強化軟體安全為民服務再升級

悠遊卡公司落實源碼檢測

撰文 | 叡揚資訊 行銷部

一分鐘看問題

導入產品

Checkmarx 源碼安全檢測工具

營運項目

準金融機構，多用途電子票證

遭遇挑戰

- 透過各項資訊安全評估作業，發現資安威脅與弱點，藉以實施技術面與管理面相關控制措施，需在表定時間內完成導入之要求。
- 第一次導入源碼檢測工具，需要顧問協助。
- 使用多種程式語言開發，環境相對複雜。

產生效益

- 如期達成源碼檢測機制導入目標，並改善弱點。
- 叡揚顧問協助導入，並建立安全程式開發習慣。
- 檢測環境設定簡單，不需準備多種開發環境及設備。
- 圖形化顯示弱點路徑及「最佳修復點」，可迅速修復弱點。

悠遊卡公司於2000年3月正式成立，初期是以非接觸式IC智慧卡整合大台北地區公車、捷運及北市公有路外停車場，為電子交通票證系統揭開新的里程碑，目前悠遊卡使用範圍已向外發展至纜車、動物園、高鐵、臺鐵、國道客運、藍色公路、特約商店小額消費等，提供民眾更便利之生活環境。

自2010年4月開始，悠遊卡開始提供特定商店的小額消費，其服務範圍已從單純的交通票證轉向多用途電子票證，相對的主管機關也從經濟部變成金管會，悠遊卡公司除已通過ISO 27001資安認證及BSI 10012個人資料保護認證外，仍不斷強化資訊安全管理，因此悠遊卡公司遂開始調查源碼檢測工具，以提升資訊安全管理之目標。

因應源碼檢測目標 導入Checkmarx

悠遊卡公司為提升資訊安全管理機制，特別針對網站及客戶端軟體進行弱點掃描、源碼掃描或黑箱測試進行資訊安全評估作業。黃士展經理表示：「為達公司提升資訊安全之要求，我們今年3月開始導入Checkmarx進行系統的源碼檢測，例如：web-based系統或一般消費者會使用的系統，目前透過Checkmarx進行對外系統的資安強化作業，以達公司目標。」

悠遊卡公司系統部經理 黃士展

操作及管理方便為選擇工具之首要條件

事實上選商時，悠遊卡公司也比較了其他工具，經過多方考量後，最後選擇了Checkmarx，黃經理明確的指出採用Checkmarx的主要原因有3：

1.系統操作容易且無須安裝編譯器：悠遊卡公司開發的程式涵蓋.NET、Java、PHP、ASP，及行動裝置iOS（Objective-C）、Android等，因此需要一套好管理且不需額外建立檢測環境的工具。而Checkmarx不需另外安裝編譯器（Compiler）、可隨修隨掃的特性，雙雙提升修改程式的便利性及方便管理的需求，且不增加開發人員操作負擔。

2.隨企業政策，彈性自訂檢測規則：工具可搭配企業政策規範，客製化檢測規則，以符合企業管理目的。

3.多種報表格式及圖形化報告：悠遊卡公司的AP多，負責單位也不同，Checkmarx的檢測報告可提供多樣報表供內部及委外廠商參考，並以圖形化顯示弱點路徑指出「最佳修復點」，讓相關單位修復弱點時可更方便、更具效率。

建立開發團隊安全程式開發觀念

悠遊卡公司除導入Checkmarx源碼檢測工具外，也藉此建立安全程式開發的觀念，同時參與安全程式開發課程建立開發人員資安風險意識。開發團隊也逐漸習慣在撰寫程式到一個階段即立刻進行源碼掃描，避免開發完畢後，系統互相關聯導致弱點數量倍增。

工具評估外企業配套制度及導入廠商專業能力也是重點

黃經理最後笑著說：「悠遊卡公司在網路、傳輸等都已有相對應的資安機制，但這是第一次導入源碼檢測工具。所幸導入之初，獲揚的資安顧問協助安排導入流程及給予掃描建議，也適時地提供豐富的輔導經驗提供參考，目前公司也持續提昇資安防護機制，讓悠遊卡公司為民服務的便利生活願景能夠更安全、也讓民眾更安心。」

更多客戶案例、資安資源 http://www.gss.com.tw/index.php/focus/security