弱點管理

弱點管理方法：

- 資安健診 (Information Security Diagnostic)
    - 說明：由第三方顧問廠商每年定期進行全面的安全檢查，屬於預防性資安措施，找出潛在的安全弱點。
    - 檢視項目：
        - 網路架構檢視、網路惡意活動檢視。
        - 使用者端電腦與伺服器主機的惡意活動檢視。
        - 目錄伺服器設定檢視、防火牆連線設定檢視。
        - 政府組態基準(GCB)檢視、資料庫安全檢視。
- SOC服務 (Security Operation Center)
    - 說明：由外部或內部建立 SOC 團隊，透過集中式監控與管理系統日誌來主動偵測與處理安全事件。SOC團隊通常由資安分析師、事件處理人員、威脅情報人員等角色所組成。
    - 問題單工作流程：查看可疑系統日誌 → 建立事件通報單 → 分派至相關經辦人處理並追蹤到解決。
      相關標準：NIST SP 800-61《電腦安全事件處理指南》，提供事件回應的流程與最佳實務。
    - 常用工具
        - 安全資訊與事件管理(SIEM)
            - ➢ 用途： 集中蒐集系統日誌、網路活動，進行事件關聯分析、告警及報告。
            - ➢ 常用軟體： OSSIM、ArcSight、Splunk。
        - 端點偵測與回應(EDR)
            - ➢ 用途：安裝於終端設備，偵測惡意軟體、未授權存取、異常行為，進行事件調查、隔離或封鎖威脅。

            - ➢ 常用軟體：CrowdStrike、SentinelOne。
        - 威脅情報平台(TIP)
            - ➢ 用途： 提供最新威脅情報、威脅指標 (Indicators of Compromise, IoCs)，協助分析師快速比對、識別威脅來源及性質。
            - ➢ 常用軟體：MISP、Recorded Future。
        - 安全自動化與協調回應(SOAR)
            - ➢ 用途： 自動化事件處理流程（如隔離主機、封鎖IP），降低分析人員負擔、提升回應速度與效率。
            - ➢ 常用軟體：Splunk Phantom、Cortex XSOAR。
    - 應用：
        - 快速偵測並應對異常行為 (如未授權存取、惡意流量等) 。
        - 強化事件回溯分析能力。
- 原始碼掃描(Source Code Analysis)
    - 說明：對應用程式的原始碼進行安全掃描，找出潛在漏洞 (如未檢查的輸入、寫在程式中的密碼等) 。
    - 執行方式：
        - 通常由內部自行使用工具掃描。
        - 遇到無法修補的漏洞，會詢問廠商顧問協助。
    - 特性：
        - 適用階段：程式開發過程中即可進行，無須等到系統上線後執行。
        - 支持多語言：大多數原始碼掃描工具支持多種程式語言的混合分析 (如 Java、Python、C++ 等) 。
        - 優勢：能早期發現程式漏洞，降低修復成本。

        - 限制：無法全面檢測邏輯瑕疵、業務漏洞或駭客刻意植入的惡意程式碼。
    - 常見軟體：SonarQube、Checkmarx、Fortify。
- 弱點掃描 (Vulnerability Assessment)
    - 說明：利用掃描工具檢查主機、系統或應用程式的已知漏洞。快速找出已知漏洞，但無法模擬實際攻擊行為。
    - 執行方式：可自行安裝軟體掃描，或交由第三方廠商協助。
    - 類型：
        - 主機系統弱點掃描：檢查伺服器和工作站的系統漏洞。
            - ➢ 常見軟體：Nessus、OpenVAS、Nexpose。
        - 網頁應用程式弱點掃描：檢查網站與 API 的潛在安全問題。
            - ➢ 常見軟體：Burp Suite、OWASP ZAP。
    - 相關標準：
        - 重點整理：
            - ➢ CWE 定義軟體開發中的常見弱點類型。
            - ➢ CVE 具體標識已發生的漏洞。
            - ➢ CVSS 為漏洞的嚴重程度打分。
            - ➢ NVD 是詳述漏洞資訊與修補建議的資料庫。
            - ➢ CPE 指出漏洞可能影響的軟硬體平台。
            - ➢ KEV 標示已知被攻擊者實際利用的漏洞清單，強調修補優先順序。
        - CVE(Common Vulnerabilities and Exposures)：
            - ➢ 全球統一漏洞編號系統，用於識別和追蹤已知漏洞。
            - ➢ 範例：CVE-2017-0144，永恆之藍 (EternalBlue) 漏洞，利用 SMBv1 通訊協議的遠端代碼執行 (RCE) 漏洞，曾被用於 WannaCry 勒索病毒攻擊。

