



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。

III 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

The screenshot shows a software interface for managing development processes. At the top, there's a navigation bar with tabs like '任務範本' (Task Template), '定義標準上版流程' (Define Standard Release Process), and '階段' (Phase). Below this, a table lists '任務範本名稱' (Task Template Name) as 'A 類專案上版流程' (A-class Project Release Process), '描述' (Description) as '公司公版 - A 類專案上版流程', and '管理' (Management) with a green checkmark. A yellow arrow points from the '描述' field to a section titled '訂定共用規範' (Define Common Standards). Another green button labeled '定義各個子流程' (Define Sub-processes) is also visible. The main content area is titled '階段- 白箱檢測' (Phase - Whitebox Testing) and contains a table of tasks:

任務	前驟	後驟	操作
+ Checkout(GIT)	1 版本控管：取得 Source Code		編輯 刪除
+ Checkmarx	2 SAST: 源碼檢測		編輯 刪除
+ WhiteSource	3 SCA：開放原始碼安全檢測		編輯 刪除
+ GitPush(SCM)	Checkmarx, WhiteSource		編輯 刪除

Below this is another section titled '階段- 黑箱檢測'.

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

This screenshot shows the configuration of security audit parameters. It includes sections for 'Checkout(GIT)' and 'Checkmarx'. The 'Checkmarx' section has a table of parameters:

參數	值	描述
高風險數	0	型態：數字；描述：通過此任務的
中風險數	0	型態：數字；描述：通過此任務的
低風險數	0	型態：數字；描述：通過此任務的
未達門檻狀態	未通過	型態：

Below this is a red box labeled 'Checkmarx 放行門檻' (Checkmarx Release Threshold) with values: 'JOB_FAILED' and 'EMAIL'. To the right, there's another table for 'WhiteSource' with similar parameters and a red box labeled 'WhiteSource 放行門檻' (WhiteSource Release Threshold) with values: 'JOB_FAILED' and 'EMAIL'.

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

This screenshot displays a summary of security audit results. It shows a table titled '程式清單' (Program List) with columns for '程式名稱' (Program Name) and '掃描工具' (Scanning Tools). The table lists various Java files and their corresponding analysis tools used:

程式名稱	掃描工具
gssdgw/core/web/api/CustomGsonMessageBodyProvider.java	Checkmarx
gssdgw/portal/web/controller/FirstEncryptController.java	Checkmarx
gssdgw/portal/web/controller/TempMetaApiController.java	Checkmarx
gssdgw/core/service/impl/MetadataFileServiceImpl.java	Checkmarx
gssdgw/portal/web/controller/MetadataController.java	Checkmarx
bootstrap-3.3.7-3.3.13.js	Checkmarx Whitesource
gssdgw/portal/web/controller/MetadataFieldController.java	Checkmarx
angular-1.5.8.js	Checkmarx Whitesource
gssdgw/core/schedule/BaseScheduledJobFactory.java	Checkmarx
gssdgw/core/jobs/ScheduledJobFactory.java	Checkmarx

At the bottom, there are pagination controls: '首頁', '< 上一頁', '1', '下一頁 >', '末頁', '10 每頁', and '顯示條目 1 - 10 共 867'.

主動回饋 / 資安通報機制

The screenshot displays the Checkmarx system interface with several notifications overlaid:

- 簽核通知**: AVC 申請單簽核通知, 日期: 2022年1月28日 上午 9:42.
- 申請單完成通知**: AVC 任務執行結果未通過通知, 日期: 2022年1月28日 上午 9:42.
- 任務失敗通知**: AVC 任務執行失敗通知, 日期: 2022年1月18日 下午 1:29.

下方是系統配置界面，顯示了任務失敗的門檻設置和通知方式：

參數	高風險數 中風險數 低風險數 未達門檻狀態
通知模式	JOB_FAILED
通知方式	EMAIL

註：型態：字串，描述：通知

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



III 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

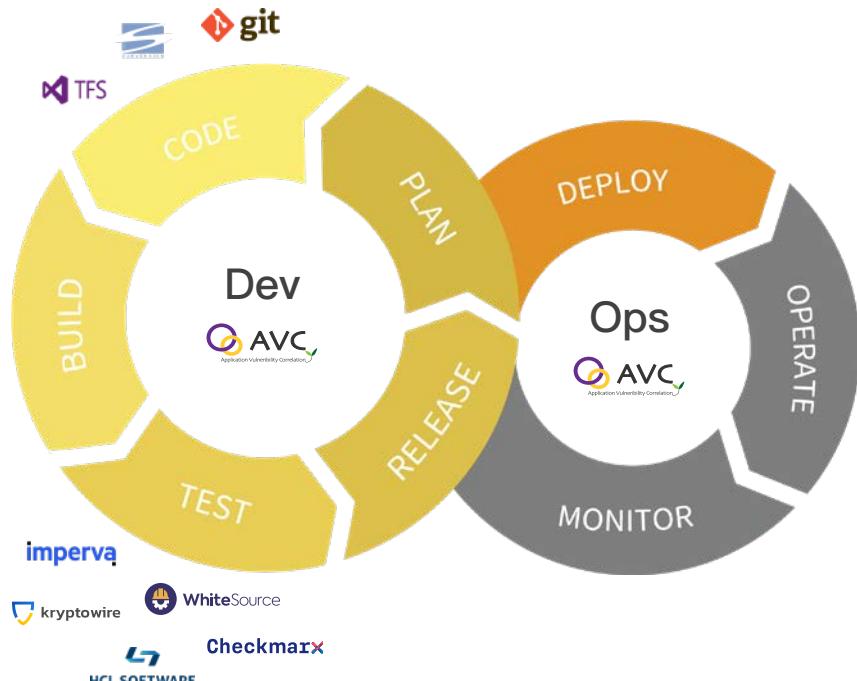
1. 有效且輕鬆地組態管理
2. 減輕佈署作業的負擔

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

III 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）



III 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