雲端個資安全包

(A) 個資自動盤點模組

(D) 電子郵件社交工程演練模組

(B) Web/雲端程式源碼檢測模組

(C) Web 雲端滲透測試/黑箱檢測模組

以上功能模組擇一勾選，
機關構得依據需求，增購各種模組組合。

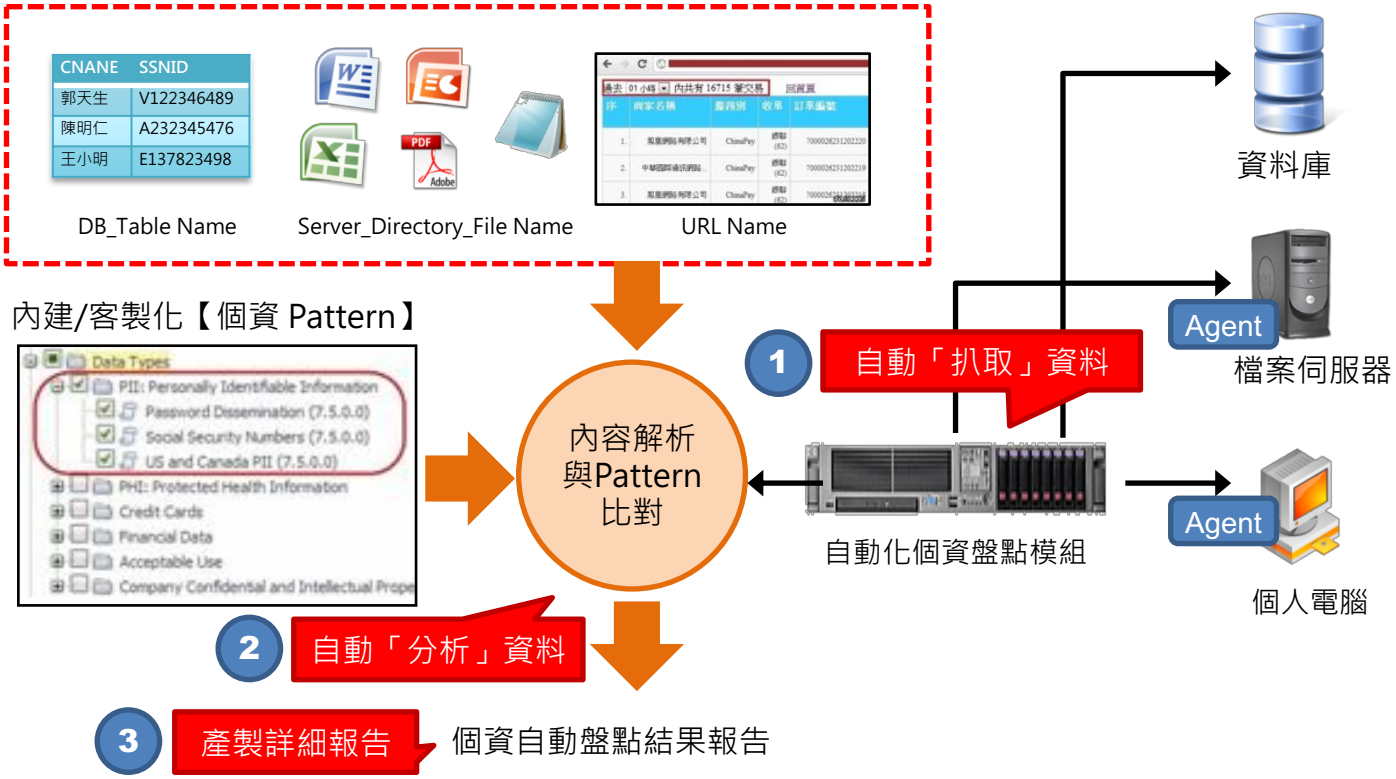
各模組功能，詳見後續內容說明

(A) 個資自動盤點模組

個資清查掌全貌，自動盤點見績效

企業或機關的個人資料以各種型態(如：檔案、資料庫、表單、報表等)散落在各作業流程、電腦設備、資訊系統、儲存媒體、文件櫃或檔案室中。企業或機關該如何在千頭萬緒的個資防護要求下，著手規劃可以符合個資法要求也能強化個資保護的行動方案？首要應該先針對分散於各地的電子型態個資進行完善清查，方能根據個資所在與風險高低，對症下藥進行相對風險處理與管理，善用預算資源創見績效。

