Fortify

產品效益

■提早發現安全弱點早期修補，降低上線後修補的問題與成本

■提供量化數據呈現軟體品質與差異

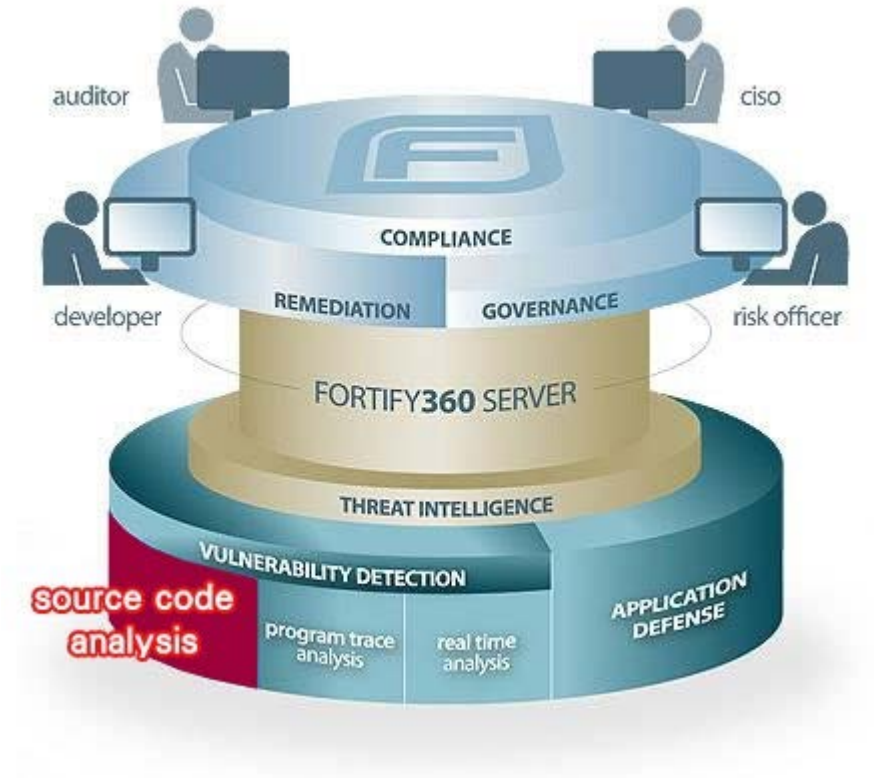
■確保委外開發軟體的安全品質

符合法規需求： 本產品符合相關法規需求，如 PCI-DSS、ISO27001、金融機構資訊系統安全基準等。

符合 SSDLC 軟體開發準則： 於 SDLC 開發階段導入本產品可增加軟體資訊安全強度。

軟體運作原理：

HP Fortify SCA 靜態源碼檢測分析工具



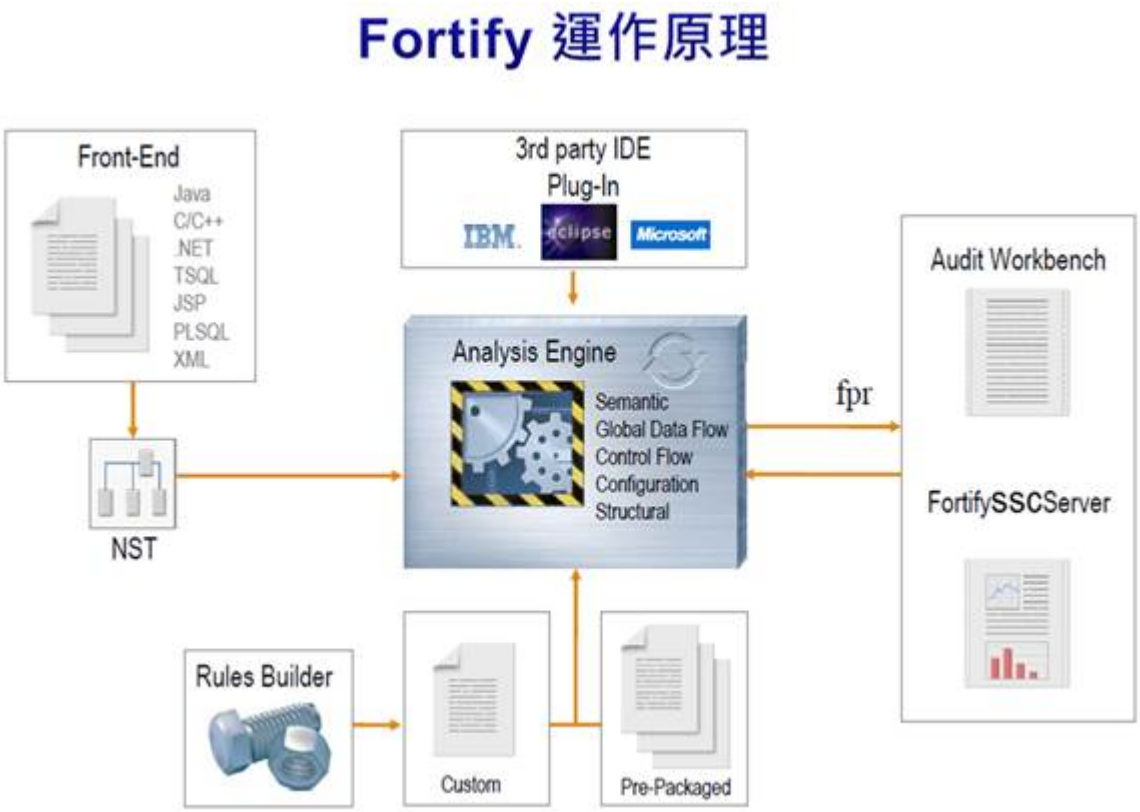
在軟體發展過程中，如果可以愈早發現軟體的弱點及瑕疵，就愈能降低因修補所帶來的負面影響與付出的額外成本。而程式源碼之自動化檢測與分析工具，可以有效、完整及精確地協助開發人員找出程式碼中的弱點，讓開發人員可以看到安全弱點所在位置，並排定弱點的優先次序進行修補，避免相同弱點再度發生在其他程式碼中。

HP Fortify SCA(Static Code Analyzer)便可以協助你滿足應用程式安全檢測與分析所有需求。

一. 程式碼靜態分析專利技術

HP Fortify SCA 採用專利的 X-Tier 資料流程分析技術，完整分析各種程式語言之執行流程、資料輸入/輸出及程式語法，即使同一個應用系統中包含了不同語言的程式 碼，也可以完整分析及串接。透過 HP 持續更新的檢查規則(Rulepack)，讓最新的弱點可以被發現並修補，使用者也可以自行定義分析規則，針對特殊程式撰寫規範或要求進行檢查。

