「數位臺灣 資安共行」
- DevSecOps 資安檢驗，失敗的關鍵因數探討...

單位：叡揚資訊

報告人：陳志雄 總經理

日期：2022/07/20

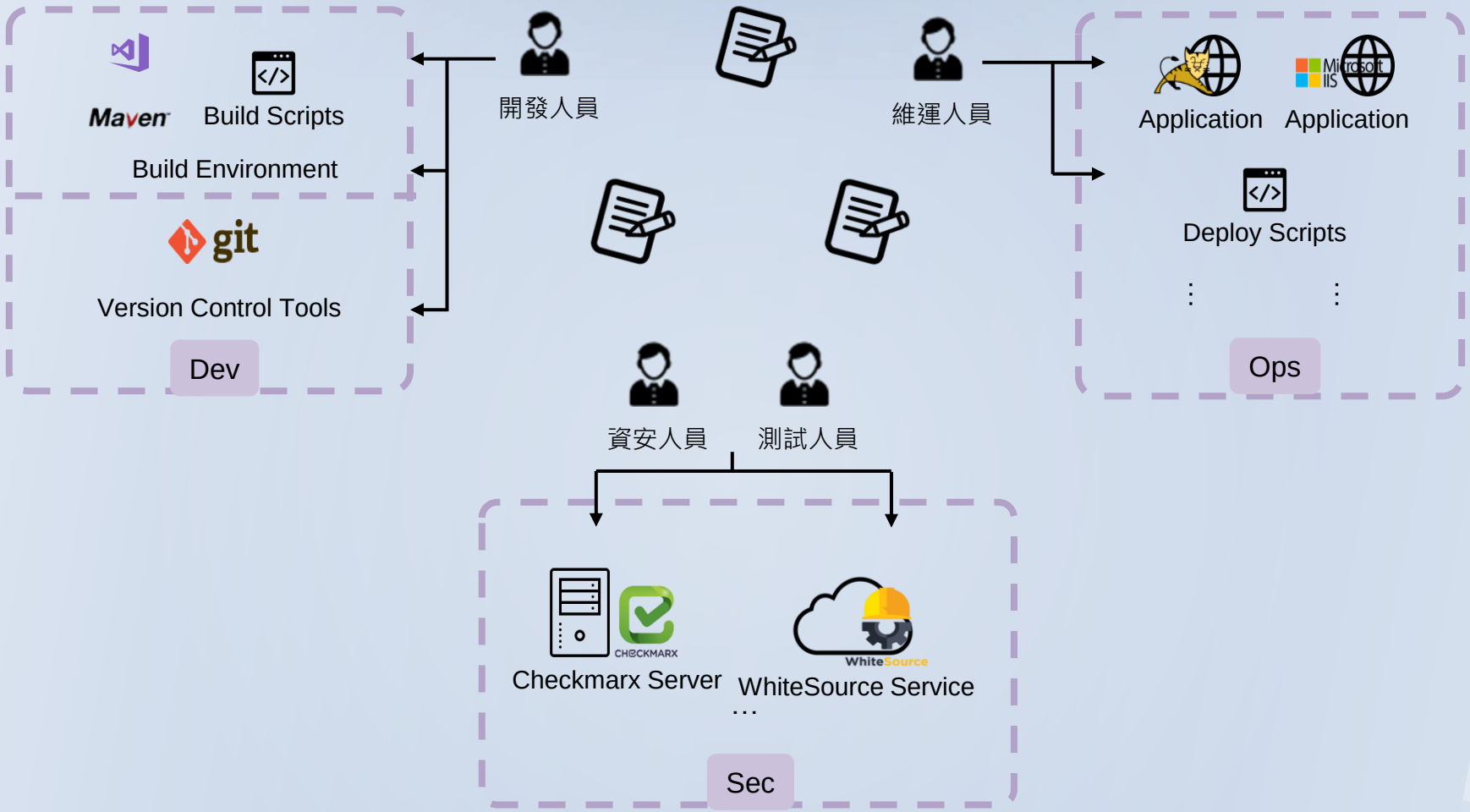
電郵：Bruce_chen@gss.com.tw

Agenda

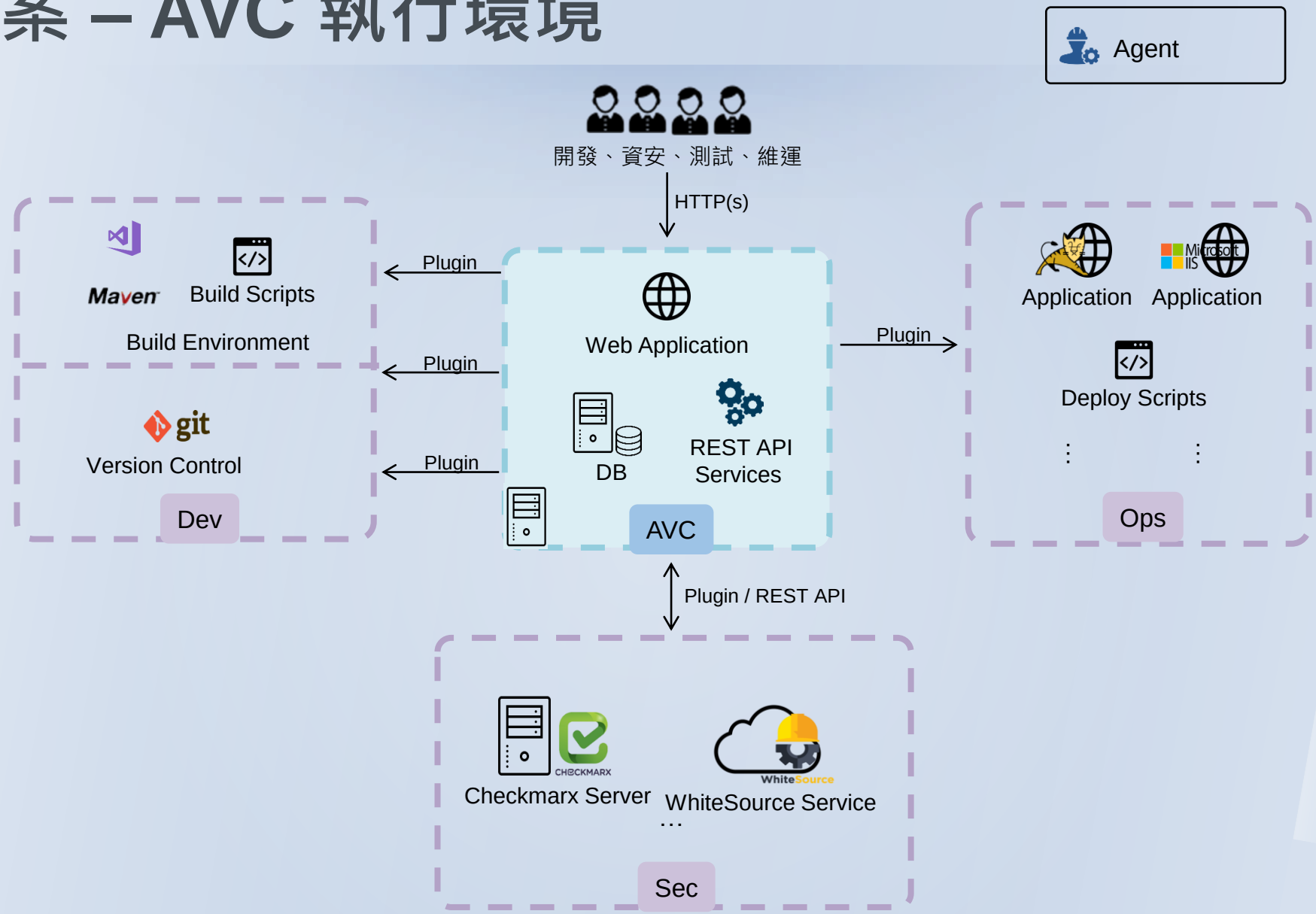
- DevSecOps 觀念介紹
- 實際案例與功能分享
- 規劃/導入/建置 建議

