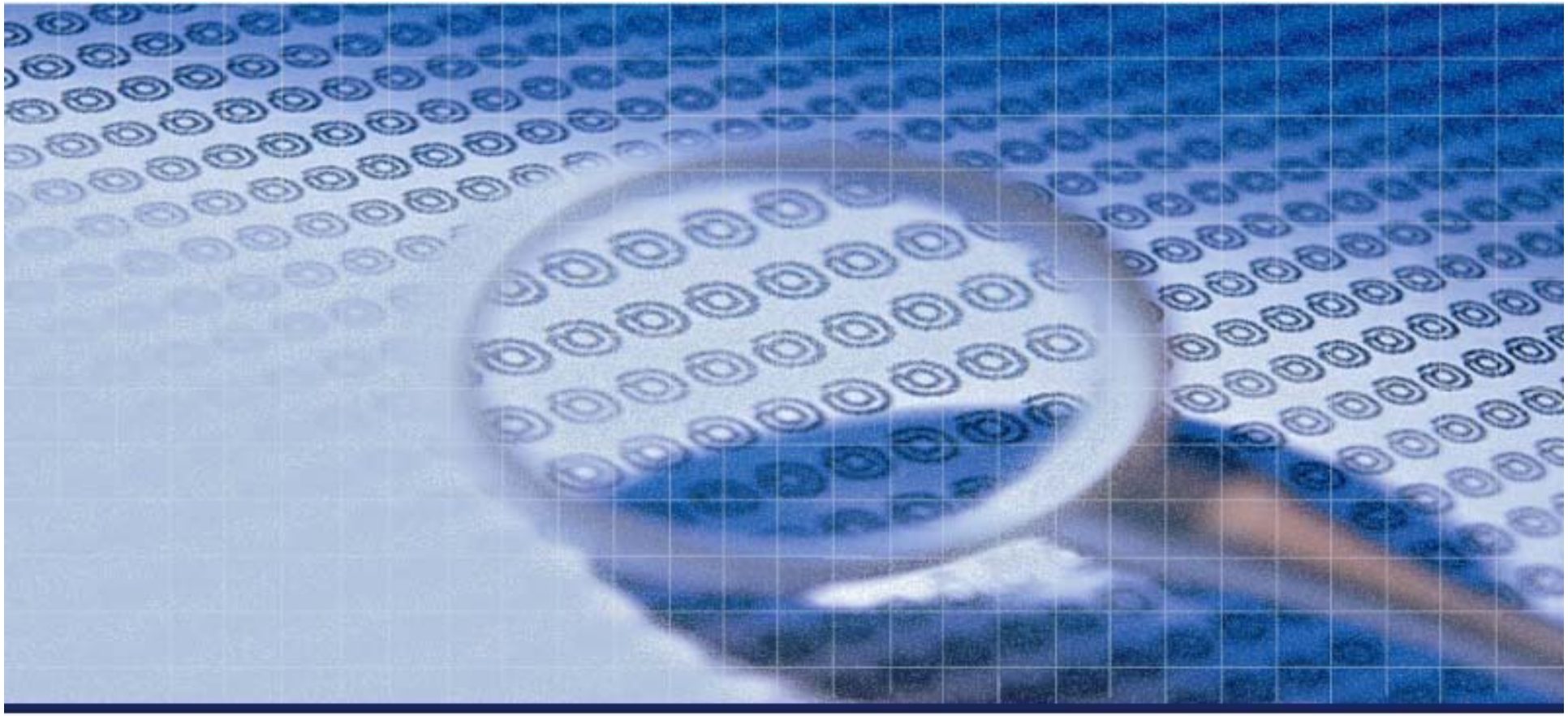
敦陽科技資安顧問　楊伯瀚

講師

- 楊伯瀚 (*lucifer.yang@sti.com.tw*)
- 現任: 敦陽科技IT管理技術開發處資安顧問
- 專長
  - 滲透測試
  - 網頁應用程式安全
  - 系統入侵事件分析
  - 資安事件處理
- 資安認證
  - CISSP (Certified Information Systems Security Professional)
  - CEH (Certified Ethical Hacker) /CEI (Instructor)
  - CHFI(Computer Hacking Forensic Investigation)
  - Cert/CC Advanced Incident Handling 講師

大綱

- 事故現場作業程序
- 本機網路分析
- 系統活動分析
- 檔案分析
  - 動態程式查找
  - 一般的查找方式
  - 一般的查找工具
  - 靜態木馬檢查
  - 木馬防查殺的目標
  - 進階的躲藏方式
- 其他資安系統記錄
- 植入原因推測
- 問題與流程討論



事故現場作業程序

異常現象回報

- 監控通報
  - 發現不允許的特定連線
  - 發現內部主機在進行掃瞄
  - 資料庫稽核記錄異常
  - 主機或網路無法正常提供服務
- 使用者感覺
  - 螢幕上出現不正常自動操作
  - 網路變慢，開機久且會跳錯誤訊息
- 第三方回報
  - 資料外洩
  - 網站被置換或植入程式
  - 犯罪調查
- 較難感覺到
  - ARP木馬

緊急應變的事故成因

- 惡意攻擊
  - 漏洞入侵(網站伺服器、AP主機)
  - 資料非經授權竊取(資料庫伺服器、AD主機)
  - DoS或DDoS
- 後門、木馬或病毒
  - 人為點擊(電子郵件、網頁瀏覽、偽裝盜版程式/破解軟體社交攻擊)
  - 自動散佈(網芳擴張)
  - 資料遭竄改或刪除
  - 盜竊或勒贖(Ransomware、Sniffer)
- 其他單位通知跳板(Command-and-Control)

