叡揚資訊與 Checkmarx 助攻 關貿網路打通 SSDLC 安全血脈經絡

撰文 | 轉載 iThome

前往目錄

66

- *關貿網路從 1998 年承作網路報稅專案開始，自覺責任重大，決心就此貫徹 SSDLC（安全的軟體開發生命週期），立下「未經源碼檢測不得佈版上線」的天條；惟考量公司負責維運的系統量體龐大，日常變更作業需求繁多，唯有採用極高效能的源掃工具，才能順利落實「安全左移（Shift-Left）」完美境界。幾經審慎評估，於 2014 年拍板導入由叡揚資訊引薦的 Checkmarx 源碼檢測方案。*

99

源起於國家貿易通關自動化基礎建設的關貿網路，自 1996 年轉制為企業後，憑藉扎實技術底蘊，接連在流通供應鏈、電子市集、國稅與地方稅務、地政資訊、保險雲等重大公民營專案扮演要角，服務版圖涵蓋全民食、衣、住、行等生活大小事。

鑒於自身開發的系統皆屬重中之重、不容許絲毫差錯；因此關貿網路多年來如履薄冰，屢屢走在國內業界的最前沿，很早就導入 CMMI 軟體開發成熟度驗證並奉為圭臬至今，並領先引進系統/網站弱點掃瞄工具、 SOC 監控平臺，也在 2004 年通過 BS 7799 、亦即現在的 ISO 27001 資安認證，以彰顯充分保障個人隱私與企業機敏資料安全的實力，爭取業主信任。

更重要的，關貿網路從 1998 年承作網路報稅專案開始，自覺責任重大，決心就此貫徹 SSDLC （安全的軟體開發生命週期），立下「未經源碼檢測不得佈版上線」的天條；惟考量公司負責維運的系統量體龐大，日常變更作業需求繁多，唯有採用極高效能的源掃工具，才能順利落實「安全左移 （Shift-Left）」完美境界。幾經審慎評估，於 2014 年拍板導入由叡揚資訊引薦的 Checkmarx 源碼檢測方案。

得力於差異比對，成功突破源掃瓶頸

關貿網路副總經理兼資安長方念德表示，回顧多年前關貿網路承作網路報稅系統開發，深覺其中涉及全民個資，茲事體大，務求做到滴水不漏的資安防護，因此不僅傾全力強化網路資安建設，亦力求系統開發嚴謹性。因而決定遵照 CMMI 規範，限定今後所有系統上線前，皆需通過品保中心的源掃程序、沒有便宜行事的空間。

一開始，品保工程師以人工方式執行 Code Review ，考量長此以往恐因效率有限導致專案卡關，故於 2008 年引進源碼檢測工具。

關貿網路品保中心副理邱明昇說，可惜受限於當年工具技術尚不成熟，僅支援「整包掃瞄」，亦即每套系統不論更改的程式碼多寡、通通都得從頭到尾測過一輪，以致部份大型系統耗時 1~2 天甚至更久才完成掃瞄，造成專案時效冗長，且品保中心也無力承接臨時變更單。

「於是在 2011 、 2012 年期間，我們積極評估其他源掃工具，期望解決當時痛點，」邱明昇指出，當年市場上相關產品選項不多，且幾乎都停留在整包掃瞄層次，可說遍尋不著合適標的；直到發現了叡揚剛引進 Checkmarx ，才真正看見轉機。

經過品保中心執行 PoC ，確認 Checkmarx 不僅掃瞄速度更快，且支援差異比對技術、僅掃瞄異動程式碼，有效避免作業時間延宕，一般專案都能在 3 、 5 分鐘內檢測完畢，與先前冗長時程相比天差地遠；而且僅憑簡單勾選設定，即可依據關貿網路所需遵循的 OWASP Top 10 、 OWASP Mobile Top 10 、 SANS Top 25 及 PCI DSS 等國際規範執行檢測與產出報告。因此當品保中心提出 Checkmarx 採購建議，旋即獲得公司高層支持，就此定案。

專業團隊鼎力支持，打造最佳檢測環境

圖說：左起叡揚資訊資安事業處業務代表蘇家汝、副處長郭俐佳、資深資安工程師林泓宇、關貿網路股份有限公司副總經理兼資安長方念德、品保中心副理邱明昇、資安整合服務部資安總監林恆生

受惠於叡揚團隊的專業服務能力，使 Checkmarx 導人過程極為平順。叡揚不僅依據關貿網路當下與未來檢測量能，針對主機容量進行最適規劃，也悉心安排教育訓練、系統安裝及使用諮詢等工作，讓使用者無痛接軌新環境。隨著系統上線至今，只要 OWASP 等規範出現更新，叡揚都會立即提供 Patch 檔，確使品保中心恆常套用最新安全程式碼撰寫規則。

現在，開發部門會將預計在 2~3 天後上線的程式碼，先行送交品保中心檢測。關貿網路資安整合服務部資安總監林恆生說，無論發現高中低等級之風險，品保中心便轉交資安部門識別是否為誤判，若證實非誤判，會連同修改建議交回原單位做修正，改完再送測一次，確認正確與有效修補後，才可上線。

如果開發部門有緊急變更需求，可直接填妥系統變更單、送交品保中心執行源掃，一旦檢測無虞，就直接透過 CI/CD 程序佈版上線。

落實安全左移。其次品保中心可藉由 Checkmarx 完整掃瞄紀錄檔，形成扎實的佐證，隨時因應嚴格的外部稽核要求。

再者自從 Checkmarx 上線後，成功扭轉開發者等待修正問題的被動慣性，而會主動針對被檢測出來的錯誤、思索如何避免再犯，使整體退件率顯著下修，持續精進程式開發品質。

方念德補充說，此外考量現今快速付的時代，系統開發案引用越來越多開源框架與元件，而近年來由元件導致的資安事件頻傳，也可能蘊藏高風險漏洞，因此公司規定，若開發者有意採用未曾通過公司檢測的新框架與元件，須在撰寫程式前，將它們連同第一支 Sample Code 送交品保中心執行 Checkmarx 掃瞄，確認安全無虞才能繼續採用。 未來也規劃一系列的開源碼管控措施，加強專案的安全性。

叡揚資訊資安事業處副處長郭俐佳則表示， Checkmarx 考量用戶亟欲打造安全程式碼、又想降低 Loop 周期，開始提供安全程式碼課程，引導企業達到安全與效率的完美平衡。不僅如此， Checkmarx 有感於駭客攻擊手法日新月異，導致企業必須顧及更多資安檢測環節，因此除了持續精進源掃核心功能外，也不斷擴展應用程式組成分析模組，如今舉凡第三方框架或元件、 IaC 腳本或 API ，都已納入檢測範圍，希冀為包括關貿網路等眾多用戶持續挹注更大價值。

瞭解更多 Checkmarx 解決方案：https://www.gss.com.tw/checkmarx

最新 Checkmarx 白皮書下載：AWS 與 Checkmarx 共同對談：如何保護雲端開發維運