DevSecOps 觀念介紹

現況與挑戰 - 一般執行環境



解決方案 – AVC 執行環境



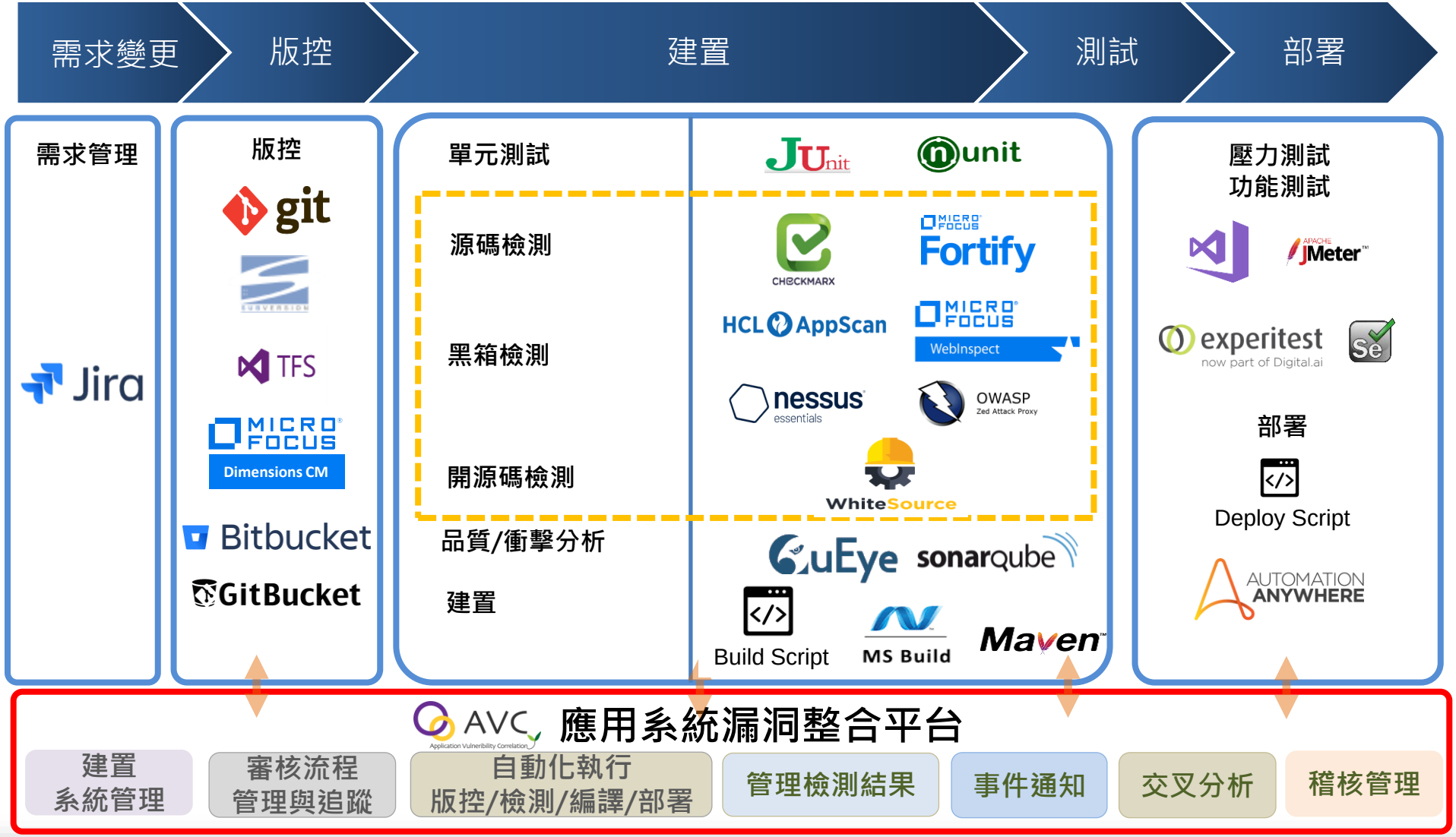
現況與問題

△ 導入多樣化工具，整合成本高

△ 無法自動控管合規性

△ 查核紀錄監管資訊不易

Secure Software Development Life Cycle (SSDLC)



整合運作平台

制定安全上版流程

- 共用範本
- 環境參數
- 放行門檻
- 簽核設定
- 節點/主機設定

系統管理員

專案(系統) 管理

- 權限設定
- 任務範本
- 組態設定
- 簽核設定

專案管理者

申請單

- 自動化作業
- 排程設定
- 事件通知
- 自動化合規
- 簽核紀錄

專案成員

放行人員

實際案例與功能分享

AVC
Application Vulnerability Correlation

應用系統合規流程
自動化集中管理平台

平台特色

AVC
Application Vulnerability Correlation

簡易、彈性的流程設計

持續擴充的整合工具清單

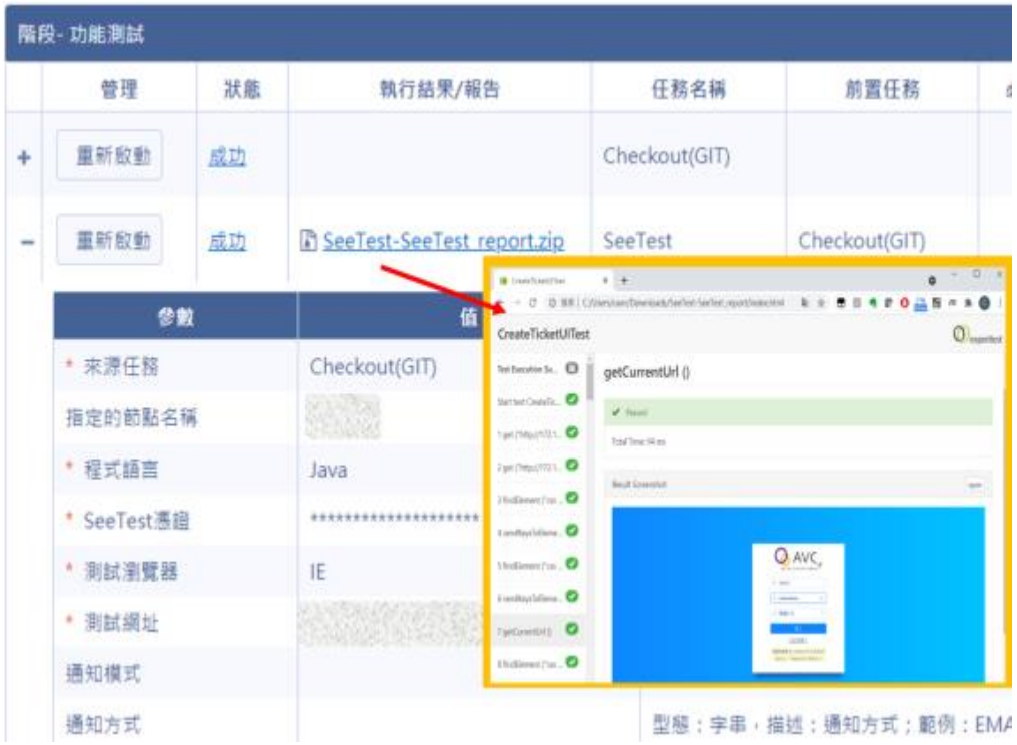
平台特色

執行任務 – SAST / SCA / DAST (白箱/開源授權/黑箱) (Web/APP)