事故影響等級

- 不重要的系統中斷
- 重要系統受影響且造成服務品質降低
- 重要系統無法運作
- 影響範圍大或短期間發生頻繁的事故
- C&C或犯罪調查

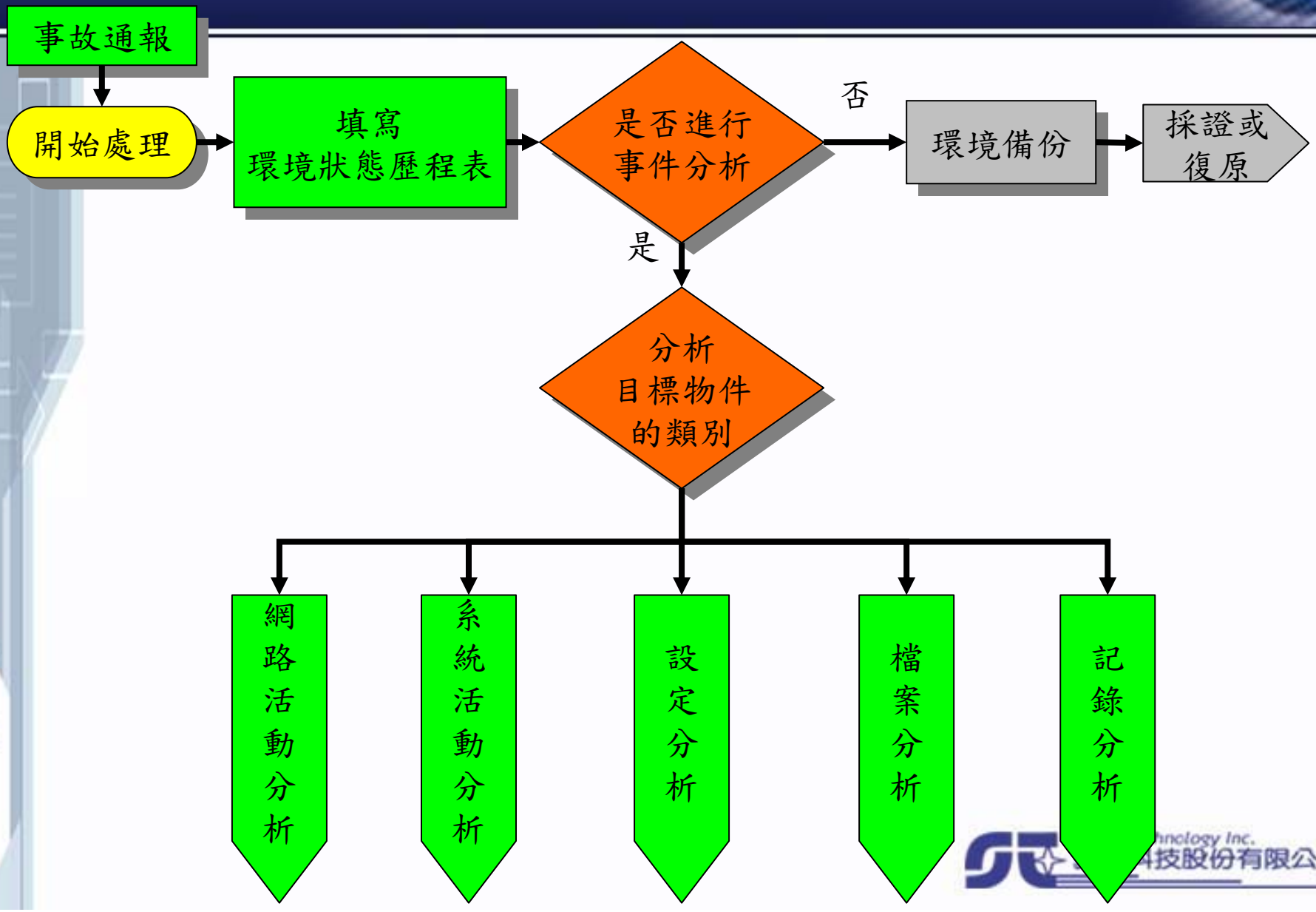
決定採取步驟

- 依事故成因與影響等級判斷
- 事故回復：先回復運作為主
  - 決定是否備份事故環境
  - 將系統回復至前次正常狀態，完全破壞事證
- 事故排除：無法直接還原，須線上排除
  - 決定是否備份事故環境
  - 調查事故發生細節
  - 消滅事故成因，確認系統正常運作，可能破壞事證
- 事故存證：未來具法庭需求，或電腦犯罪等與惡意程式無關時（例如查密帳）
  - 依證據標準備份事故環境
  - 決定系統重新上線時間
  - 使用備份環境的備份調查事故發生細節
  - 媒體控制
  - 法庭程序

從哪裏下手？

- 使用者以及管理者
  - 第一手觀察資料
- 系統
  - 系統活動記錄
  - 系統環境
  - 系統檔案，包含入侵殘留物(程序,檔案)
  - 資安系統記錄與備份媒體
- 網路/通訊
  - 網路封包側錄記錄
  - 其他資安系統記錄

作業流程概觀


事故通報
開始處理
填寫
環境狀態歷程表
是否進行
事件分析
否
環境備份
採證或
復原
是
分析
目標物件
的類別
網路活動分析
系統活動分析
設定分析
檔案分析
記錄分析

