看準Checkmarx簡單、明瞭、清晰　連美國陸軍也愛用

華泰銀行落實源碼檢測無縫接軌程式開發

撰文 | 叡揚資訊　行銷部

華泰銀行在卓越雜誌2014年「中型銀行服務品質調查」，一舉奪得「最佳客戶服務」及「最佳銀行財富管理服務」二項大獎，矢志成為「最關心客戶健康的銀行」，更著眼於IT服務之資安防護，提供給客戶最好最健康的虛擬服務環境。

一分鐘看問題

導入單位及目的

華泰銀行 AP 團隊及檢核管理委外素質

導入產品

Checkmarx

被 Gartner 評為應用系統安全領域「Cool Vendor」，其使用便利、檢測精準、管理便利、採購彈性深受開發及稽核人員青睞，已被美國陸軍、道瓊斯 (新聞集團)、Salesforce.com、Samsung、全球財富 1000 大之電信、金融保險、汽車、媒體娛樂、軟體服務等集團採用。

產品效益

- Checkmarx 可結合版本控管
- 開發人員最喜歡弱點流程圖還有最佳修復點建議
- 系統畫面人性化 & 簡單明瞭
- 叡揚顧問專業服務

長達半年之久的嚴謹POC

面對不斷進化的資安攻擊及因應金管會之資安要求，「花了半年的時間針對源碼掃描工具做過嚴謹的概念驗證(POC)，更別提前置的Survey作業！」華泰銀行資訊部陳嘉祥資深經理笑笑地說，從需求面來看，華泰銀會想要作應用程式的檢測，有3大考量：

自我要求

資安問題層出不窮，華泰銀近年成立資安處，顯示其重視資安之程度，「除了內部自行開發外，不少專案乃與委外團隊合作，故透過導入Checkmarx嚴謹把關源碼、制定更明確的KPI，讓系統上線制度更透明、更安全、更高效。」

法規要求

為因應金管會之資安要求，所以需要定期實施安全檢測。

華泰銀行陳嘉祥資深經理：如果源碼健檢後，是一本厚厚的弱點報告，對於AP開發團隊來說，不僅繁瑣而且會抗拒！

應變能力

對於既有之系統，陳嘉祥資深經理從更長遠的管理模式下手，「就目前駭客能力進化之快，沒人敢保證我們”認為”安全的系統可以永保安康！」故針對既有系統，華泰銀定期以Checkmarx健診，「一來可以建立內部監控機制，二來可以持續精進同仁資安防禦觀念，達到真正落實教育深耕之效。」

重視User為AP單位管理有一套

談到資安管理，陳嘉祥資深經理有一套「栓螺絲」理論，「欲速則不達，吃緊弄破碗，建立開發AP同仁之資安觀念架構要步步經營，而不是強迫一次到位全盤接受。」從AP出身的陳嘉祥資深經理，對於資安與AP開發之間的愛恨糾葛瞭若指掌，而Checkmarx有效分析，直指不安全程式碼發生處，更是華泰銀AP開發團隊肯定之處。

不要厚厚的弱點報告而是具有建議價值的檢測結果

「如果源碼健檢後，是一本厚厚的弱點報告，對於AP開發團隊來說，不僅繁瑣而且會抗拒！」陳嘉祥資深經理坦言，在開發程式壓力下，還要面對資安檢驗，加上源碼檢測一定會有灰色地帶，「要同仁照單全收不可能，但是源碼檢測一定要靠工具，而且讓同仁理解源碼檢測非Loading而是多一個輔助，故Checkmarx的簡單、明瞭、清晰特性，就是我們所需要的!」陳嘉祥資深經理斬釘截鐵直言經過半年POC選擇Checkmarx的主因。

Checkmarx的好用連AP也認同

故從評選到導入，陳嘉祥資深經理聰明地利用「雙軌制」進行，「就我所知，很多單位都是以資安團隊單方向推動主導，但最受影響的卻是AP開發團隊！」故華泰銀以「User」為中心，從評估、POC及最後採購，AP開發團隊都參與其中，「目前，我們很開心看

Tips

Checkmarx 實用、簡單、好上手

我們比較重視實用、簡單、好上手，功能太多太複雜反而未必是我們要的。所以有些源碼掃描產品，功能很多圖表很華麗，不見得會是第一選擇；另外，有些產品宣稱掃描速度很快，這點華泰銀倒是覺得要審視其資安邏輯，「資安產品原則上我們會花三個月到半年的時間 POC，以全盤性考量為主！」

以 WebGoat 為例，改一處即可同時修復 20 個問題

到預期效果，源碼掃描可以落實在程式開發生命週期，Checkmarx 順利融入 AP 開發作業流程中，不會淪為表面制式，也不會造成龐大 Loading ！」

實際上，華泰銀在選擇源碼掃描產品，有六大考量點：1. 使用難易度，2. 使用介面，3. 支援語言，4. 檢測能力，5. 檢測結果及報表品質 6. 合作廠商之服務專業能力

