持續整合 CI 與應用系統安全測試

軟體開發最佳實務 – 避免人為錯誤 有效提升軟體品質

文章來源：Checkmarx 翻譯整理：叡揚資訊 資訊安全事業處

持續整合 (CI) 在軟體工程中是個每日會進行多次的開發合併與分享 (merge & share) 工作

持續整合 CI 與應用系統安全測試的挑戰

持續整合讓企業能在一天內建構數百個專案以及在短時間內應付多次的程式異動，也越來越流行於敏捷開發的團隊中。

敏捷開發在整個開發生命週期中 提供了調整方向的機會

使用規律的循環開發，如 sprints 或 iterations，在循環結束的時候，團隊必須展示一個可交付且包含新增修改的版本。相較於其他開發流程，敏捷開發強調的並非看單一次的結果，而是評估每次的 sprints 結果，一般兩週為一個周期並根據需求調整專案往新的方向。在 SaaS 的領域已經廣泛的採用敏捷的持續整合 / 交付。開發團隊利用敏捷開發及雲端管理工具，於同一時間內執行正確的技術，有效率的於一天內多次地遞送和修改版本。

傳統應用系統的安全法則 可能無法支援這些快速的週期

1. 大多數安全檢測技術都依賴於專案完成後，通常需要很長的時間來進行，可能會延誤預定的發布日期。
2. 開發人員為各自原始碼發現的安全性弱點負責。傳統的應用系統安全測試方案適用於開發過程結束後，有些甚至是程式碼開發完成數個月後。在這種情況下，開發人員必須回頭檢視舊的程式碼，這需要很長的時間重新熟悉。傳統的應用系統安全測試方案一旦發現弱點，在無法處理的情況下往往選擇忽略它。這是持續整合的關鍵，以防止這種「障礙」，並加強對開發人員最有效的修復方式及技術教育。

3. 滲透測試在大多數情況下，需要獨立的測試團隊或第三方廠商在開發週期的尾聲執行如黑箱測試類型的軟體。滲透測試是昂貴且耗時的。最重要的是，他們必須確保在每一個新版本變更是不影響安全性。但在談到 CICD（持續整合 / 持續部署，Continuous Integration Continuous Deployment）這幾乎是不可能達成且費用是滿可觀的。

如何滿足持續整合？

Checkmarx CxSAST 是一個精確度高和靈活的應用程式安全分析產品，使企業能夠自動掃描未編譯 / 未建置的原始碼，並於常見開發語言中定義了數百個安全性弱點。CxSAST 有效地與 SDLC(軟體開發生命周期，Software Development Life Cycle) 整合且簡化檢測與修復流程。

Checkmarx 的主要任務是使應用程式安全成為 SDLC 的一環

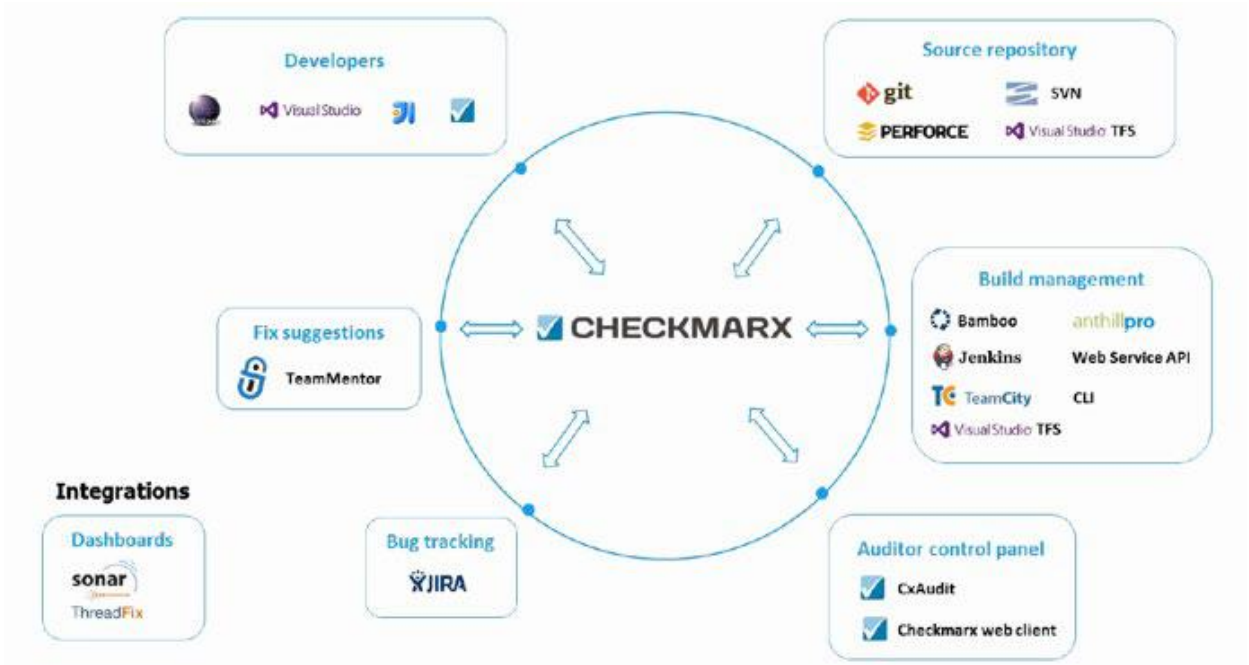
持續整合是敏捷軟體開發生命週期中的其中一個環節，提高了開發人員發現和解決安全性相關問題的能力，達到一個提供「無缺陷」的建置與發佈。

