應用程式弱點整合平台

AVC 應用程式弱點整合平台
Application Vulnerability Correlation

為了能夠應對快速變動的軟體需求，軟體架構從過去的單體式架構（Monolithic）走向微服務架構（Microservices），軟體開發也由瀑布式開發（Waterfall）到敏捷式開發（Agile），軟體發行作業變得更為頻繁。如何落實持續整合與快速交付，且同時維持軟體品質，並排除軟體的資安疑慮，成為開發人員及維運人員共同面臨的挑戰。

AVC 利用「任務範本」來實現安全軟體開發流程，整合版本控管、源碼掃描、單元測試、靜態掃描、動態掃描、負載測試、壓力測試、軟體變更影響分析、建置及佈署工具，輔助軟體開發生命週期中的各項作業自動化，且可針對不同類型的專案彈性設計不同的流程。增加軟體開發流程中的安全強度，輔助企業輕鬆地落實 DevSecOps。

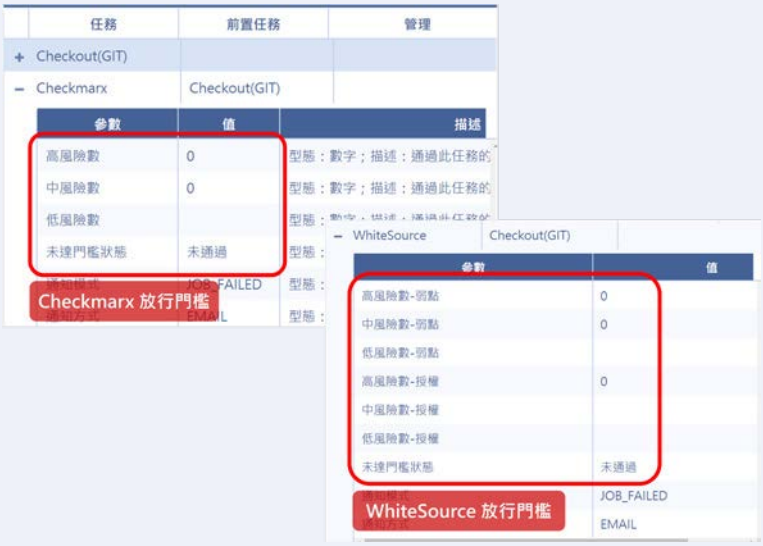
產品特色

安全軟體開發流程管理

提供彈性且有效率的安全軟體開發生命週期管理方式

安全自動化資安弱點檢測

自動化資安弱點檢測，減少人工操作之等待時間以及成本浪費。自訂放行門檻，加強流程中對軟體安全的控制強度及完整度



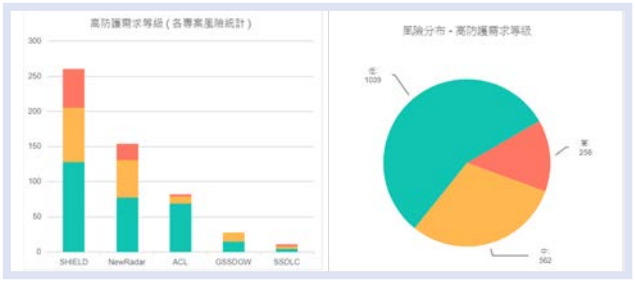
各項資安檢測結果彙整

各項資安檢測結果彙整，以提升自動化持續整合之管理綜效

主動回饋 / 資安通報機制

多角度管理報表

提供多角度管理報表，符合資安稽核之需求



系統效益

主管

1. 對各團隊、各專案之風險一目了然
2. 易於持續整合與持續交付之開發流程
3. 提供資安稽核之佐證資料

資安人員

1. 快速掌握公司面臨最大的資安風險
2. 輕鬆落實資安控管工作

維運人員

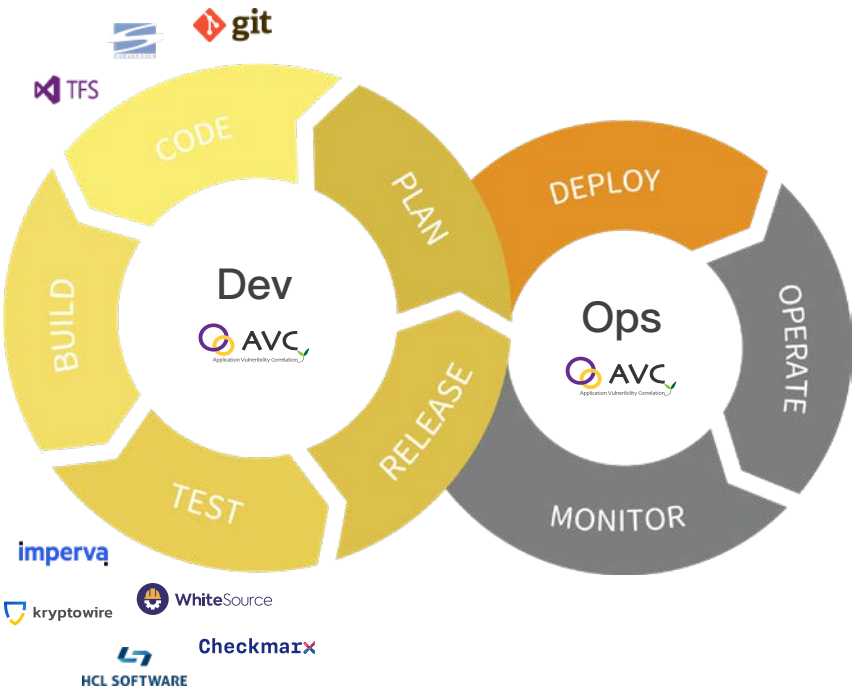
1. 有效且輕鬆地組態管理
2. 減輕佈署作業的負擔

開發人員

1. 自動化檢測，可更專注於開發工作
2. 即早發現程式問題
3. 修復弱點不再單槍匹馬，可參考不同專案及過去修復經驗

流程自動化

管理人員透過共用範本制定符合規範的安全軟體變更程序、以及定義每項流程中須執行的任務後，各專案可套用公版來啟動專案，再透過申請單來觸發一連串的自動化流程，涵蓋 Plan、Code、Build、Test、Release、Deploy，以一張申請單驅動 DevSecOps 各階段之作業進行，並管理流程中各項作業之產出。（例如：檢測報告）



主要規格

可整合的工具

需求管理
1.Jira

單元測試工具
1. GIT
2. SVN
3. TFS
4. Dimensions CM

單元測試