三階段分析技術原理：

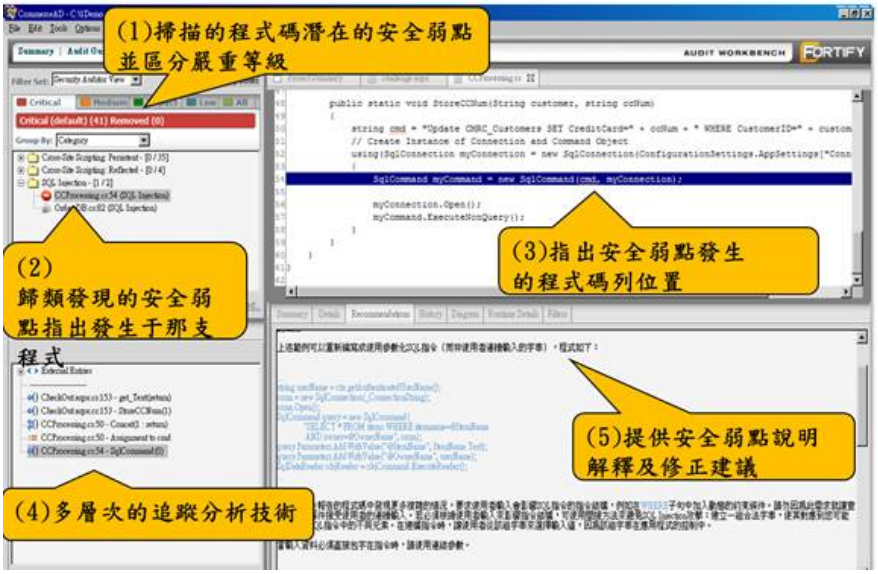


1. 轉譯階段(Translation Phase) 將各類不同的程式語言轉譯成分析引擎可以分析的中繼語言(Metaleangeage)。
2. 分析階段(Analysis Phase) 依據內建或自行定義的檢查規則分析中繼語言中是否有符合條件的安全弱點或品質瑕疵。
3. 稽核階段(Audit Phase) 呈現分析後的結果，讓稽核人員或開發人員可以很容易地瞭解所發現的問題，並確認是否應進行修補。

二. 全面完整的分析結果呈現

在檢測結果分析畫面中，可以很彈性性的改變弱點分類及過濾的方法與條件，讓弱點分析及審查人員可以用不同的角度來析發現的弱點，促進弱點修補的效率。

Audit workbench 程式碼安全漏洞審核分析工具



三. 支援最完整的程式語言

目前 HP Fortify SCA 可以支援超過 20 種以上的程式語言，包含：

Microsoft 系列：ASP.Net、VB.Net、C#.Net、ASP、VBScript、VB6。 ．

Apple Mac 系列：Objective-C、Action Script。 ．

Java 系列：Java、JSP。 ．

其他 Web 系列：HTML、 JavaScript、PHP、XML、ColdFusion 5.0、Python。 ．

Database 系列：T-SQL(MSSQL DB)、PL/SQL(Oracle DB)。 ．

傳統第二代語言：C/C++、COBOL。 ．

SAP 系列：ABAP/BSP。 ．

行動 APP 系列：Objective-C(iPhone)、Java(Android)、C#.Net(WinPhone)

四. 支援最廣泛的程式碼問題偵測

目前 HP Fortify SCA 可檢測超過 500 種的軟體弱點，包含：程式安全與品質類型的偵測規則。例如：

Input Validation 類型：SQL Injection、Cross-Site Scripting、Resource Injection、Open Redirect 等。 ．Security Features 類型：Password Management、Insecure Randomness、Weak Encryption 等。 ．

Error Handling 類型：Poor Error Handling 等。 ．

API Abuse 類型：Code Correctness、Missing Check againt Null、Dangerous Method 等。 ．

Code Quality 類型：Dead Code、Unrelease Resourse 等。 ．

Environment 類型：Misconfiguration 等。

上述各種類型中已包含 OWASP 2010 與 OWASP 2013 等 Top 10 弱點。

檢測問題等級的區分方法

檢測問題等級的歸類方式

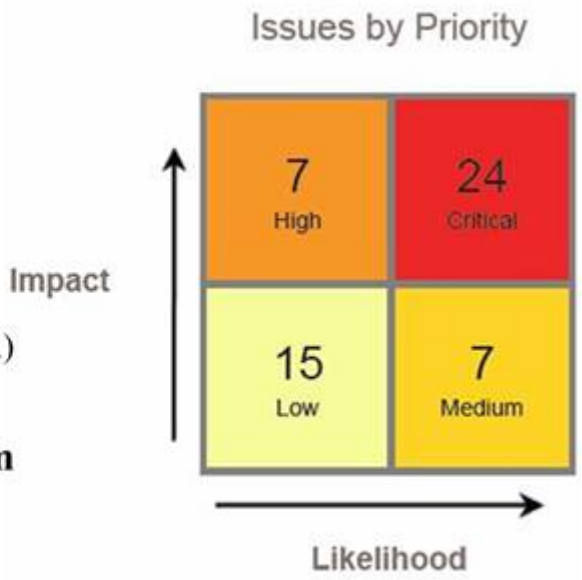
是以兩個座標值做為量化區分依據

(1) Likelihood

(問題準確度的可能性)