- CWE (Common Weakness Enumeration)：
  - ➢ 公開的弱點分類系統，用於識別和標註軟體開發過程中的常見弱點。
  - ➢ 範例：CWE-119 - 特定語言容許直接取得記憶體區域 (Improper Restriction of Operations within the Bounds of a Memory Buffer)，永恆之藍的核心弱點。
- CVSS(Common Vulnerability Scoring System)：
  - ➢ 漏洞評分標準，量化漏洞的嚴重程度 (範圍 0 – 10)。
  - ➢ 範例：CVSS v3.1 總分 8.5 (高危漏洞)，攻擊難度低，無需用戶交互，可遠端觸發。
- NVD(National Vulnerability Database)：
  - ➢ 美國國家漏洞資料庫，基於 CVE 提供漏洞詳細資訊與 CVSS 評分。
  - ➢ NVD 詳細描述 CVE-2017-0144 的攻擊場景，影響的系統包括 Windows 7、Windows Server 2008，並建議用戶安裝相關安全更新 (MS17-010) 以修補漏洞。
- CPE (Common Platform Enumeration)：
  - ➢ 通用平台枚舉，用於標識漏洞影響的特定軟體或硬體版本。
  - ➢ 範例：CPE 編碼範例 - "cpe:2.3:o:microsoft:windows_7"，代表 CVE-2017-0144 對 Windows 7 作業系統的影響。
- KEV (Known Exploited Vulnerabilities Catalog)：
  - ➢ 由 CISA 維護的「已知被利用漏洞清單」，收錄已被攻擊者利用的漏洞，幫助組織優先處理高風險項目。根據 CISA/NIST 統計，所有 CVE 中實際

被利用的比例不到 1%，因此 KEV 能幫助快速聚焦真正的重點。

➢ 範例：CVE-2017-0144 也收錄於 KEV，因為該漏洞被廣泛利用於 WannaCry、NotPetya 攻擊，KEV 同時會標註修補期限與建議措施。

- 滲透測試 (Penetration Test)
  - 說明：模擬攻擊者行為，利用弱點的串聯找出進入系統的路徑。
  - 特性：
    - 具破壞性，可能導致服務中斷或資料損毀。
    - 測試前後需詳盡溝通，以免造成誤解或事故，需要明確界定測試範圍與時間，並簽署賠償條款。
  - 類型：
    - 一般性滲透測試：針對單一目標或範圍 (如網站、伺服器) 。
    - 紅隊演練
      - ➢ 說明：檢測整體系統的防禦能力，模擬真實攻擊場景。角色定義為紅隊：模擬攻擊者進行滲透。藍隊：負責防禦，應對紅隊攻擊。紫隊：中立第三方，協助紅藍隊溝通與協作。
  - 白箱 vs 黑箱 vs 灰箱 vs 雙黑箱演練
    - 白箱演練
      - ➢ 測試者了解內部系統結構與資訊 (如程式碼、網路配置)。
      - ➢ 應用場景：內部安全測試，檢測內部邏輯與權限管理弱點。
    - 灰箱演練

        - ➢ 測試者擁有部分關於目標系統的內部資訊，例如架構圖、API 文件、部分程式碼片段或有限權限的帳戶。
        - ➢ 應用場景：更貼近現實的滲透測試，針對特定系統或功能的安全性評估、資安事件應變演練，通常最能有效率地發現潛在漏洞並模擬真實攻擊。
    - 黑箱演練
        - ➢ 測試方式：測試者對系統完全不了解，僅基於外部公開資訊 (如域名、IP) 進行攻擊。
        - ➢ 應用場景：外部滲透測試，模擬外部攻擊者的真實行為。
    - 雙黑箱
        - ➢ 攻防雙方在測試過程中都不知道對方的具體情況。
        - ➢ 應用場景：模擬真實的攻擊和防禦場景，測試藍隊的響應能力與檢測能力。
  - 常見指令：Nmap、CURL、SQLmap、Netcat、John the Ripper、HashCat、Aircrack-ng、Hydra。
  - 常見軟體：Wireshark、Metasploit、Burp Suite、OWASP ZAP、Mimikatz、Nikto。
- 社交工程演練
  - 說明：模擬社交工程攻擊來測試人員的安全意識。通常由第三方顧問廠商每年定期辦理。提升員工的安全意識，減少因人為疏忽造成的安全事故，故通常搭配教育訓練，以強化員工的資安意識。
  - 測試項目：
    - 最常見是釣魚郵件和簡訊演練，但不限於電話或真人實體測試。