1. JUnit
2. NUnit

靜態掃描
1. Checkmarx
2. Mend
3. Fortify
4. SonarQube

動態掃描
1. HCL AppScan
2. Acunetix
3. WebInspect
4. kryptowire

功能 / 壓力 / 負載測試
1. Selenium
2. SeeTest
3. Visual Studio Load Test
4. JMeter

建置及佈署
1. Maven Build / MS Build / Docker Build
2. WebSphere Deploy /JBoss Deploy/Tomcat Deploy / IIS Deploy / Docker Deploy

其他
1. Arxan
2. Automation Anywhere
3. SFTP
4. Shared Folder
5. Call REST API
6. 執行腳本

掃描結果彙整

支援的標準
1. OWASP TOP 10 2013
2. OWASP TOP 10 2017
3. OWASP TOP 10 2021
4. CWE
5. 使用者自行組合定義

支援的報表
1. Checkmarx Report
2. Mend Vulnerability Report
3. Mend Due Diligence Report

軟硬體需求

1. **硬碟空間**：500 GB 以上（不含 OS，視專案大小）
2. **CPU**：2 Cores 以上
3. **RAM**：32 GB 以上
4. **作業系統**：Linux （CentOS 7 以上）

功能規格

系統管理

1. **共用任務範本**：制定多個標準流程，規範安全軟體開發週期之程序，供所有專案引用
2. **共用簽核設定**：根據共用任務範本，以角色的方式制定簽核流程，供所有專案引用
3. **系統參數**：設定共用的全域參數
4. **使用者管理**：使用者帳號、密碼及基本資料維護
5. **使用者群組管理**：使用者分群維護

專案管理

1. **權限管理**：管理該專案之各角色使用者，亦可設定為使用者群組，決定該專案的管理角色等
2. **任務範本**：可引用共用任務範本，自訂任務參數，亦可自訂專案範本
3. **組態設定**：針對專案中共用的組態進行管理及設定
4. **簽核設定**：可引用共用任務範本所設定的簽核流程，也可根據專案自訂的範本定義簽核流程

申請單

1. **執行任務**：可執行手動或自動執行及重啟各項任務
2. **通知機制**：任務執行完成或失敗時，以及簽核流程當中，自動通知任務執行者或簽核者，可自行設定關閉或開啟通知
3. **簽核紀錄**：記錄各關卡簽核資訊