平台特色

AVC
Application Vulnerability Correlation

執行任務 – 功能測試



版更記錄與上版後服務品質確認

平台特色

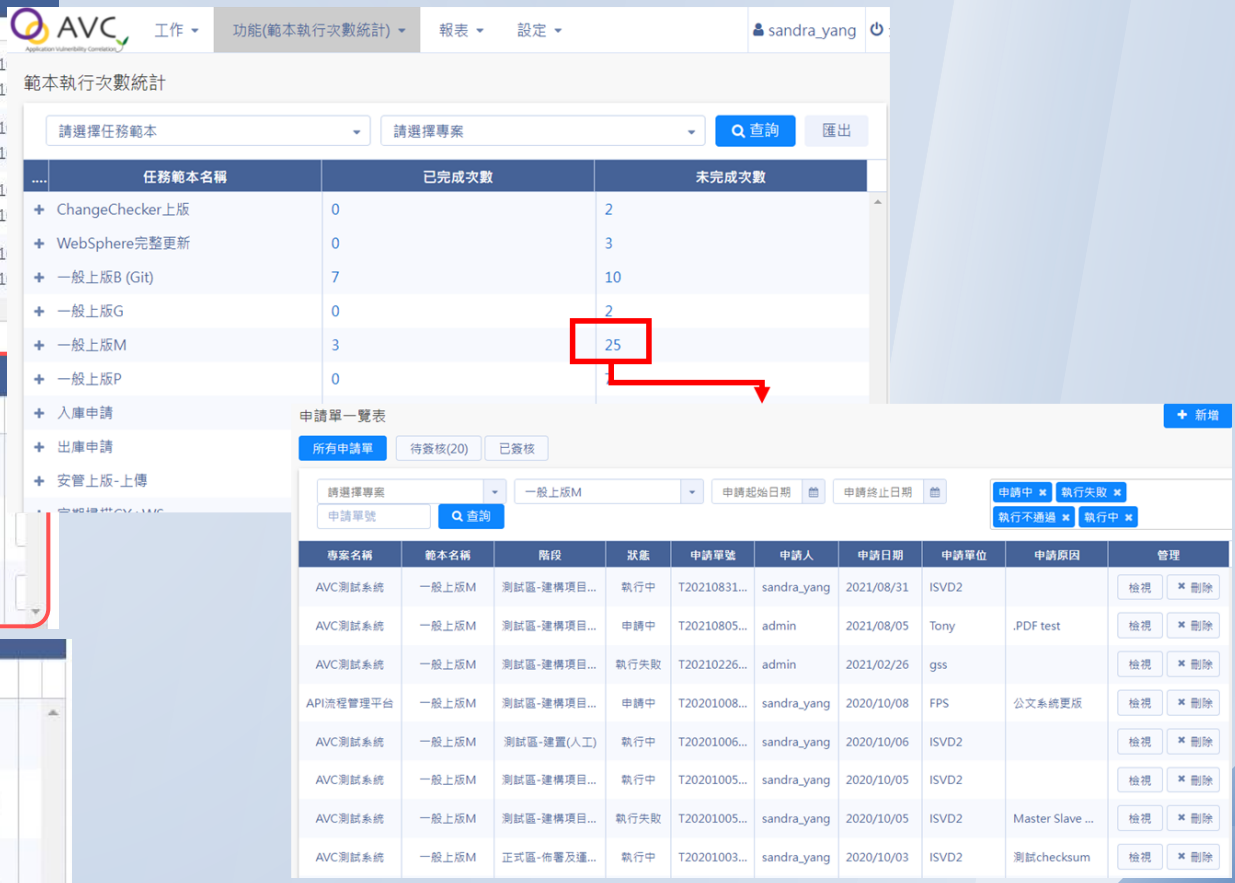
深度整合資安檢測工具，自動控管合規性

平台特色

AVC Application Vulnerability Correlation

輕鬆追蹤稽核軌跡

上版次數統計



整合GitLab Webhook提升自動化作業效率

› 自動觸發檢測作業

主動回饋/通報機制

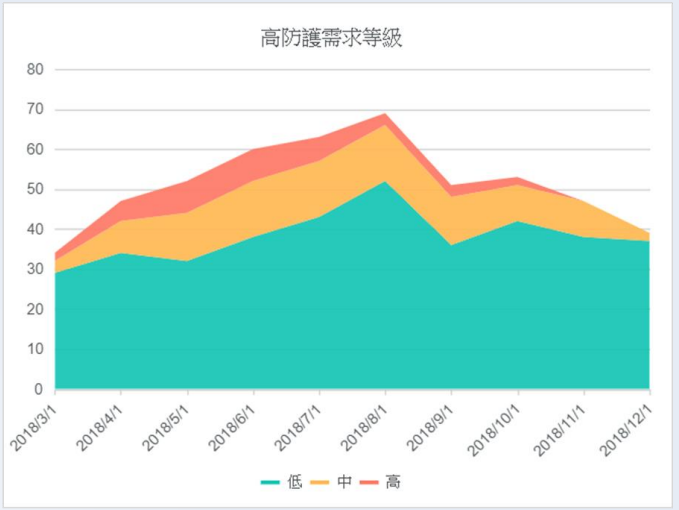
- 透過通知機制設定，提升軟體開發生命週期中各項作業之反應效率