1. 使用難易度

「Checkmarx 介面好懂，操作便利，所需的環境準備起來也不複雜，對開發人員來說容易上手、負擔小。」華泰銀行選擇工具的重點在於「最適合」企業及使用者 (開發、稽核人員) 所需，若使用的工具功能遠多於企業所需，對使用單位而言，反而造成負擔。

2. 使用介面

支援中文介面，相關的選項設定，甚至對於弱點的修補建議都是中文，降低使用難度。

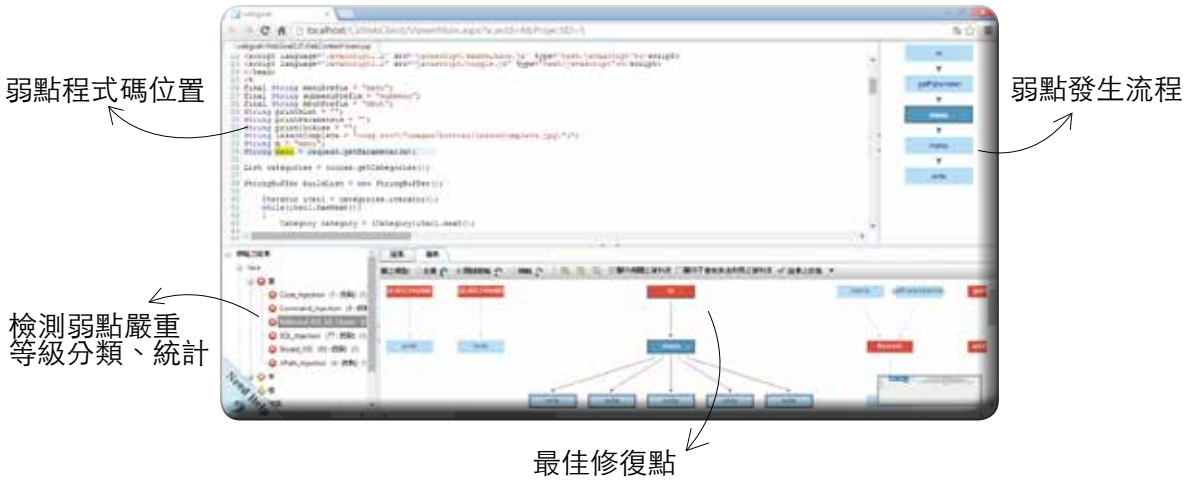
3. 支援語言

除了支援常用的 Java 、.NET 外，也支援其他主流開發語言及 iOS、Android 等，未來如有其他語言的掃描需求，即可直接採用。

4. 檢測能力

檢測工具除了速度外，更重要的是本身的 methodology 及檢測能力。經過測試比較，發現 Checkmarx 可以確實、有效地發現埋藏在 AP 中的 OWASP Top10 及其他弱點。有效發現

一目了然 簡單好操作
AP、稽核愛用的源碼掃描介面



真正的弱點，這比單純比較檢測速度、弱點數量更為重要。

5. 檢測結果及報表品質

是否包括執行摘要、漏洞描述、程式修補建議等。很多公司的困境為，在掃瞄完成之後，出了厚厚一本詳盡的弱點報告給客戶，但開發單位認為問題多到不知從何下手，導致反彈。故華泰銀相當重視報表內容品質是否實用，太繁雜的報表圖表反而不列入考量，相對的 Checkmarx 提供弱點嚴重等級區分，以及弱點的「最佳修復點」，能協助開發人員有效的針對問題下手，快速解決問題。

6. 合作廠商之服務專業能力

選擇工具後，安裝建置、教育訓練、技術支援能力都是影響導入成效的因素。叡揚在金融單位深耕多年，源碼檢測領域亦有豐富的銀行建置經驗，廠商的技術能量、經驗及合作態度亦是考量重點。

金融業第一家導入Checkmarx 慎重考慮之久

「我們是金融業第一家導入 Checkmarx，前無古人的情形下，真的慎重考慮非常久。」陳嘉祥資深經理解釋說明，Checkmarx 算是源碼掃描後起之秀，故市場知名度不若其他競爭廠商，「但從 POC 表現來看，加上之前恰好有導入別的以色列產品，其高性價比、高 Performance 令人印象深刻，此外，叡揚有豐厚的金融業合作經驗及資安服務能量，所以最後還是選擇叡揚資訊所代理的 Checkmarx。」

比較跟過往用人工檢核的模式相比，陳嘉祥資深經理也認同 Checkmarx 清晰量化源碼檢查這塊，「目前，凡是對外的 AP 一定要經 Checkmarx 這關，如有 Urgent 等級，則規定兩個禮拜內一定要如期改善！」未來，還可利用 Checkmarx 做資安健檢應用，例如將已上線的 AP 定期用最新檢測規則掃描，確保系統遠離最新的漏洞威脅，鞏固華泰銀的資安基本功。

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