        - 統計測試成功和失敗的比例，查看員工的整理資安意識。
    - 後續措施：
        - 被發現弱點的員工需參加教育訓練。
        - 定期測試提高組織防範社交工程的能力。
- 軟體組成分析 (Software Composition Analysis)
    - 說明：來掃描軟體中引用的第三方元件（尤其是開源套件），並分析其版本、安全漏洞、授權合規性及潛在風險。現今軟體開發很少從零開始，大多是引用第三方套件，而套件若有弱點便會一併繼承到自己的軟體中。
    - 舉例：Apache Log4j 安全漏洞 (CVE-2021-44228) 爆發時，公司若有上百套系統，要如何在第一時間掌握哪些系統引用了該版本並存在漏洞？因此必須透過軟體材料表 (Software Bill of Materials, SBOM)，它是一份結構化清單，詳細列出軟體中所有組件名稱、版本、依賴關係（包含直接依賴與間接依賴）、供應鏈來源等資訊，可視為「軟體成分說明書」。
        - 步驟 1：使用 SCA 工具掃描原始碼或二進位檔，生成 SBOM（列出所有組件與依賴層級）。
        - 步驟 2：SCA 工具進一步分析 SBOM 中的組件，標示出是否存在 **安全漏洞 (CVE/NVD)**、**版本狀態**（是否已落後於最新穩定版，或存在已知修補卻未更新的情況，注意最新版不一定代表安全）、**維護狀態**（套件是否仍有持續更新，若專案已停更則長期風險極高），或 **授權風險** 的項目：
            - ➢ Apache / MIT → 相對寬鬆，可自由商用，只需保留聲明

        - ➢ LGPL → 可商用，但若修改需開源相關部分；特別是 **靜態連結/整合原始碼** 時，限制較多，若僅使用 **DLL/動態連結** 則較寬鬆
        - ➢ GPL / AGPL → 限制最嚴，可能要求公開整個程式碼
    - 步驟 3：開發人員根據 SCA 的報告進行組件更新或修補，SBOM 則自動同步至最新版本與風險狀態。
- 外部攻擊面管理 (External Attack Surface Management, EASM)
    - 說明：從攻擊者角度持續發現、監控與控管對外暴露的資產，補足弱點掃描、滲透測試、SCA 僅能針對「已知資產」檢測的不足，特別用來解決影子 IT 與遺忘資產風險，屬於非侵入式的外部資產曝險評估，常用於供應鏈管理。
    - 流程：
        - 資產盤點 (Discovery)：網域、子網域、IP、API。
        - 風險分析 (Assessment)：憑證、協定、CVE 漏洞。
        - 持續監控 (Monitoring)：新資產、假冒網站、異常變動。
        - 修復回應 (Remediation)：關閉服務、更新憑證、修補漏洞。
    - 檢測風險類別：電子郵件安全、憑證安全、SSL/TLS 安全、IP/域名聲譽、DNS 安全與健康狀態、網路通訊安全、網頁應用程式安全、漏洞修補、錯誤配置、暗網洩漏。
    - 工具：商用平台（Microsoft Defender EASM、CyCognito）、本地產品（奧義科技 CyCraft XCockpit 平台）。