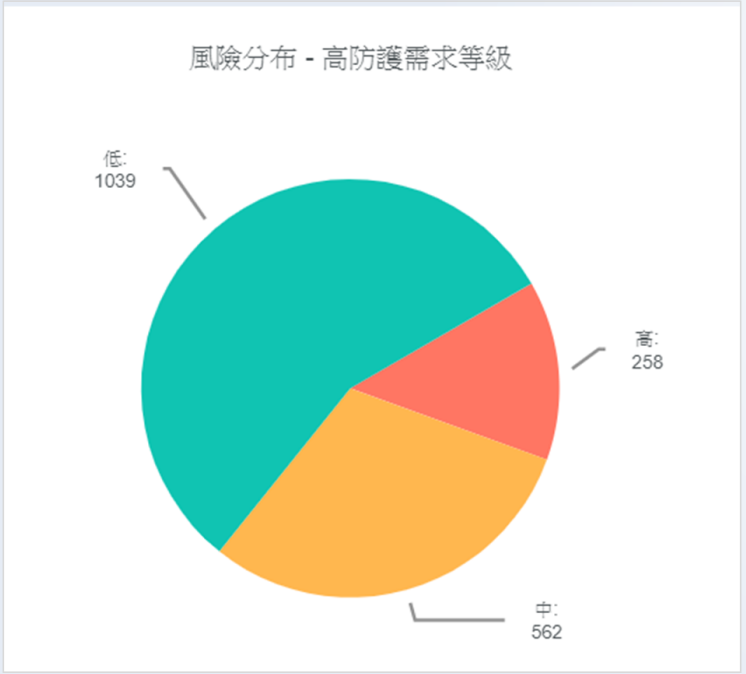
掃描結果彙整

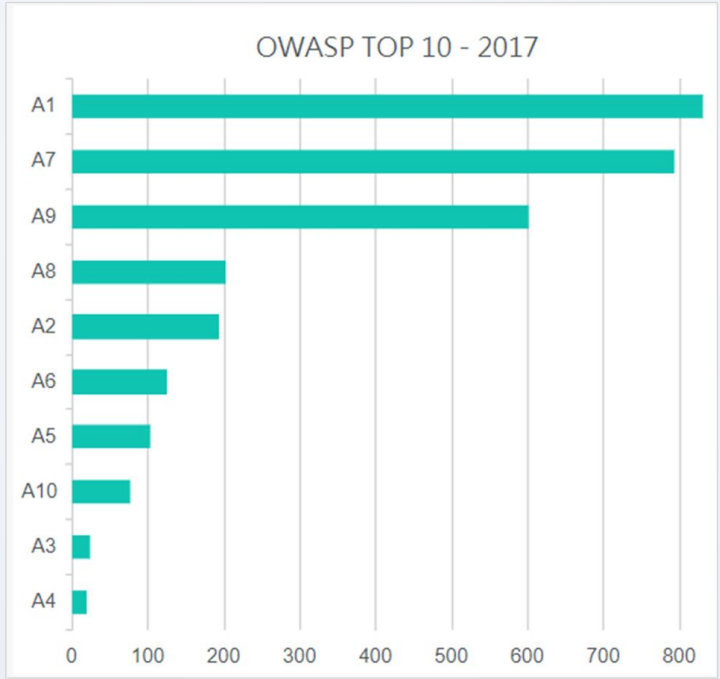
- 彙整**不同工具**檢測結果於同一報表，管理者可**直覺掌握**組織風險概況

專案名稱	最新檢測結果
GSSDGW-元資料管理系統	Checkmarx WhiteSource
SSDLC-上版流程管理系統	Checkmarx WhiteSource
ACL-權限控管系統	Checkmarx WhiteSource
SHIELD-屏蔽系統	Checkmarx WhiteSource
NewRadar-HR系統	Checkmarx WhiteSource