模組運作架構

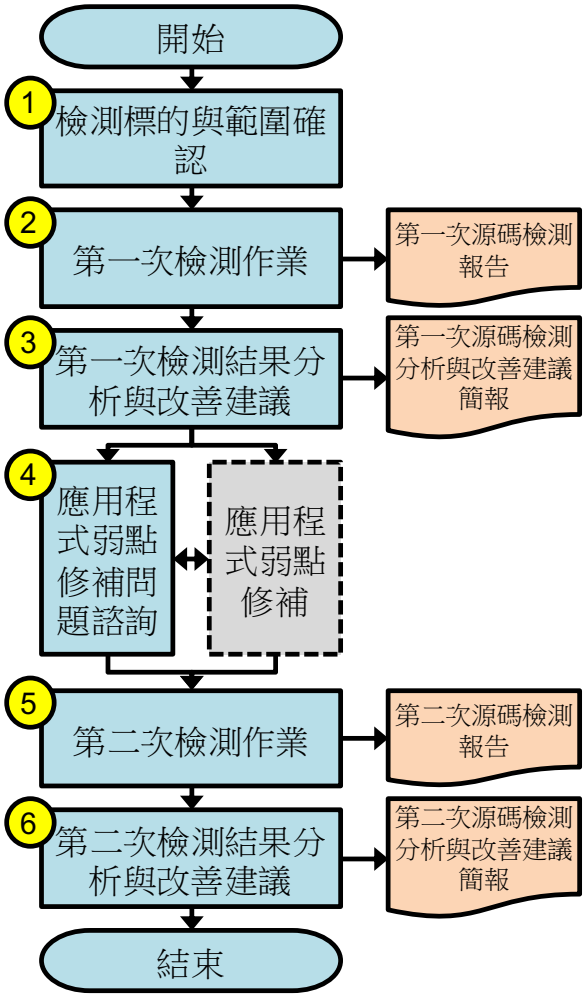


特色效益

- ■ 完整瞭解【機敏個資】儲存的現況
- ■ 避免人工盤點的遺漏，導致個資衝擊風險
- ■ 降低【個資盤點】人力負擔
- ■ 提高 DBA /程式設計師 生產力與績效
- ■ 提高個資風險評鑑的【正確性與完整性】
- ■ 做為個資風險評鑑的重要參考資訊

(B) Web/雲端程式源碼檢測模組

應用程式源碼檢測模組以「掃描檢視原始程式碼」的授權方式，讓客戶可了解網頁程式(Web AP)、行動APP(iOS & Android) 開發期間或上線前後，程式碼中潛藏的安全性弱點，同時透過分析其弱點種類、攻擊路徑等資訊，促使應用程式開發人員可以正確快速的修改程式弱點，強化網站應用程式之防護能力，避免遭受SQL Injection、Corss-Site Scripting與其它各式攻擊



特色效益

- 支援多種開發平台，同時確保資安法規遵循性。
- 允許開發人員便利且安全存進行應用程式檢測，進而推動機關企業之業務保障。
- 協助資訊部門確保機敏之安全。

(C) Web 雲端滲透測試/黑箱檢測模組

網站安全弱點，個資安全風險

政府機關(構)為因應與配合行政院研考會所編撰之「Web 應用程式安全參考指引(http://www.icst.org.tw)」以及「網站個資不當揭露」的嚴重性，期待快速有效地針對政府機關(構)既有與未來開發建置的網站定期或者不定期自動檢驗其可能的原始程式弱點與漏洞、網站個資掃描盤點檢測、網站系統弱點檢測以及網站安全個資稽核紀錄檢測等等，本模組乃一套有系統有效益的「Web 網站個資安全檢測」，助於提早發現程式漏洞，評估網站個資風險，提早進行網站應用程式改寫與修補動作，目前也支援 iOS 與 Android 行動 App 的安全檢測。

模組功能

■針對 OWASP 「跨網站腳本攻擊(XSS)」、「SQL Injection資料隱碼攻擊」、「命令注入攻擊 (Command Injection)」、等等 網站應用程式原始碼弱點安全問題之檢測 (http://www.owasp.org)。

■提供「網站/行動 App 安全原始碼檢測結果報告」，其中包含原始碼「弱點嚴重性分析」等風險高低評估計分與圖表，協助政府機關自行程式開發人員 或者委外開發承商，規畫安排程式原始碼弱點安全問題修復的優先順序。

■「安全原始碼檢測結果報告」提供完整的程式原始碼弱點安全問題，清楚標明程式原始碼弱點安全問題的結果與源頭，協助政府機關自行開發、委外開發或 專案管理人員了解【網站安全原始碼弱點】安全問題之發生程式行數與弱點來源，其中包含下列資訊：