Checkmarx 不僅能檢測原始碼 / 未經建置程式碼的弱點，也能於任意的時間點下進行完整或部分程式碼掃描，提供給開發人員：

- 圖形化顯示弱點資料流程、弱點修復的具體位置 (即最有效率修復點)、建議最有效率的修復方式。
- 如同 QA 流程，應用程式的安全性應該整合到開發及測試環境。

因此，這一切都是在 SDLC 過程中完成，以減少影響發佈的可能。

於 SDLC 中有效實踐資安政策



Checkmarx CxSAST 源碼檢測工具 完整支援持續整合與佈署的弱點管理

1. 整合容易：整合常見的“Continuous Integration servers”如 Jenkins, Bamboo, TeamCity, Visual Studio TFS, Anthillpro。
2. 提供 Web Services API：能輕鬆的與任何類型的建構伺服器及原始碼版本控管軟體整合。
3. 提供 CxConsole 命令提示字元界面（CLI）來觸發掃描。在軟體管理工具中直接觸發，達成軟體開發生命週期中的持續整合。

四個簡單的步驟 確保程式碼安全為建構管理流程的一部分

1. INTEGRATE 整合

Checkmarx 具有足夠的靈活性與 SDLC 無縫接軌，支援最常見的建構伺服器，或者您可以執行簡單的 API，以流暢操作簡單的環境，提供優質的 SAST（靜態應用程式安全測試，Static Application Security Testing）

2. ANALYZE & TRACK 分析與追蹤

Checkmarx CxSAST 提供優良的弱點報告，利用互動的 HTML 介面提供特定程式碼片段，包含實際弱點所在位置、何處可進行快速修改的建議，讓讀取報告的人員方便且快速的進行修復。輕鬆與問題追蹤管理工具整合 (Bug tracking) 如 JIRA。將結果（自動新增問題單）如產生弱點的位置提供給特定的開發人員，

3. SET & ENFORCE 制定和執行

落實安全政策，並確保有問題的程式碼無法上線。

當弱點超過安全政策所規定的標準時，必須標記建置為不穩定、發送警示或中斷此次建置。

4. AUTOMATE 自動化

持續整合伺服器設置自動觸發 Checkmarx 掃描流程：

- 提早檢測可能發生的安全性弱點，縮短修復時間從而降低開發成本。
- 經由立即修補問題減少開發人員的挫折與負擔，而不是回頭檢視年代久遠的程式碼。
- 減少版本發佈延遲。
- 降低持續性滲透測試的成本且調整為僅用於驗證測試。

延伸閱讀成功案例：[採用敏捷開發 / 持續整合的大型軟體公司 (LIVEPERSON)，落實 Secure SDLC 大幅降低軟體弱點]

更多最新資安電子報：請瀏覽 http://www.gss.com.tw/index.php/focus/security