1 2 1 - 5 條 共 6 條數據

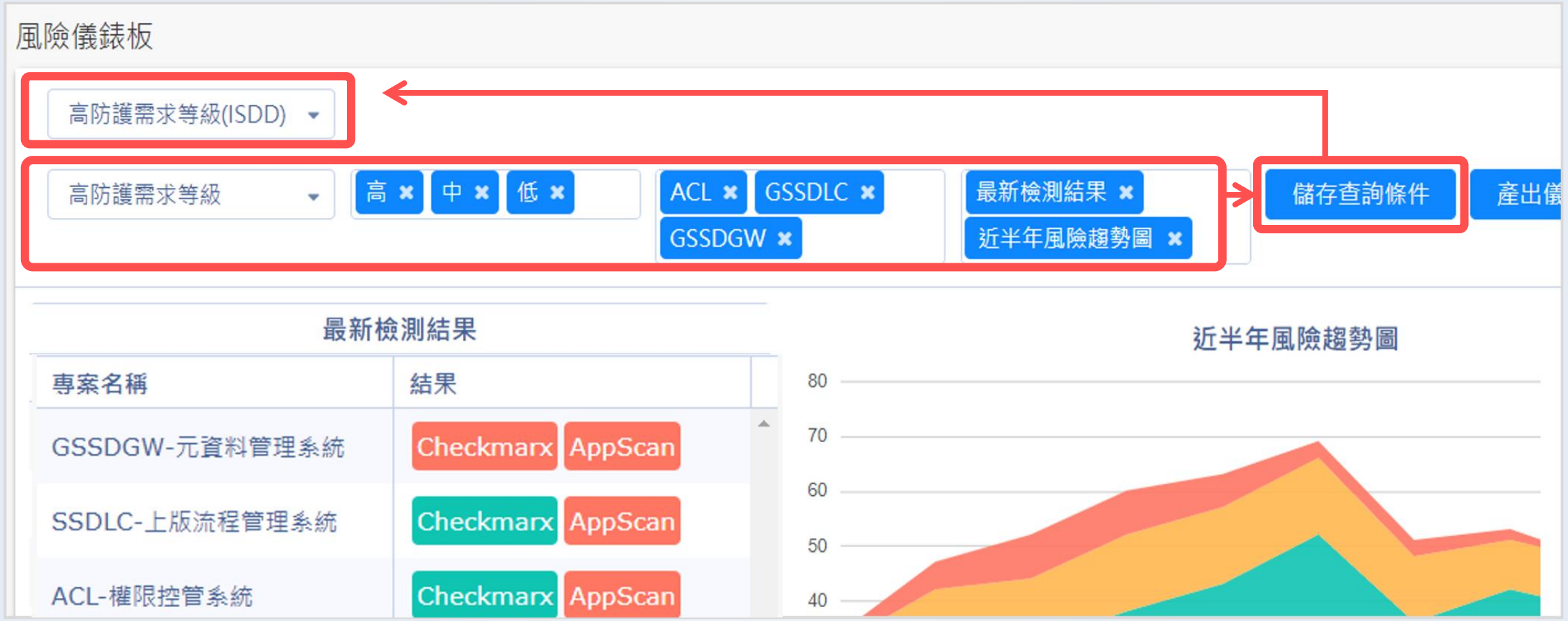






個人儀錶板

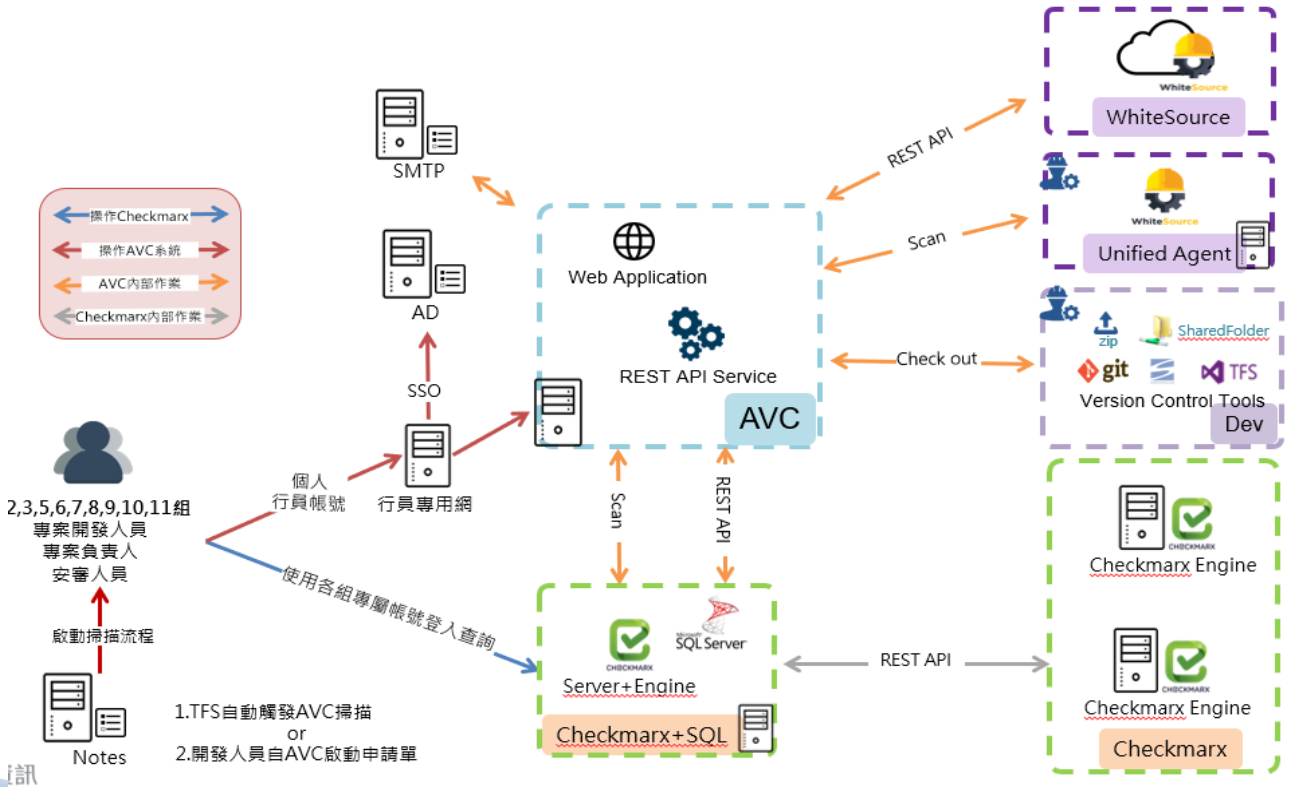
- 建立個人常用儀錶板，快速掌握不同視角之統計圖表



建置專案實績-銀行

- **流程自動化**
- **需同時執行多項檢測工具**

- 整合既有系統(Notes、Jenkins、VMS)
- 舊系統流程轉換至AVC
- 整合 SVN、TFS、Shared Folder、GitLab
- 整合 Checkmarx、WhiteSource
- 導入 **96個** 系統，**333個** 子系統
- 每個月最高完成近 **550次** 檢測作業



