軟體供應鏈必學資安課題 如何拉近開發與資安距離？

資料來源｜ TechOrange 科技報橘

今年 IT 圈最熱門的話題之一，便是資本額達百億元以上的上市櫃公司須在年底前完成設立資安長及資安專責單位。以往資深資安人才本就難尋，如今更是炙手可熱。

日前臺灣資安主管聯盟的成立大會上，會長金慶柏曾指出，目前全台資安人才缺口超過 4 萬人！既然對外招募不容易，那麼從企業內部培養資安人才、提升人員資安意識便是另一途徑。

國內資訊軟體領導廠商叡揚資訊資安事業處范家禎處長指出，許多企業已建置防火牆、入侵偵測或防禦系統等，在網路安全方面有較完整的部署，但在應用程式安全上卻留下缺口。

75% 資安攻擊事件 針對應用程式弱點下手！ 企業卻往往無法真正落實源碼檢測！

根據 Gartner 調查，75% 的資安攻擊事件是針對應用程式弱點展開攻擊，然而應用程式安全的議題在企業裡卻容易成為三不管地帶，資安團隊不熟軟體開發，而開發團隊則不夠認識安全。因此，企業資安長的一大挑戰是培養內部資安人才，並建立起重視資訊安全的文化，拉近資安與程式開發團隊之間的距離。

應用程式安全不是安裝一套源碼檢測工具掃描弱點就結束，掃描後還得讓開發人員進行修復、測試再部署上線，許多企業往往礙於專案時程，無法落實源碼檢測。

范家禎處長指出，與其程式開發完才進行檢測，更好的做法是強化開發人員的程式碼安全教育訓練，在開發前就建立安全開發的概念。而開發過程中，則可透過工具協助，「邊寫邊掃」並立即修復弱點，從做中學建立實作經驗。

（左）叡揚資訊資安事業處范家禎處長 /（右）叡揚資訊資安事業處郭俐佳經理

企業源碼檢測挑戰多 系統委外開發、自行開發有不同解方

范家禎處長指出，一套好的源碼檢測工具必須能跟企業開發作業流程整合並滿足產業標準。

連續五年在 Gartner 應用程式安全檢測魔力象限中位於領先者地位的 Checkmarx，在平台中便內建教育訓練模組，當開發人員掃到程式中有弱點，可串接到訓練模組學習如何完整修改弱點，並立即修復程式，可說是完整整合企業開發流程的一套源碼檢測解決方案。

叡揚資訊則與 Checkmarx 攜手，透過多年的安全程式開發導入經驗，協助各大產業客戶進行工具導入，同時以累積十多年的顧問輔導經驗，協助客戶從導入、規劃到後續顧問服務，全方位提升應用系統安全。

例如目前政府機關資安等級 A 級單位與金融業都受到法規要求，在程式開發後需

> 范家禎處長指出，對金融業來說委外開發最常遇到的挑戰是，即使驗收階段工具掃描出有弱點，但外包商卻認為有爭議。

進行源碼檢測，而叡揚資訊資安事業處郭俐佳經理也進一步從叡揚資訊過去投入於資安領域十多年的經驗提出分析：委外廠商開發系統以及自行開發系統的企業，在進行源碼檢測或導入源碼檢測工具時，亦各有需要注意的關鍵重點。

以金融業者為例，指出金融業與政府單位經常由委外廠商協助開發系統，因此須在需求規格書中明定，將通過源碼檢測列入驗收項目之一，且建議直接明定採用最新版本的商業檢測工具檢測，以避免委外廠商採用相對容易掃出最少弱點的工具敷衍驗收流程，而安全性卻仍然堪憂。