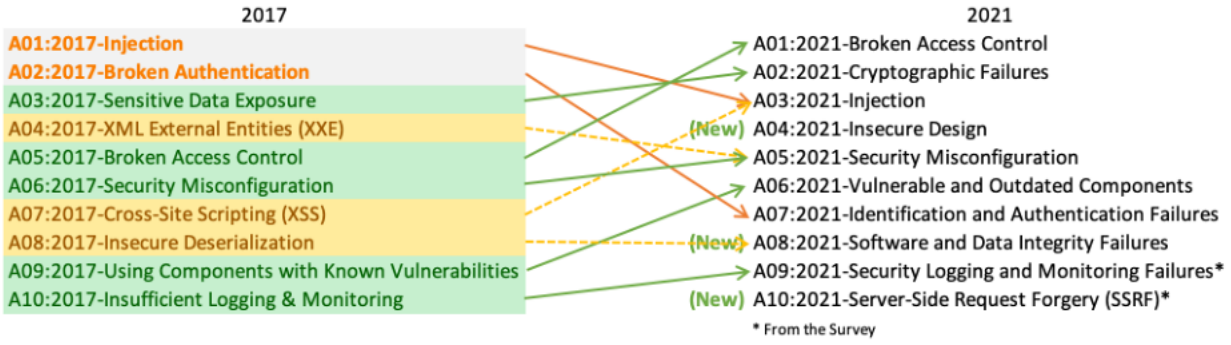
事件處理與調查方法

- 數位鑑識 (Digital Forensics)
    - 說明：透過系統化的蒐證與分析電子證據，還原資安事件發生過程，確認攻擊來源與影響範圍，作為法律程序或內部調查依據。
    - 執行方式：
        - 蒐集系統日誌、記憶體、網路封包等電子證據。
        - 分析證據以重建事件經過。
        - 提供正式報告供法律或管理決策使用。
    - 常用工具：
        - FTK Imager、Autopsy、Volatility、Wireshark。
    - 特性：
        - 需符合法律程序與證據保全原則，維持完整的證物證據鏈和監管鏈（Chain Of Custody），確保證據在法律程序上有效。
        - 因為需要專業的數位鑑識軟體和通過ISO / IEC 17025資安檢測實驗室，通常由具專業認證外部人員執行。

OWASP Top 10 常見十大漏洞：

- OWASP Top 10 心智圖：https://gitmind.com/app/docs/mr6cibxy
- 為網路應用程式漏洞的指南，每年統計最常見的十個WEB應用伺服器漏洞，目前最新版為2021年版。2021 與 2017 相比，新增「A04: 不安全設計」、「A08: 軟體及資料完整性失效」。
    - **A01:2021-權限控制失效**：直接在網址改 ID 從 /user/1 改成 /user/2 就能查到別人的資料。
    - **A02:2021-加密機制失效**：使用明文或簡單 MD5 儲存密碼。

- **A03:2021-注入式攻擊**：輸入 ‘admin' or ‘1’ =’ 1’ 繞過登入驗證繞過登入驗證。
- **A04:2021-不安全設計**：網站未限制登入次數，可以暴力破解密碼。
- **A05:2021-安全設定缺陷**：使用預設的管理者帳號密碼 admin/admin，或是錯誤網頁顯示太多資訊。
- **A06:2021-危險或過舊的元件**：使用有漏洞的舊版 Log4j 套件。
- **A07:2021-認證及驗證機制失效**：密碼重設連結可以直接從 email 網址看到重設 token。
- **A08:2021-軟體及資料完整性失效**：未驗證更新程式的數位簽章就直接安裝。
- **A09:2021-資安記錄及監控失效**：系統未記錄登入失敗紀錄。
- **A10:2021-伺服端請求偽造**：未驗證來源網站，可偽造請求從其他網站發送交易。



日誌管理

日誌管理：

- 日誌保存基本原則
  - 異地備份：日誌應存放於本機以外，防止竄改與遺失
  - 即時監控：使用 SIEM 工具進行分析(如 Splunk)
  - 必要資訊：裝置的來源、時間、使用者、來源和目的、動作、結果
  - 使用目的：故障排除、合規性記錄、支援威脅檢測、安全性問題確認等目的
  - 傳輸加密：由於日誌通常會傳輸到日誌伺服器，因此傳輸當中應該要加密處理
  - 容量控管：是否有容量控管的機制，比方說硬碟滿了從最後一筆開始寫入
- Windows 事件管理(Event Viewer)
  - 預設位置：%SystemRoot%\System32\winevt\Logs\
    - 系統日誌：系統運作相關（驅動程式、服務狀態）
    - 應用程式日誌：應用程式錯誤與警告資訊
    - 安全性日誌：重要安全事件（登入登出、權限變更）
    - 設定日誌：系統設定變更（軟體安裝、系統更新）
  - 常見事件 ID：4624(登入成功)、4625(登入失敗)
  - 可擴充性：可自行擴充其他類型