作業流程概觀

環境狀態歷程表

時間	目標物件	位置	關係人	處理員	描述

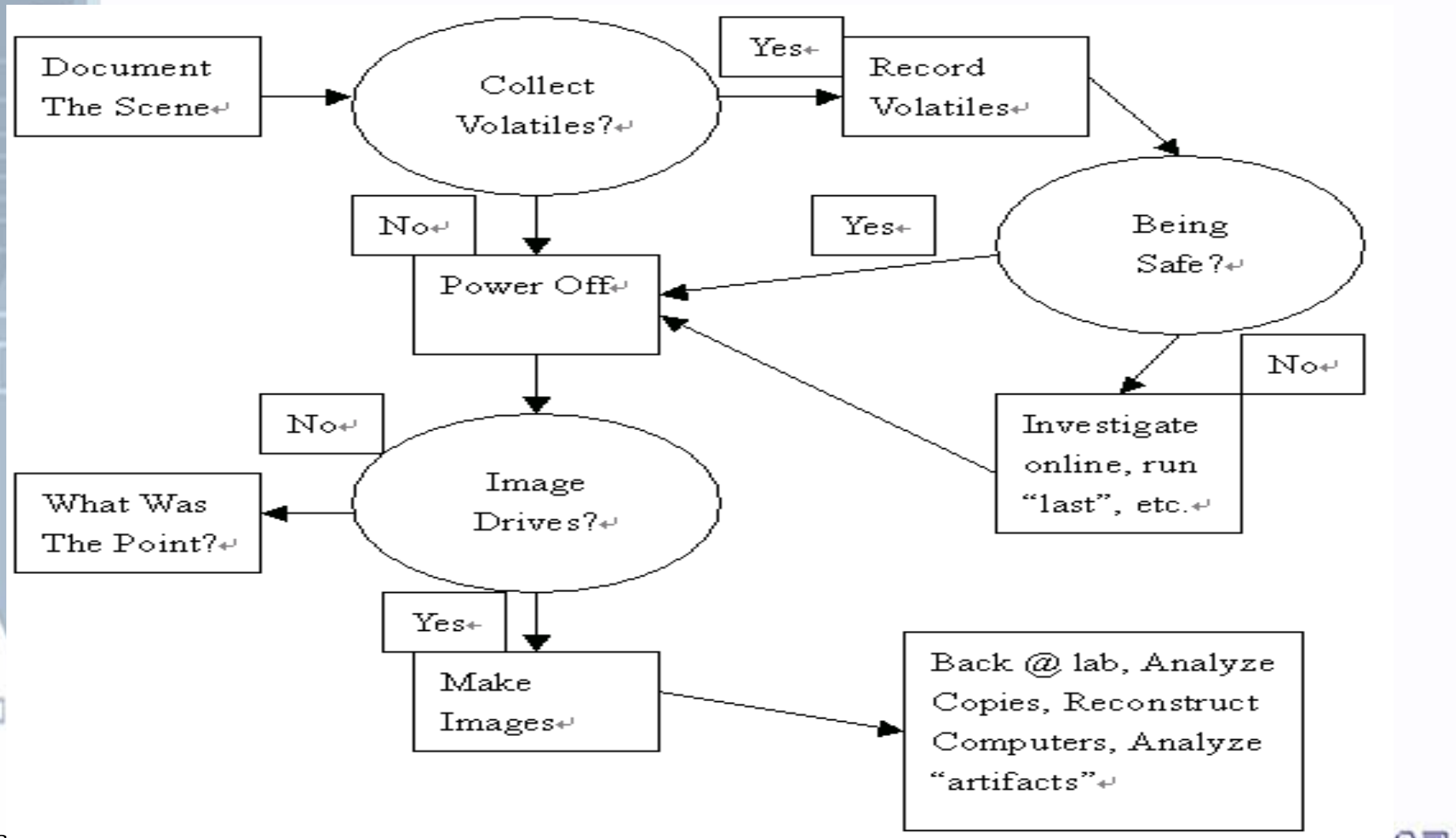
注意*：記得要先對時

注意***： 各種資料來源的時區與時間格式都不同

數位證據

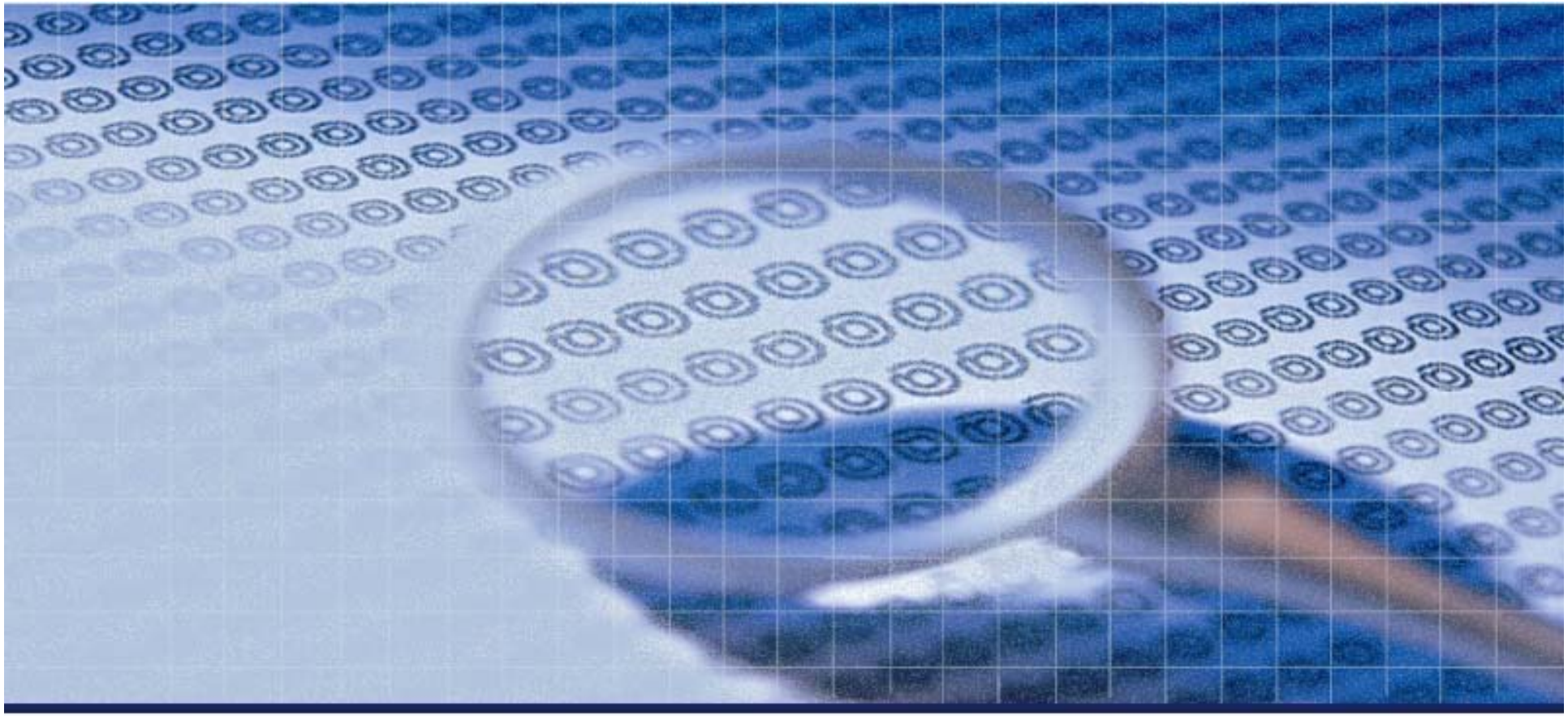
- 利用特定技術，將事發現場所蒐集的各種資料加以分析並找出可以被法庭(律)採納的證據。
- CSIRT專門負責調查和處理數位證據，其主要工作包括：
  - 蒐集證據 (Collect)
  - 檢驗和分析證據 (Identify and Analyze)
  - 保存證據 (Preserve)

國際上鑑識流程範例


Document The Scene
Collect Volatiles?
Yes
Record Volatiles
No
Power Off
Yes
Being Safe?
No
Investigate online, run "last", etc.
No
What Was The Point?
Image Drives?
Yes
Make Images
Back @ lab, Analyze Copies, Reconstruct Computers, Analyze "artifacts"