- ➢程式源碼弱點掃描統計數據、弱點分類圖表、弱點細節。
- ➢程式源碼弱點所在之程式源碼片段、行數。
- ➢導致程式源碼弱點之函式名稱以及變數等。
- ➢程式源碼弱點安全漏洞相對之【直接修復建議】，方便開發人員修補漏洞。

■支援 應用程式開發語言：

- ➢MS .Net 架構 (C#、F#、J#、VB.NET)
- ➢Java
- ➢PHP

■支援 應用程式資料庫系統：

- ➢MS Access、MySQL、MS SQL/SQL Azure、Oracle

■系統需求：

- ➢ 作業系統：Windows Server 2008、2012 (含)以上
- ➢ 開發環境： Visual Studio 2010 (含)以上 、Eclipse 4.3 (含)以上
- ➢ 硬體需求：CPU 1.6GHz 雙核心(含)以上 、記憶體 4 GB (含)以上

(D) 電子郵件社交工程演練模組

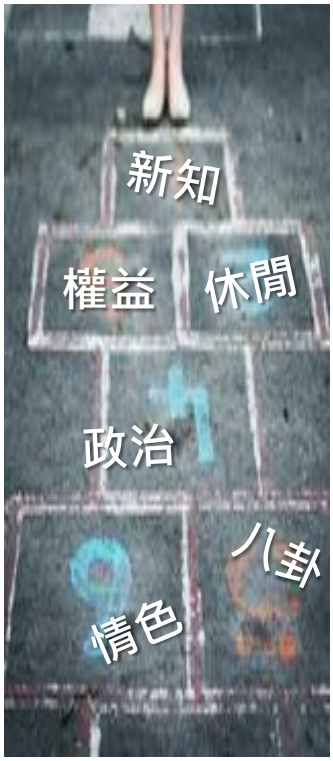
打破傳統！嶄新社交工程演練！

傳統迷思

■**輕忽威脅**：根據 Xecure Lab 分析研究結果，成功攻陷 Google 的極光行動、 EMC/RSA 的 SecurdID 被竊、Sony PSN 的億筆個資外洩 等等資安事件中，「社交工程惡意郵件」都是 **APT (進階持續性威脅)** 有心組織人士的重要成功滲透手段，千萬不能輕忽，否則 MIS 一世英明，將因為某位同仁的不小心開啟而毀於一旦。

■**配合形式**：多數政府機關、企業單位，可能形式上配合上級或稽核單位需求，雖然固定每年自辦或者委外進行「電子郵件社交工程演練」，但是因為**【演練信件強度】參差不齊**、**【演練方式受限傳統】**及**【演練週期過長】**，導致演練成效難以持續落實。

我們是否持續跳得過這些誘惑？



圖片來源：Google 圖片關鍵字搜尋結果，版權屬於原先網站所有。

嶄新作法

■**密集演練、立即提醒**：「關鍵三分鐘」往往是同仁開啟習慣調整改變的最大挑戰，然而我們面對的外部攻擊威脅卻是狂派團隊、持續不斷、一旦鎖定、絕不罷休的 APT 攻擊。因此，嶄新電子郵件社交工程演練在週期上建議「**每月四封 或者 每週一封**」，**一旦點選演練信件，立即警示畫面提醒**，將能強化印象，持續有效！

■**演練成績、自動通知**：演練後的成績公布，往往讓承辦人員左右為難，透過系統【自動分權】寄發成績給當事人、主管與承辦人，面面兼顧，簡易方便！

■**主管成績、另行計算**：根據單位機關的組織文化與管理哲學，另行統計計算主管演練成效。

特色效益

專為防護目的而全新開發之電子郵件社交工程演練系統，蒐集演練記錄並分析以下【**四種**】行為模式：

■**習慣行為**：分析同仁錯誤之【Client 組態設定】，助於避免誤會，同時判斷【開信習慣】，快速矯正根治。

■**衝動行為**：瞭解每位同仁之點閱連結與開啟附件之【類別與屬性分析】，助於提醒矯正，對症下藥。

■**散播行為**：過濾關鍵同仁中樂於分享之【轉寄信件】行為分析，佐以輔導提醒，降低風險。

■**成癮行為**：特殊個案之【成癮行為】分析，重點對象之強化教育，密集觀察與主官關懷，調整改變去癮。

AMXECURE
台北市信義區基隆路一段141號 12F-2　安資捷股份有限公司
www.amXecure.com