此外，檢測不應只在交付驗收時做一次，現今系統經常推出新功能、新版本且攻擊的技術也不斷增長，演生新一代的弱點，因此建議要不定期且持續的掃描才能確保程式安全。

至於自行開發的系統，源碼檢測工具則須能與版本控制系統整合，彈性設定檢測頻率，如每週、每月、每半年檢測，掃出的弱點能分級分類並且通報相關人員，也可結合 Bug tracking system 管理追蹤，讓弱點修復後直接佈署上線。

范家禎處長指出，對金融業來說委外開發最常遇到的挑戰是，即使驗收階段工具掃描出有弱點，但外包商卻認為有爭議，此時，叡揚資訊便能扮演公正第三方的角色，協助企業判斷弱點，甚至是提供單次掃描服務進行安全性驗證。

找到弱點問題不難 能提出「快速修復建議」更為關鍵

范家禎處長點出，在軟體世界裡，如何快速又安全的開發，降低安全漏洞所產生風險，才是解決資安問題最低成本的解方，若能於 SDLC（軟體開發生命週期）初期就找到問題，才能實現快而安全的漏洞修復。

叡揚資訊在臺灣市場與 Checkmarx 合作超過九年，經過長期的觀察，范家禎處長指出，來自以色列的 Checkmarx 本身具備強大檢測量能，其技術團隊也致力於即時提供更新版本，因應程式語言以及資安風險的快速變遷。同時提供完整的軟體安全解決方案在統一的平台 (Checkmarx One) 上，囊括靜態白箱測試（SAST）、軟體組成分析（SCA）、惡意套件分析 (SCS)、互動測試（IAST）、API Security、雲端環境檢測 (KICS)、容器化檢測 (Container security) 與前述教育訓練模組（Codebashing），並以創新的 Checkmarx Fusion 在直覺的圖表中呈現威脅，顯示軟件組成與雲端資源間的關聯，還具備以下三大特色：

特色 1. 容易使用

Checkmarx 支援超過 20 種常用程式語言，包括行動 App。而且程式上傳即可掃描，不需另建環境。此外，能與 DevOps 流程、CI/CD 無縫整合，只要完成設定即可自動檢測掃瞄。

特色 2. 快速修復

找出弱點問題許多工具都做得到，但透過獲得專利的「最佳修復點」技術，Checkmarx 能做到圖形化顯示弱點路徑、最佳修復點，只需修改最關鍵的一個弱點，便能一次處理好其他相關聯的弱點，修一個抵十個，高效減輕開發人員的資安壓力。

同時 Checkmarx 還公開弱點掃描規則，這種透明的做法，能讓開發人員更清晰了解弱點發生根因，以及有效快速修復。

特色 3. 精準掃描

許多時候檢測工具導入失敗，往往是因實務上對企業「不適用」。例如檢測工具並不是針對行動應用程式而設計，往往在掃描結果上就不能達成企業想要的效益。Checkmarx 則能將檢測規則優化，大幅降低「不適用弱點」的出現頻率，並可透過客製化工具提升檢測精準度。

降低開發團隊「維運管理負擔」亦是重要考量

范家禎處長最後提醒，選擇可以持續更新並且支援最新版本的程式語言檢測工具會是關鍵，例如行動 App 的檢測能否支援最新版本，而不須為了使用檢測工具，被迫降版掃描。以及現今大型企業開發環境日趨複雜，有 Java、.NET、Python、iOS、Android 等各種環境，是否能建置單台掃描主機就能一次性管理，以減少開發團隊維運管理負擔，也是在評估檢測工具時的重要考量要素。

弱點修復對企業來說是長期投資，需要時間與人力，透過導入好的源碼檢測工具，並且將安全程式開發概念灌輸給企業內部所有開發人員，才能真正將企業安全弱點從源頭完美把關，並且降低修復成本。

當今除了金融業、政府機關外，許多跨國企業、高科技製造業也需因應客戶需求，在產品或服務交付前經過完整的程式碼檢測，包括醫療業也有明顯成長。因此，將安全納入程式開發流程中，作為整體品質的一環，也是企業重視商譽的表現。