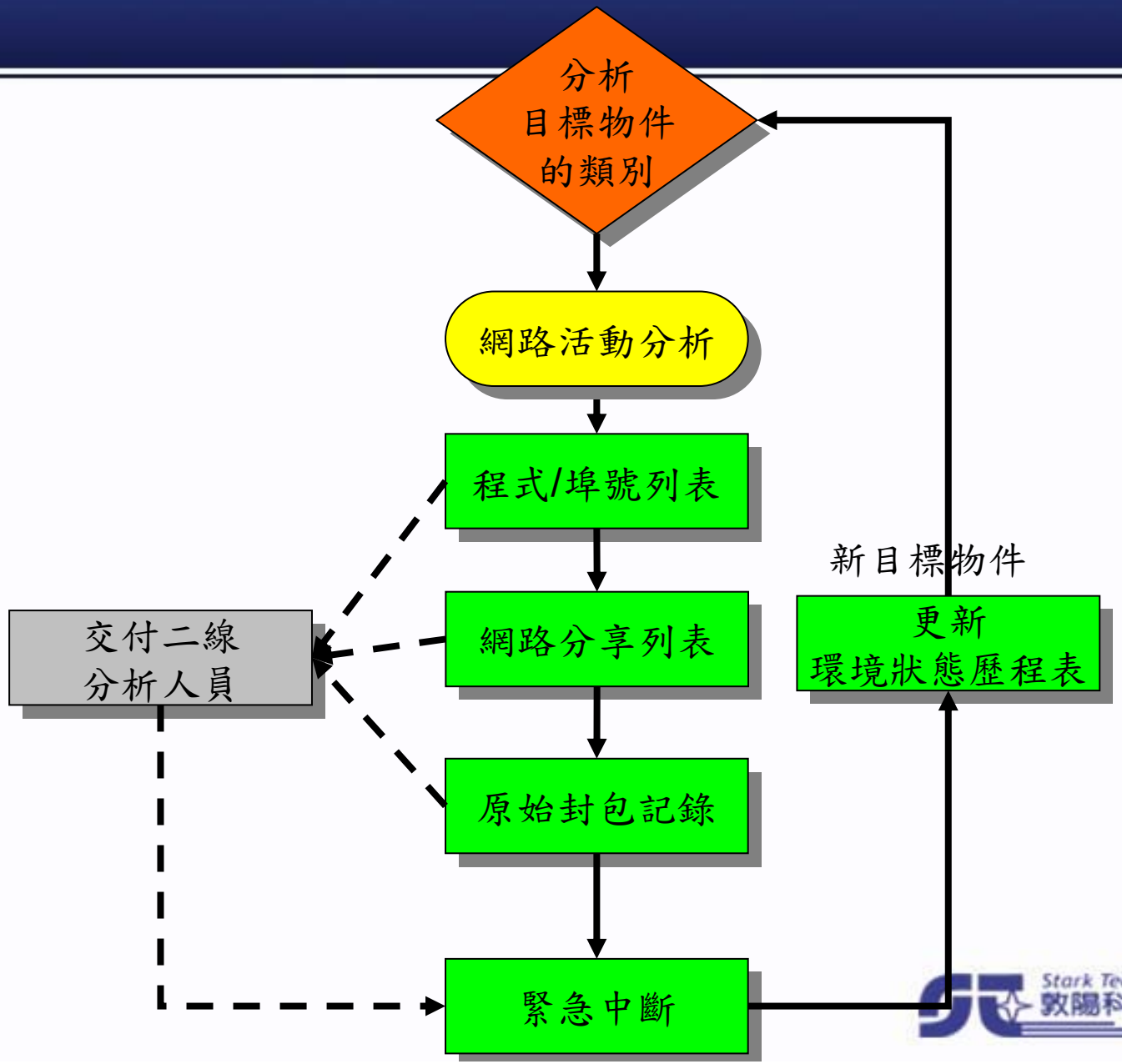
數位鑑識調查參考資料

- 計畫名稱:數位鑑識標準作業程序之實務及方法研究 -賴溪松教授
- 參考資料來源
  - http://ir.lib.ksu.edu.tw/bitstream/987654321/3486/1/%E6%95%B8%E4%BD%8D%E9%91%91%E8%AD%98%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E7%A8%8B%E5%BA%8F%E4%B9%8B%E5%AF%A6%E5%8B%99%E5%8F%8A%E6%96%B9%E6%B3%95%E7%A0%94%E7%A9%B6+%E6%9C%9F%E6%9C%AB%E5%A0%B1%E5%91%8A.ppt



網路活動分析

流程

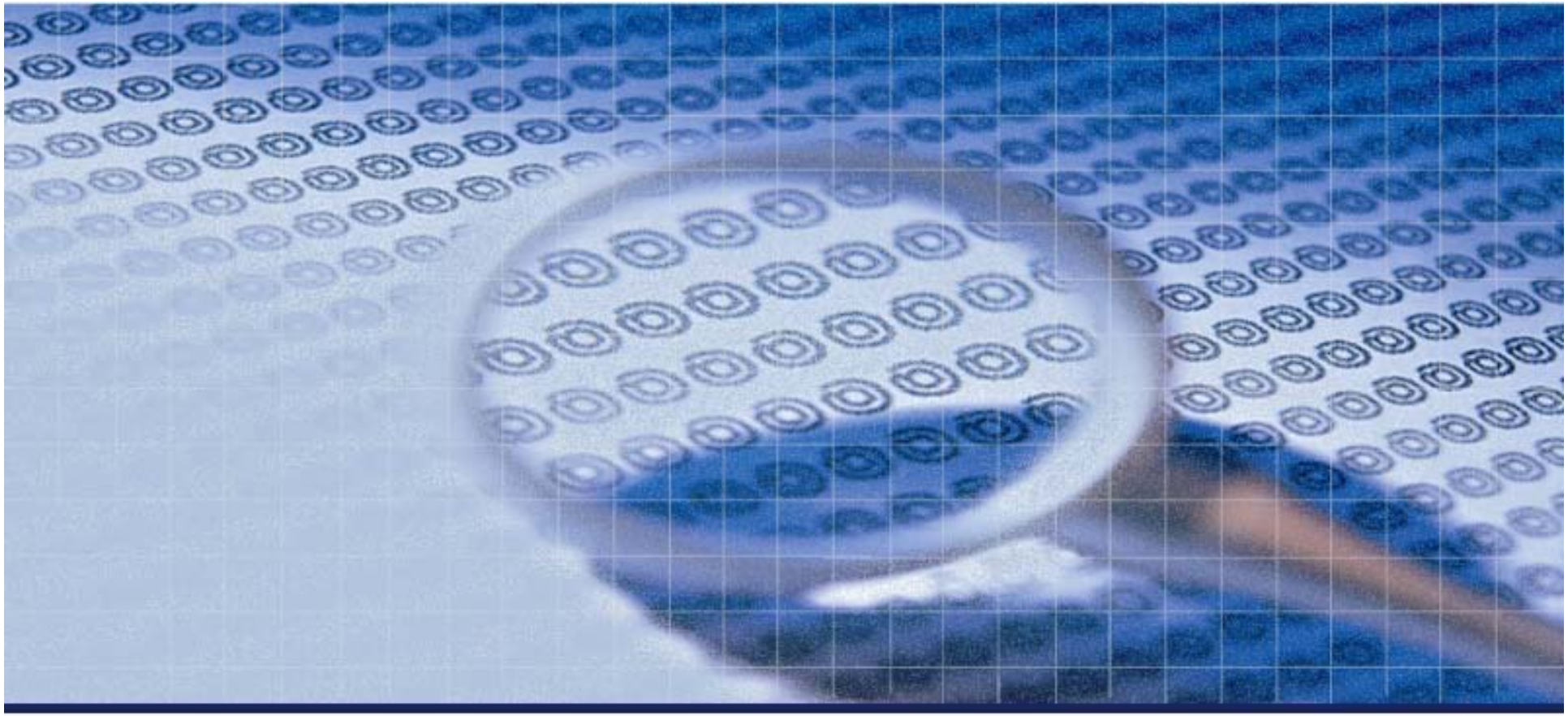


封包分析

- 相關網路設備記錄
  - 封包側錄儀(最好由旁路側錄)
  - 防火牆(L7較佳，能夠記錄Application)
  - IPS
  - WAF
- 適用於事件還在發生中，對於舊有事故通常沒有存下完整記錄，難以追查
- 運氣好可透過封包分析完整記錄到攻擊、感染、遠遙過程，以及得知攻擊者身份
- Network Discover
  - 類似安全稽核，不建議由網路發起主動探尋