AVC X 自動化 X 資安工具

省時

- 同時檢測 WhiteSource 與 Checkmarx
- 批次觸發定期掃描作業

省力

- 自動化操作版控及檢測工具、自動化上版，減少人員學習及操作負擔
- 自動控管合規性

高效率

- 稽核紀錄一目瞭然
- 常用 Report 可在一個平台同時取得，不需登多個產品下載

建置專案實績 - 政府

- 改善程序以符合稽核規範
  - **程式碼前後不一致**
  - **上版程式碼未經資安檢測**

- 根據單位 ISMS 定義標準變更上版程序
- 整合既有建置、部署環境
- 整合SVN、Checkmarx
- 輔導資訊中心**全數系統**(36個)導入合規上版程序

- ✓ **安全檢核**
- ✓ **測試通過紀錄與檢核**
  - ✓ 保留變更的測試紀錄
- ✓ **測試區源碼組態控制**
  - ✓ 提供測試與正式源碼一致性查核基準
- ✓ **測試區目的碼組態控管**
  - ✓ 不會有人為多增或變化佈署目的碼
- ✓ **正式源碼一致性控制**
  - ✓ 由系統轉為正式源碼，避免未授權變更內容
- ✓ **正式區目的碼組態管控**
  - ✓ 不會有人為多增或變化佈署目的碼
- ✓ **提供緊急上版機制**
- ✓ **保留人工作業彈性**

