## 培養安全開發概念 為ISO 27001做準備

# 中研院善用 Checkmarx 源碼檢測機制再升級

撰文 | 叡揚資訊 行銷部

### 一分鐘看問題

**導入單位**

中央研究院 計算中心

**單位任務**

計算中心的核心任務是提供中研院所有的資訊服務，包含資安通報與資安制度推行。

**源碼檢測機制 (Armorize→Checkmarx) 轉換原因**

- 權限不足，使用人數僅能一人使用
- 無法跨平台支援、程式語言相容性不（例：行動平台），導致掃描能力不全，總有疏漏
- 原有機制掃描時間過長
- 為通過ISO 27001需進行相關前置作業，並建立「安全開發」的概念

**主要開發語言或平台**

PHP、Java、.NET、Android

中央研究院身為中華民國學術研究最高機關成立於民國17年，隨著歷史因素從南京播遷來台，終於在民國43年於南港現址落地生根，歷任院長胡適、吳大猷、李遠哲等都為當代著名之學者專家，由此可見中研院在國家學術研究之重要地位。

隨著國內外資安攻擊事件頻傳，政府也開始正視資訊安全的重要性，除了行政院要求相關單位必須通過ISO 270001認證之外，各級單位也要求每件專案必須隨案提供原始碼安全白箱掃描報告，科技部對於網站源碼檢測、弱點掃描的要求亦更加嚴格。上述規範下，中研院為能順利執行專案並完成結案，在多年前便已導入源碼檢測機制，然而當初導入的機制已無法滿足當前需求，故中研院便開始思索替代方案的可能。

中央研究院計算中心資安組組員 林子煒

## 受限於支援語言
## 轉而擁抱 Checkmarx

中央研究院計算中心資安組承辦人林子煒先生坦言，既有的程式碼掃描工具支援語言種類不夠多，而且無法跨平台檢測，造成研究開發資訊安全上的瓶頸，事實上，阿碼除了開發語言支援性不足的問題外，系統權限僅在單一使用者，也成為中研院計算中心決定改採 Checkmarx 的原因之一。

↑ 支援多種開發語言（含行動平台：iOS, Android, Windows Phone）。

從阿碼轉換到 Checkmarx 後，中研院希望透過新的檢測機制可以建立各單位撰寫程式時具有「安全開發」的概念，主要做法為鼓勵工程師完成一小段程式後，立即啟用源碼檢測工具來偵測弱點程式，而非完成整個專案後才一次進行掃描，因分段式的源碼掃描遠比一次檢測所有程式更具效率，在開發中了解問題程式進行弱點分析，避免相同的弱點產生，讓工程師開發時更嚴謹，也能節省事後修復程式問題的時間與人力。

## 為通過 ISO 27001 率先導入
## 源碼檢測 Checkmarx做前置準備

除了原有機制不敷使用之外，為配合行政院宣布下轄機構組織需通過資訊安全管理標準 ISO 270001 認證，於是中研院遂針對所有研究開發工作，建立一套符合資安標準的開發流程及檢驗機制，因此 Checkmarx 便成為來日導入ISO 27001 之前導措施。

## Checkmarx 好用易上手
## 無痛轉換既有工具

提到使用Checkmarx 的心得，林子煒先生表示肯定，並補充說到Checkmarx 可以即時檢視掃描成果、嚴重等級分析、及版控整合功能，完全補足原本檢測機制的不足。

### 即時檢視掃描成果
### 直指弱點程式

在還沒有採用Checkmarx 之前，掃描程式碼有時需要等待半天，工程師面臨開發時程的壓力，卻還要等待掃描檢測，無論在時間或效率上都無法滿足計算中心的需求。相對的，Checkmarx 能支援的語言較多，所以精準度也相對提升，透過Checkmarx 進行檢測也能立即得到結果，並且標示弱點程式，回應時間縮短到15分鐘以內，源碼安全檢測時效性提高10倍以上，大幅提升開發工程師的工作效率。

↑ Checkmarx 迅速修復弱點建議。

### 明確的嚴重等級分析
### 協助有效調整防護措施

Checkmarx 根據程式的嚴重性區分出高、中、低與資訊四個等級，明確指出漏洞的嚴重性為何，相對的開發人員可以視本身對專案及程式的瞭解，調整嚴重性的應對方式，如：某支程式屬於低嚴重性，對整個專案不致造成威脅，或某個規則為必要存在但卻被

↑ Checkmarx 能與版控機制及軟體開發流程整合，輕鬆融入組織流程及管理機制。

診斷為低嚴重性，就機動調整其他的防護方式，達到安全開發的要求。

### 與版控整合
### 提升開發人員工作效率

Checkmarx可與版本控制軟體（Git）結合，整合後讓掃描源碼的工作更為方便，因此在中研院內提供兩種不同的掃描方式，一種是以版控（Git檔）為主，主要是來自計算中心內部的案件掃描，另一種是直接打包源碼（zip）進行掃描，主要是計算中心外的其他單位。

### 管理方便
### 清楚監控院內AP安全狀況

有別於阿碼檢測，Checkmarx的使用權限較有彈性，可提供多人使用讓源碼檢測工作不限於單一人員，管理者也可以清楚監控中研院內每件專案的風險程度，並不會因為系統上有多重使用者，而有難以集中管理的狀況。

### 好的源碼檢測工具＋100%顧問服務＝ 2X開發效率

身為計算中心的一員，林子煒認為自從轉換到Checkmarx之後，不僅轉換檢測機制外，好像也多請了一個顧問團隊，因為叡揚團隊適時的協助中研院在系統使用上的困難，也提供顧問建議和專家檢視這樣的協助，讓中研院在研究開發也同時進行源碼安全性校正，工作流程不但沒有產生額外的工作，反而還提升了開發效率，同時也呼應中研院希望建立開發人員進行研究開發時擁有的「安全開發」概念。

Checkmarx導入中研院近一年的時間，計算中心源碼檢測服務也上線即將屆滿一年，獲得其他單位的正向反饋，中研院在近程目標期望能將Checkmarx源碼檢測服務納入其他單位的開發流程中，當各單位在研究開發過程中更嚴謹，未來導入ISO 27001時也將會更順利。

## 叡揚深厚專業AP資安經驗
## 協助客戶源碼安全成功關鍵

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