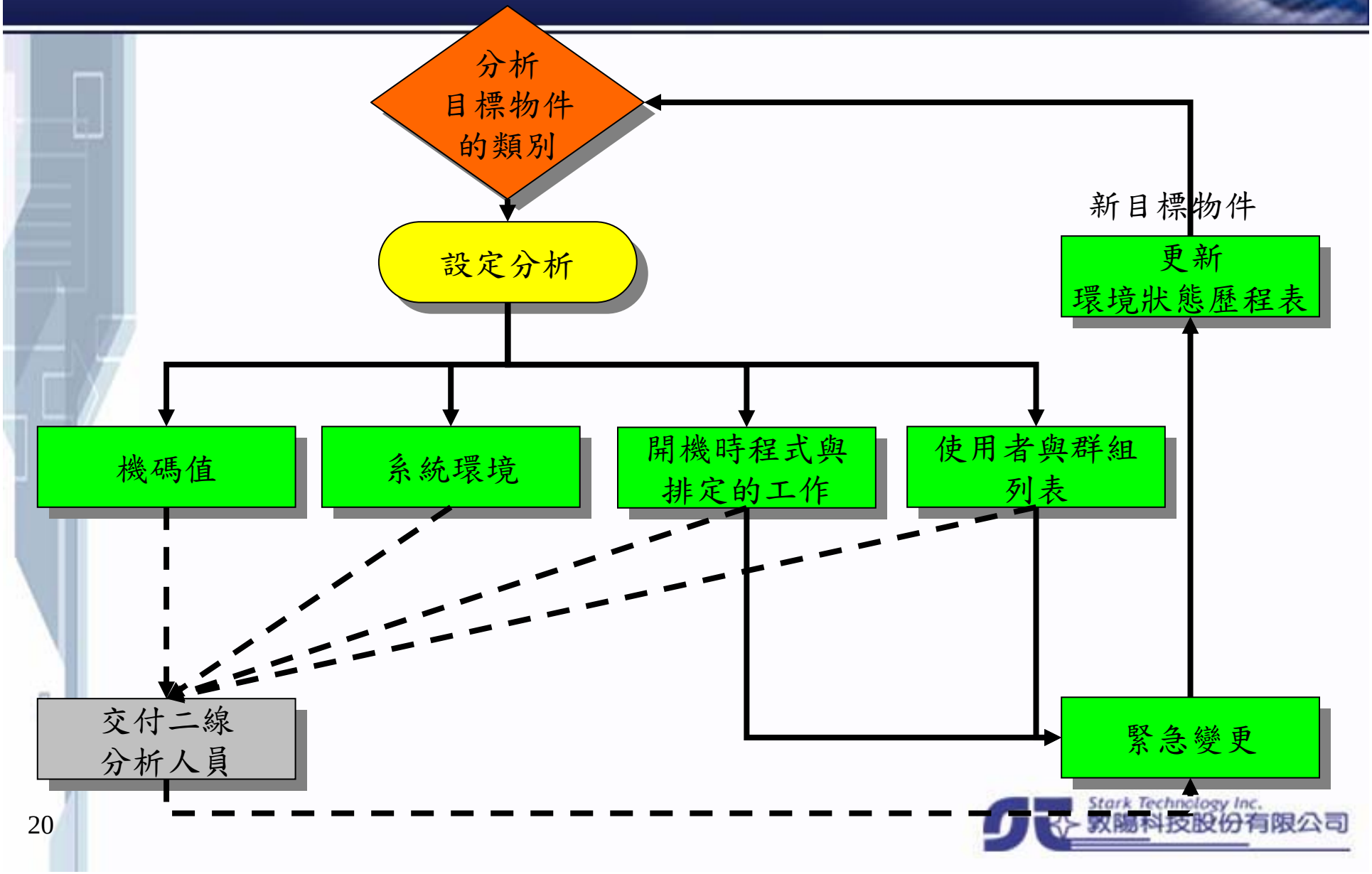
Sniffer分析目標

- HTTP Attack
- SSL Attack
- FTP from Intranet
- SMTP from Intranet
- SQL Query
- Non-http traffic on 80/443 port



系統活動分析

系統資訊收集



Event Log

- Evt(Windows XP/2003)、Evtx(Windows 7/2008
  - Application
  - Security
  - System
- 建議事先開啟檔案稽核
- 修改安全性原則

Event Log 常見蒐查目標

- 調整時間值(Security Event ID 520) 超過1天
- 讀寫 C$, D$, E$..的事件 (Security Event ID 5140)
- 程式執行失敗，例如安裝核心驅動程式失敗(System Event ID 7045)
- 登入遠端RDP失敗(System Event ID 10006)
- 指定的目錄被寫入檔案

遠端讀寫檔案

Examples of 5140

```
A network share object was accessed.

Subject:

   Security ID:  ACME-FR\Administrator
   Account Name:  Administrator
   Account Domain:  ACME-FR
   Logon ID:  0x74a739

Network Information:

   Source Address:  10.42.42.221
   Source Port:  65097

Share Name:   \\*\Dharma Initiative Protocols
```

- Event ID 5140
  - 列出所有 讀寫 C$, D$, E$..的事件，串查登入主機當時的所有登入者

登入桌面

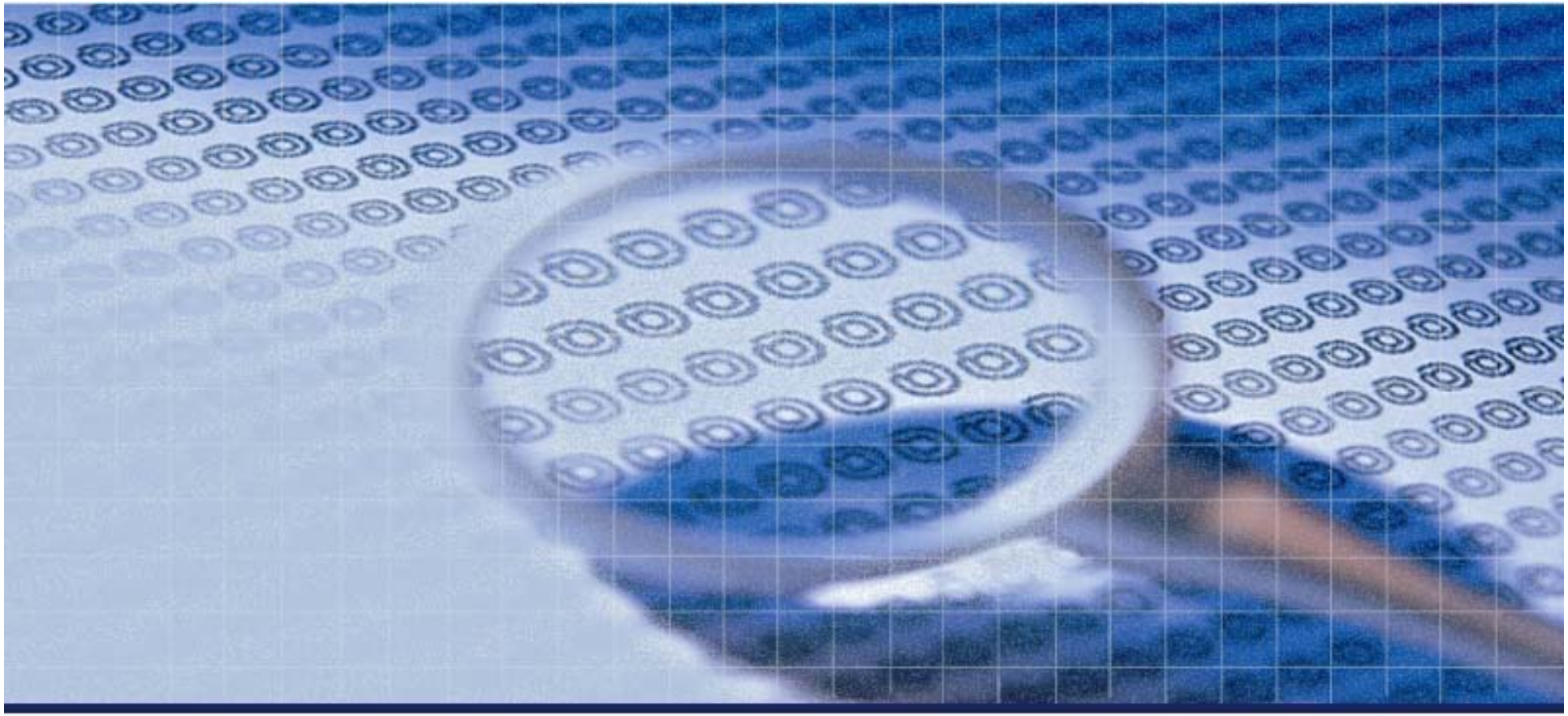
- 列出遠端登入桌面的來源和使用帳號
  - Application event ID : 4001