AVC 導入成果及效益

改善表單簽核流程與效率，減少人為失誤與SVN版控人力配置

- AVC自動執行SVN入館
- AVC自動產出差異報告

確保目的程式碼與原始程式碼一致

- 測試區程式碼與目的碼入版控
- AVC自動將測試區程式碼抄寫至正式區
- 目的碼透過SFTP傳送並增加checksum檢查碼機制

加強稽核紀錄之完整性與不可否認性

- 以系統記錄作業執行人員與時間
- 所有作業皆保留完成佐證及相關記錄

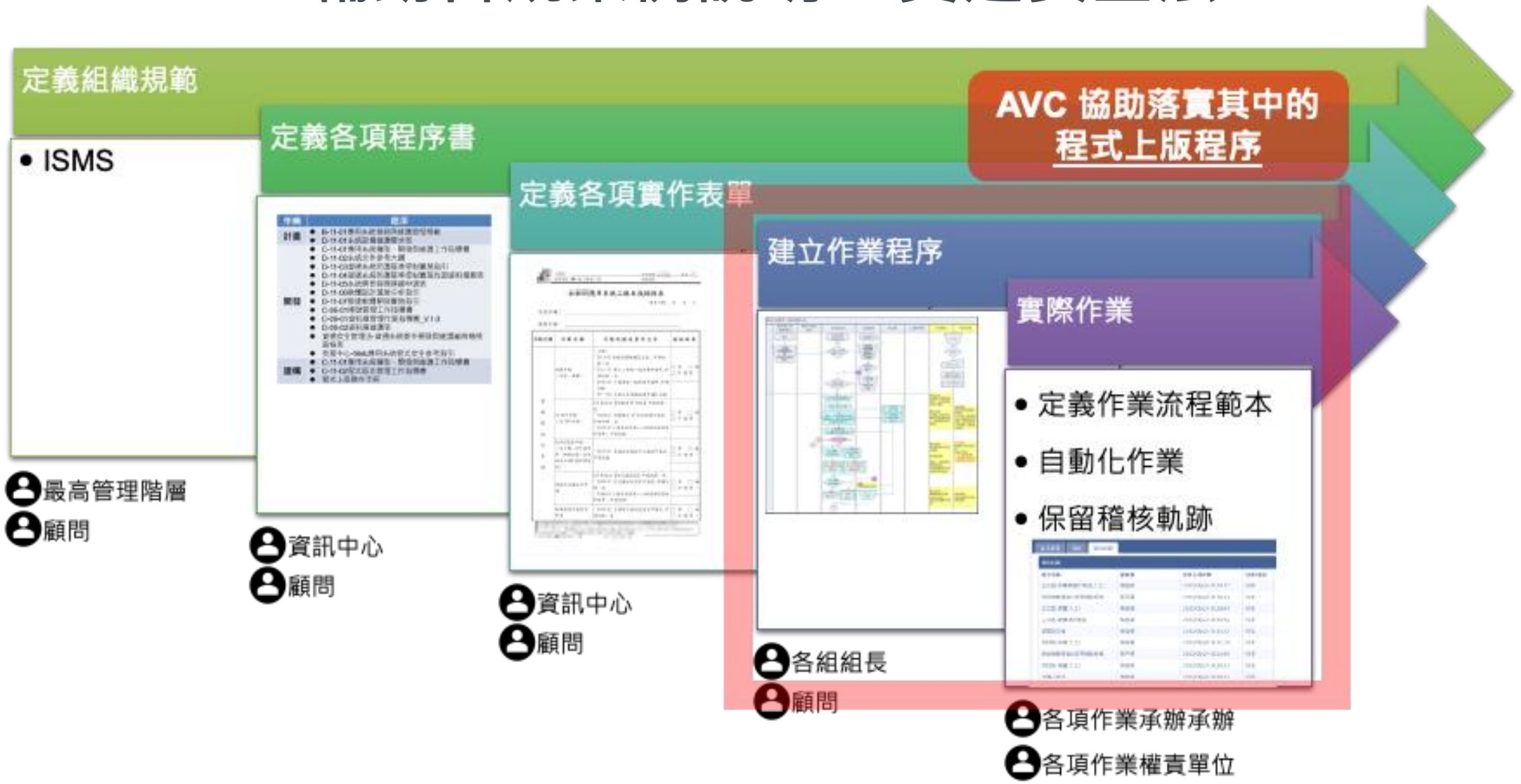
更版程式經過資安檢測

- 將安全檢核作業併入AVC上版流程，確保安全檢測有效性

整合自動建構與部署優化

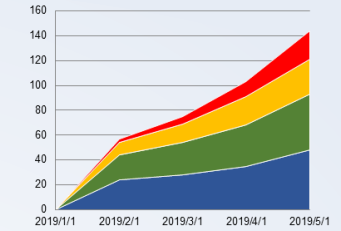
規劃/導入/建置 建議

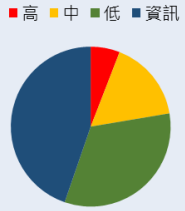
GSS-AVC 輔助合規案例說明 – 資通安全法



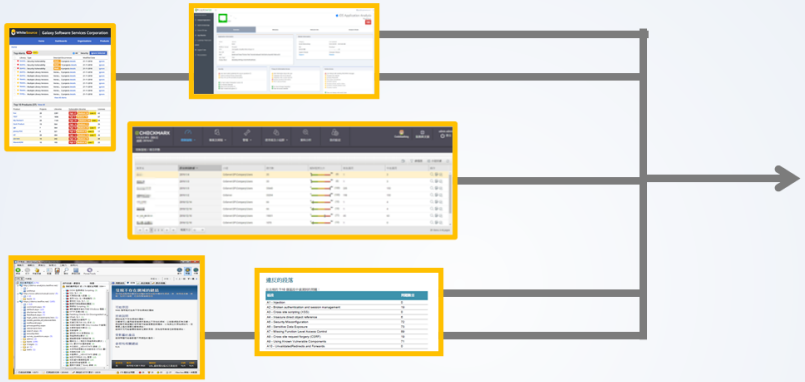
AVC整合運作平台

多角度
多維度
分析與管理





彙總
檢測結果



風險等級	OWASP
• 高風險 • 中風險 • 低風險	• A1: Injection • A2: Broken Au.. • A3: Sensitive D..

CWE	自訂標準
• CWE-78: Impr.. • CWE-89: SQL.. • ...	• 外部專案 • 內部專案 • 單位自行控管專案

流程管理
/ 自動化
資安檢測

AVC 使用效益

主管

- 對各團隊、各專案之風險統計、趨勢一目了然
- 易於推動持續整合與持續交付之軟體開發流程
- 提供稽核之佐證資料