(2) Impact

(問題對部門或企業的影響衝擊性)



高準確度區: Critical / Medium

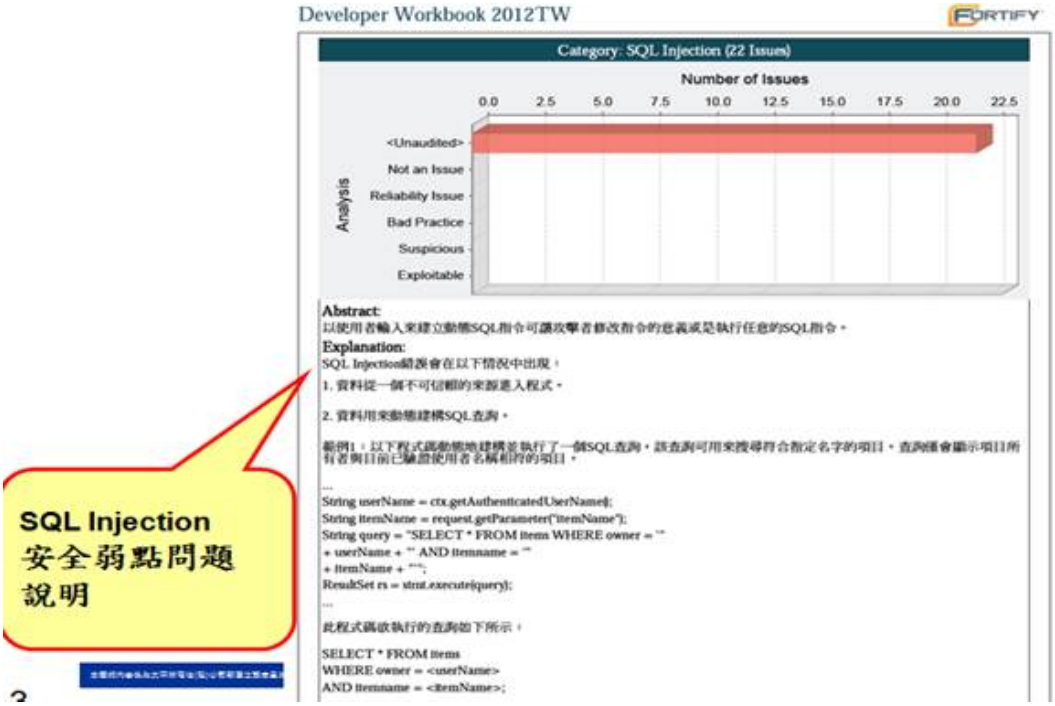
: High/ Low

凡有漏洞或品質問題的嫌疑跡象就列出的部分
必須要有資安人員再人工覆核是否有問題

五. 自動判斷問題嚴重程度

HP Fortify SCA 會將發現的安全弱點，依據弱點嚴重性(Impact)與弱點被揭露的可能性(Likelihood)，進行嚴重等級分類，可以讓稽核人員及開發人員明確清楚修補的優先順序。 ．

Likelihood：問題準確度的可能性。 ．
Impact ：問題對部門或企業的影響衝擊性

六. 完整詳細的應用程式弱點檢測報告

在 SCA 的弱點報表中，包含弱點的說明、修補的建議及弱點發生的位置(檔案名稱、程式行數)，讓開發人員可以快速對應到弱點的位置及修補的建議方法。