    登入事件，但正常事件可能很多，難以區分
- 相關事件
  - Application event ID :9003

    DWM(Desktop Window Manager)啟動失敗，代表有登入桌面
  - Application event ID :9009

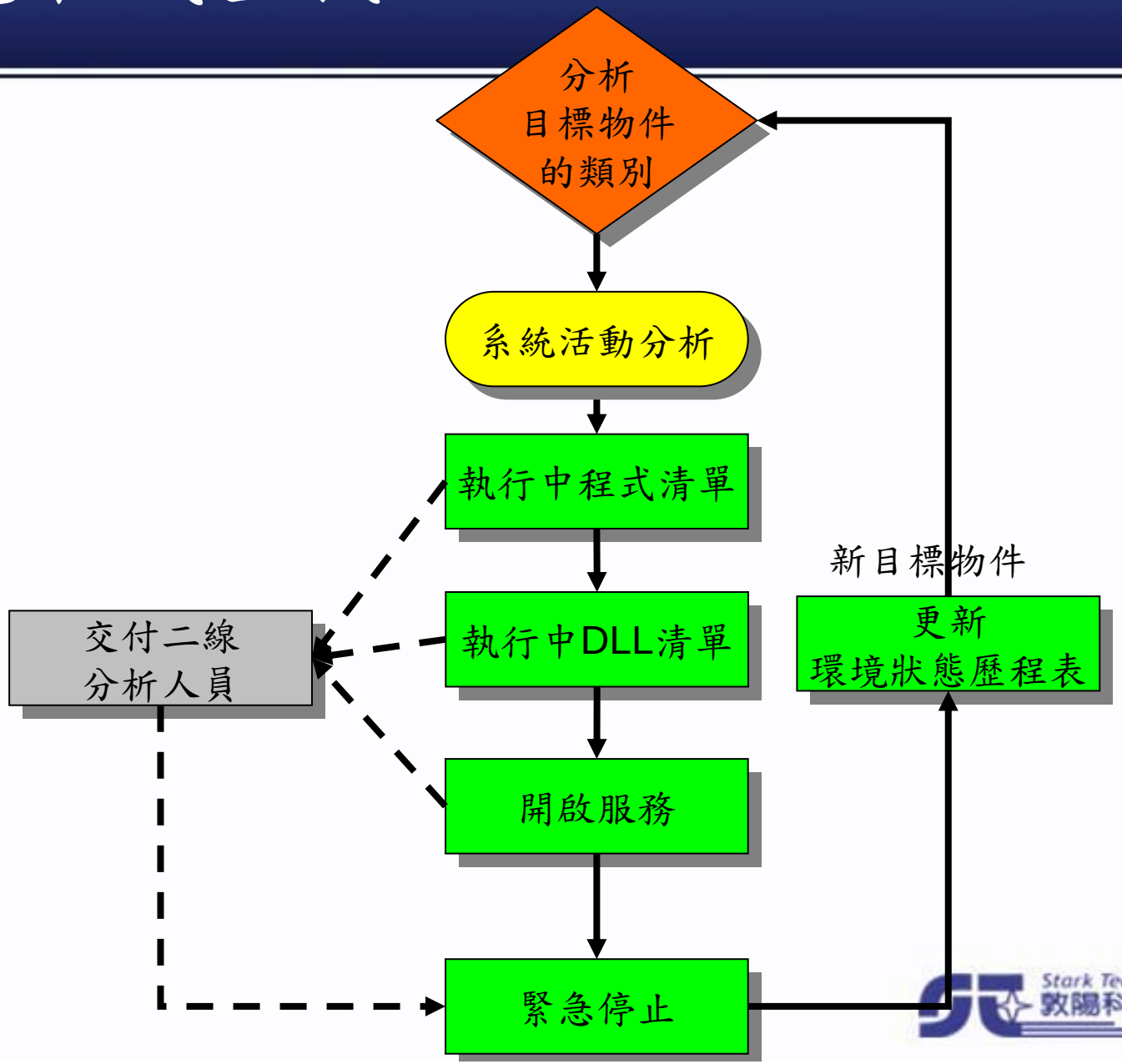
    DWM結束
  - System event ID:7001

    客戶經驗改進通知，代表有登入桌面



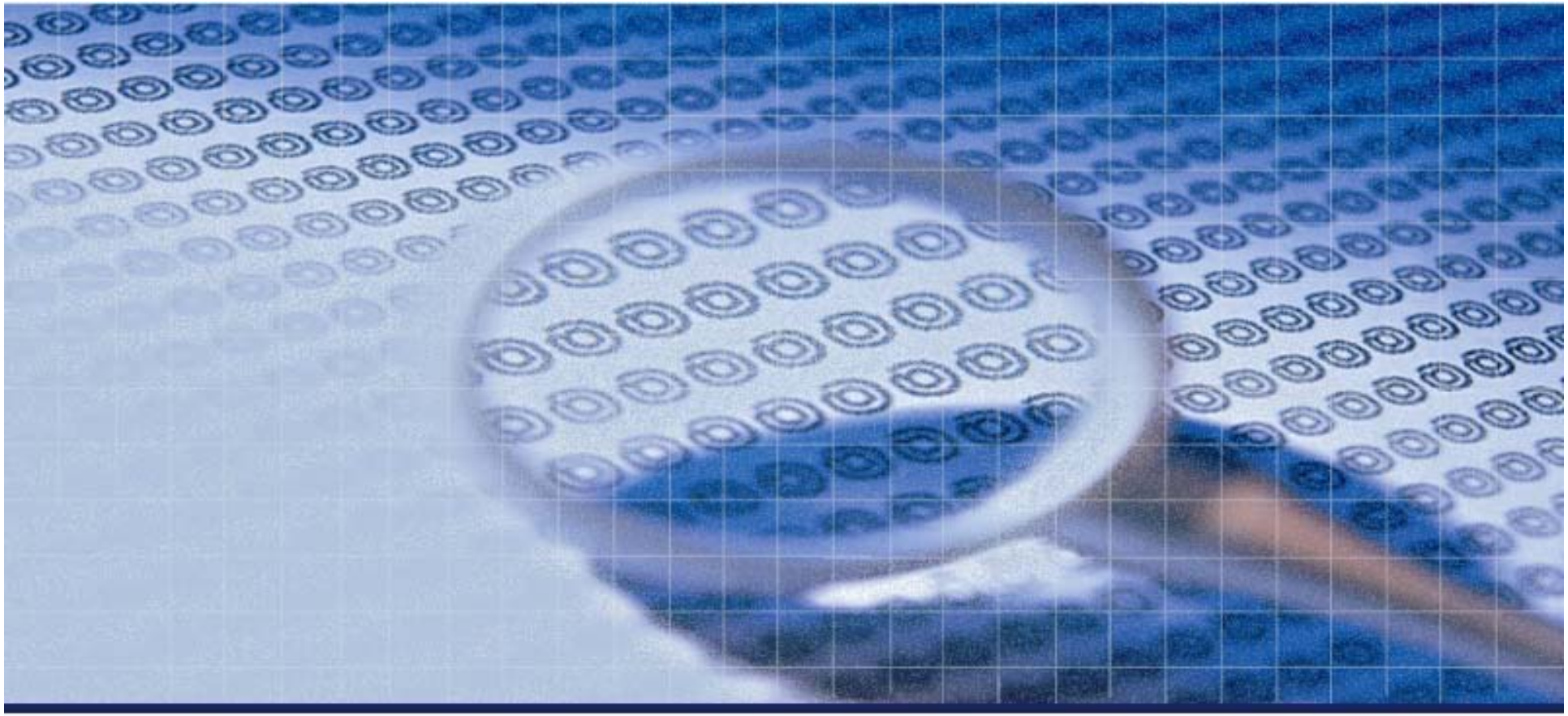
檔案分析—動態程式查找

動態程式查找



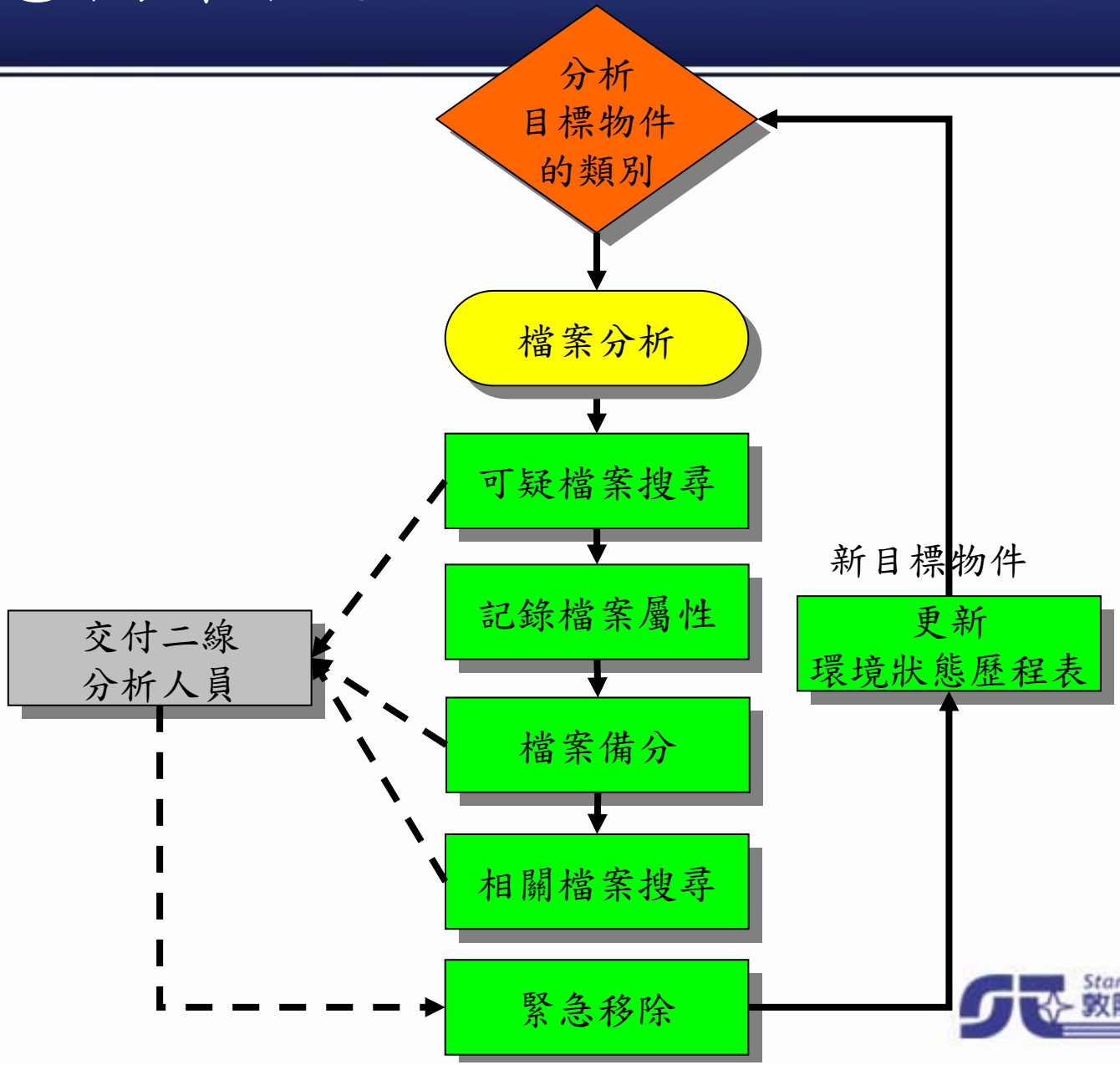
一般查找的可疑目標

- 檔案與服務的名稱
- 檔案與服務的版本與描述
- 檔案時間
- 網路埠
- 執行中程式與狀態列表
- 執行中DLL與狀態列表
- 已開啟服務狀態列表