資安人員

- 快速掌握公司面臨最大的資安風險
- 輕鬆落實資安控管工作

維運人員

- 有效且輕鬆地組態管理
- 減輕佈署作業的負擔

開發人員

- 自動化檢測，可更專注於開發工作
- 即早發現程式問題

AVC 應用程式弱點整合平台

規劃導入建議 -

- 勿太過理想 – 設定範圍與強度
  - 範圍太大
  - 自動化程度太高
  - 過度追求零風險
  - 全產品導入,無客製整合空間
- 工具+整合+顧問 - 內部流程精進
- 有機體平台 – 定期檢視,逐漸完整
  - 完成測試後之目的碼，在緊急時可能先行更新正式主機，事後才另行申請。
  - 部分系統更新頻率高，無明確訊息分析是需求經常變動或是變更不完整。

Why GSS?

成熟並經驗證的解決方案

政府、金融組織都選擇 叡揚資訊

協助他們落實應用系統上線程序合規

專業團隊

大型銀行、政府建置經驗
經市場驗證的解決方案

產品化導入

品質保證
確保專案時程
持續優化、更新與擴充

完善機制

提升管理效率
保留流程變更彈性
深度整合檢測工具
解決上版作業風險
減輕稽核作業負擔

AVC 優勢

標準產品方式導入

具大中小型企業建置導入經驗

輔助企業落實 DevSecOps

- **彈性制定作業流程**
- 整合既有Dev、Ops環境
- 整合版控工具
- 整合資安檢測工具
- 支援自動化建置及佈署
- 集中管理各項工作的報表及產出
- **提供簽核機制**
- **稽核記錄留存**
- **具報表資料彙整能力**

GSS 叡揚資訊
Galaxy Software Services

感謝聆聽 ~

國家產業創新獎
卓越中堅企業獎

www.gss.com.tw

GSS 叡揚資訊

Vital 雲端服務家族