- Linux事件管理
    - /var/log/lastlog：所有用戶「最後一次登入」時間。指令lastlog (二進制檔案，不可用 vi 看)
    - /var/log/wtmp：成功登入記錄。指令 last(二進制檔案，不可用 vi 看)
    - /var/log/btmp：失敗登入記錄。指令 lastb(二進制檔案，不可用 vi 看)
    - /var/log/messages (RHEL) 或 syslog (Debian)：通用系統訊息（核心、服務、硬體）
    - /var/log/secure (RHEL) 或 auth.log (Debian)：認證與安全事件（SSH、SUDO、PAM）
    - /var/log/audit/audit.log：系統稽核記錄
- Apache vs. IIS 日誌格式筆記
    - Apache範例：192.168.1.1 - - [10/Dec/2023:14:30:45 +0800] "GET /index.html HTTP/1.1" 200 1234 "https://example.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
        - 解讀：IP 192.168.1.1在 2023年12月20日+8時區請求 /index.html，狀態碼 200，傳輸 1234 位元組。來自 https://example.com，使用 Windows 的 Firefox 瀏覽器。
    - IIS範例：
        - 2023-12-10 06:30:45 203.0.113.45 GET /products/item1 - 80 - 192.168.1.2 Mozilla/5.0+(Windows+NT+10.0) 200 0 0 234
        - 解讀：客戶端 192.168.1.2 於 2023-12-10 06:30:45（UTC）請求埠號80的資源 /products/item1。狀態碼 200，耗時 234 毫秒，使用 Windows 瀏覽器。

資通安全管理法要求

- 管理重點
  - 保存期限：按照業務需求和法規，例如：資通安全法規定保留 6 個月
  - 存取控制：限制日誌讀取與修改權限
  - 時間同步：確保所有系統時間一致 (NTP)
  - 定期備份：建立日誌備份機制
  - 異常監控：注意異常登入與存取行為

Severity Values

Value	Severity	中文翻譯
0	Emergency: system is unusable	緊急：系統無法使用
1	Alert: action must be taken immediately	警報：必須立即採取行動
2	Critical: critical conditions	嚴重：嚴重的狀況
3	Error: error conditions	錯誤：錯誤狀況
4	Warning: warning conditions	警告：警告狀況
5	Notice: normal but significant condition	注意：正常但重要的狀況
6	Informational: informational messages	資訊：資訊性訊息
7	Debug: debug-level messages	除錯：除錯層級訊息

情境背景

某醫院資料庫儲存患者就診紀錄，包含以下欄位：

- 非機密資料：年齡、性別、就診日期、診療科別、藥物名稱、檢查項目
- 機密資料：患者姓名、身分證字號、確診疾病名稱

案例一：資料庫聚合（Aggregation）

操作方式

攻擊者執行以下查詢：

1. 統計「2023年1月」於「腫瘤科」就診的「30-40歲女性」人數 → 得到 50人
2. 查詢同一時段腫瘤科開立的「標靶藥物A」總數量 → 得到45份

結果與機密性

- 單一查詢結果：人數或藥物數量均為非機密資料。
- 組合後推導：

「50名患者 vs. 45份藥物」→ 推論出90%患者使用標靶藥物A

→ 可能揭露「該科別主要治療癌症類型」（如乳癌），屬機密資訊。

關鍵特徵

- 直接組合現有資料，無需外部知識或複雜推理。
- 資料的「加總」或「比例」直接產生敏感性。

案例二：資料庫推論（Inference）**

操作方式

攻擊者執行以下查詢：

1. 查詢「患者X」的檢查項目 → 包含 BRCA1基因檢測（非機密）。
2. 結合外部知識：
    - BRCA1基因突變與「乳癌、卵巢癌」高度相關（公開醫學研究）。
    - 患者X近期於「婦科」有密集就診紀錄（非機密）。

結果與機密性

- 間接推導：患者X可能確診乳癌或卵巢癌（機密診斷）。

關鍵特徵

- 需依賴外部知識（BRCA1的醫學意義）。
- 透過邏輯連結非機密資料（檢查項目 + 就診科別）推論機密結果。

特性	聚合（Aggregation）	推論（Inference）
資料來源	直接組合資料庫內多筆非機密資料	結合資料庫內非機密資料 + 外部知識或統計推理
機密性產生方式	資料「加總」或「比例」直接揭露敏感性	需邏輯推理或跨領域知識連結才能推導機密結果
防禦手段	限制統計查詢（如設定最小查詢閾值）	模糊化資料粒度（如合併年齡區間、隱藏細節）