檔案分析—靜態檔案檢查

靜態檔案檢查

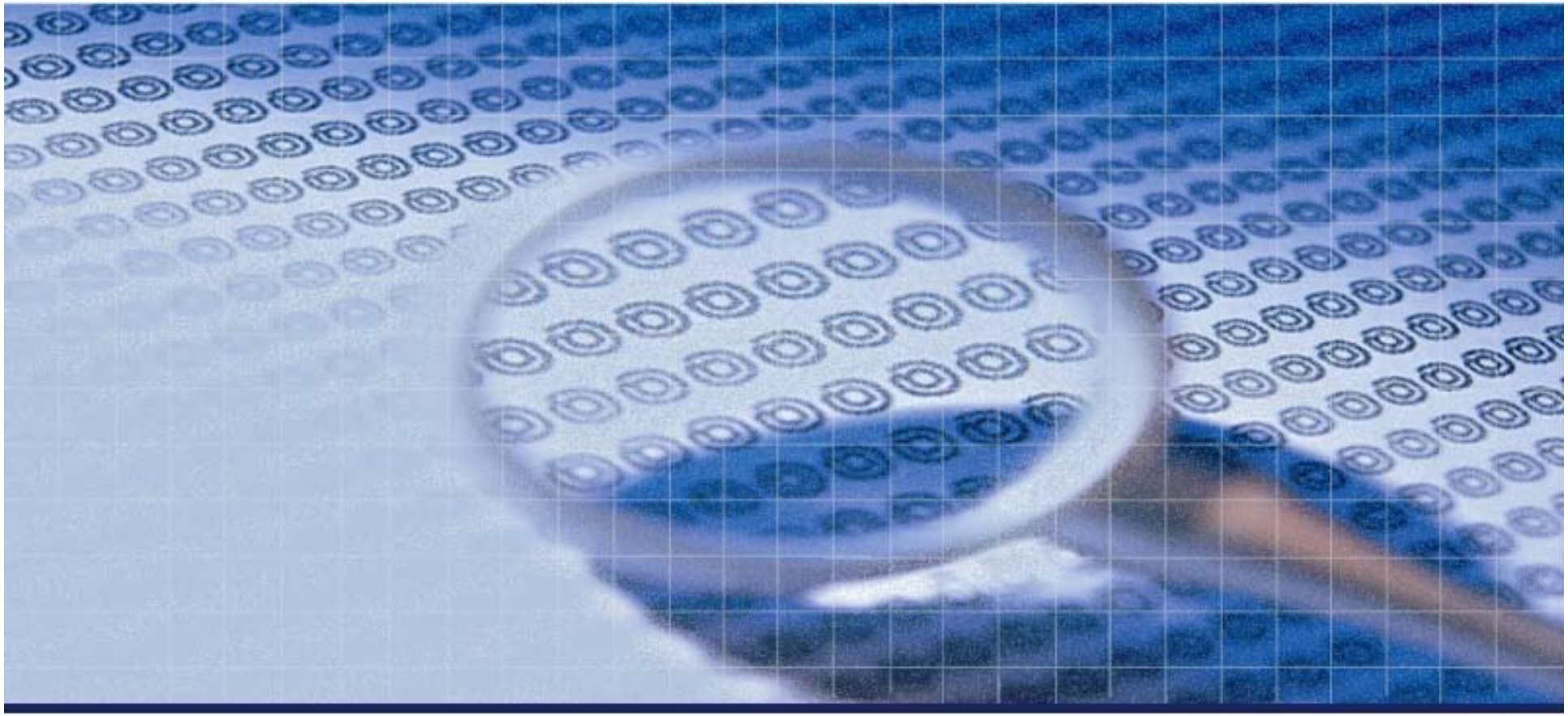


靜態尋找

- 尋找可疑檔案
- 在不執行惡意程式的情況下進行分析
- 對非二進位格式檔案可直接檢視
- 對二進位格式檔案進行先期處理
- 分析工具利用光碟執行
- 分析工具以非安裝檔為主

PE格式

- PE(Portable Executable)可移植式執行檔：可在所有 Microsoft 32 位元作業系統中執行的檔案，相同的 PE 格式檔案可在任何版本的 Windows 95、98、Me、NT 與 2000 上執行。
- 標頭為4D 5A(MZ)。
- 常用附檔名：exe、dll，但可使用.gif等其他檔名偽裝。



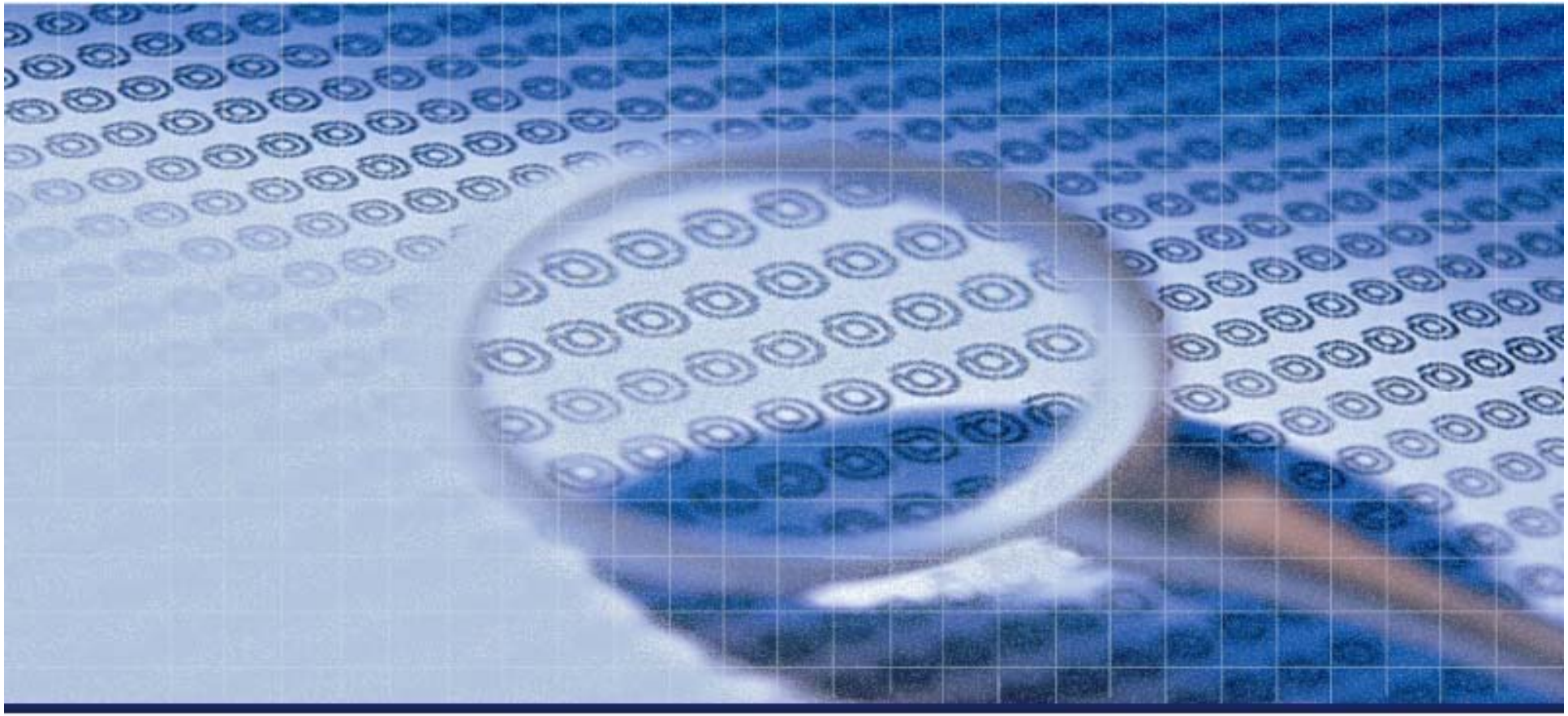
惡意程式防查殺

基本的檔案躲藏方式

- 檔名偽裝，例如exp1orer.exe
- 目錄偽裝，例如 %SystemRoot%\system32\explorer.exe
- 屬性+S +H隱藏
- 執行時刪除自身
- 系統還原
- 取代現有檔案，例如dll掛馬

進階的躲藏方式

- LNK捷徑檔
- 驅動程式
- System Volume Information
- .結尾目錄
- -結尾檔案
- 副檔名開啟
- 不可見字元副檔名
- SupperHidden
- ADS串流
- 反向檔名
- com1保留字
- 資源回收筒
- IFEO劫持
- debug執行
- PATH路徑



應用程式與資安系統記錄

檢視設備記錄

- 伺服器端
  - 長期Sniffer記錄
  - 網站伺服器記錄
  - 資料庫伺服器記錄
  - 事件檢視器記錄
  - 事件稽核記錄
- 個人電腦端
  - 郵件記錄
  - 瀏覽器記錄
  - 惡意程式殘留物，設定檔等

不道德追查

- 攻擊跳板機
- 公用帳號密碼猜解(例如:gmail.com)
- 社交工程(Mail, QQ)