

「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

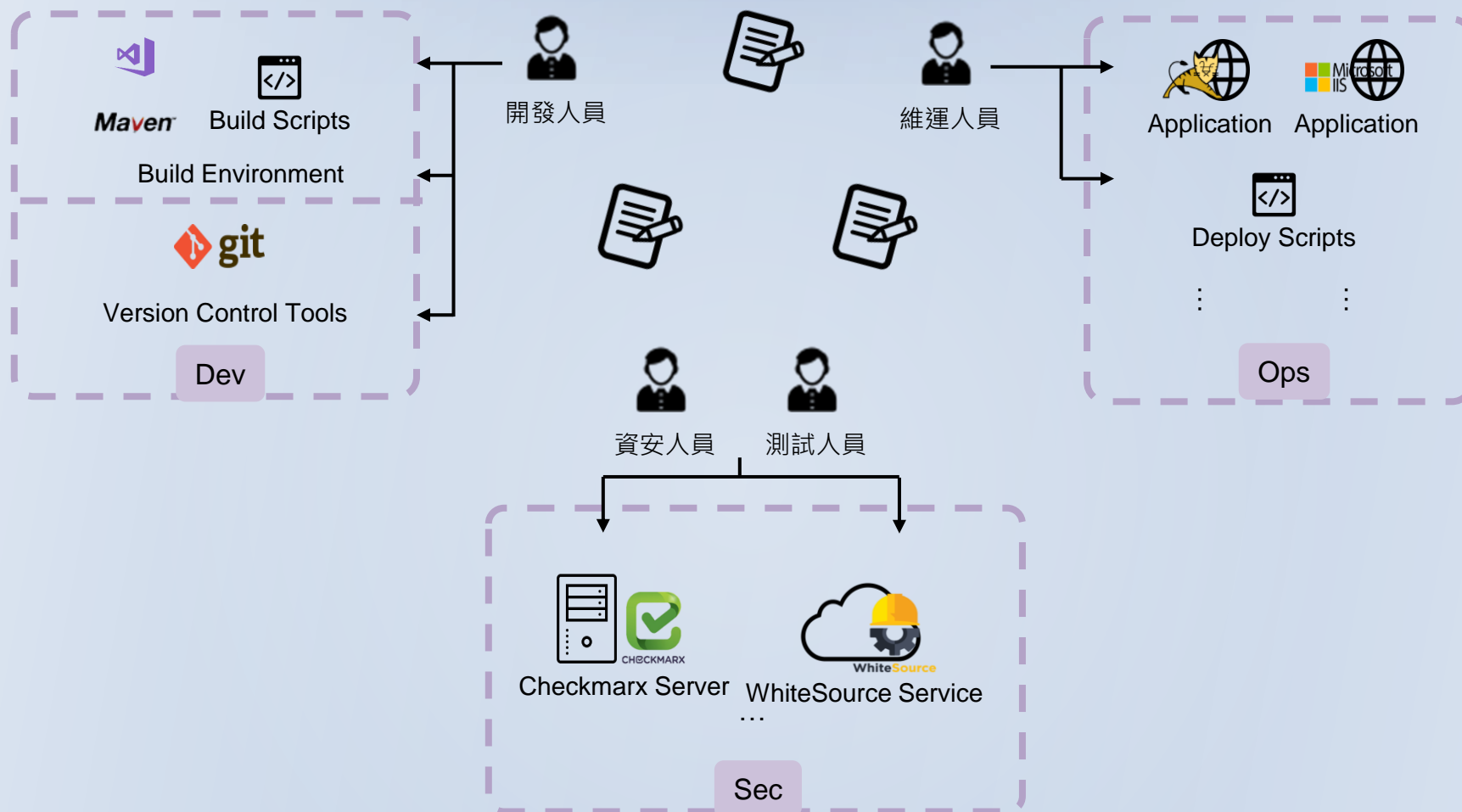


Agenda

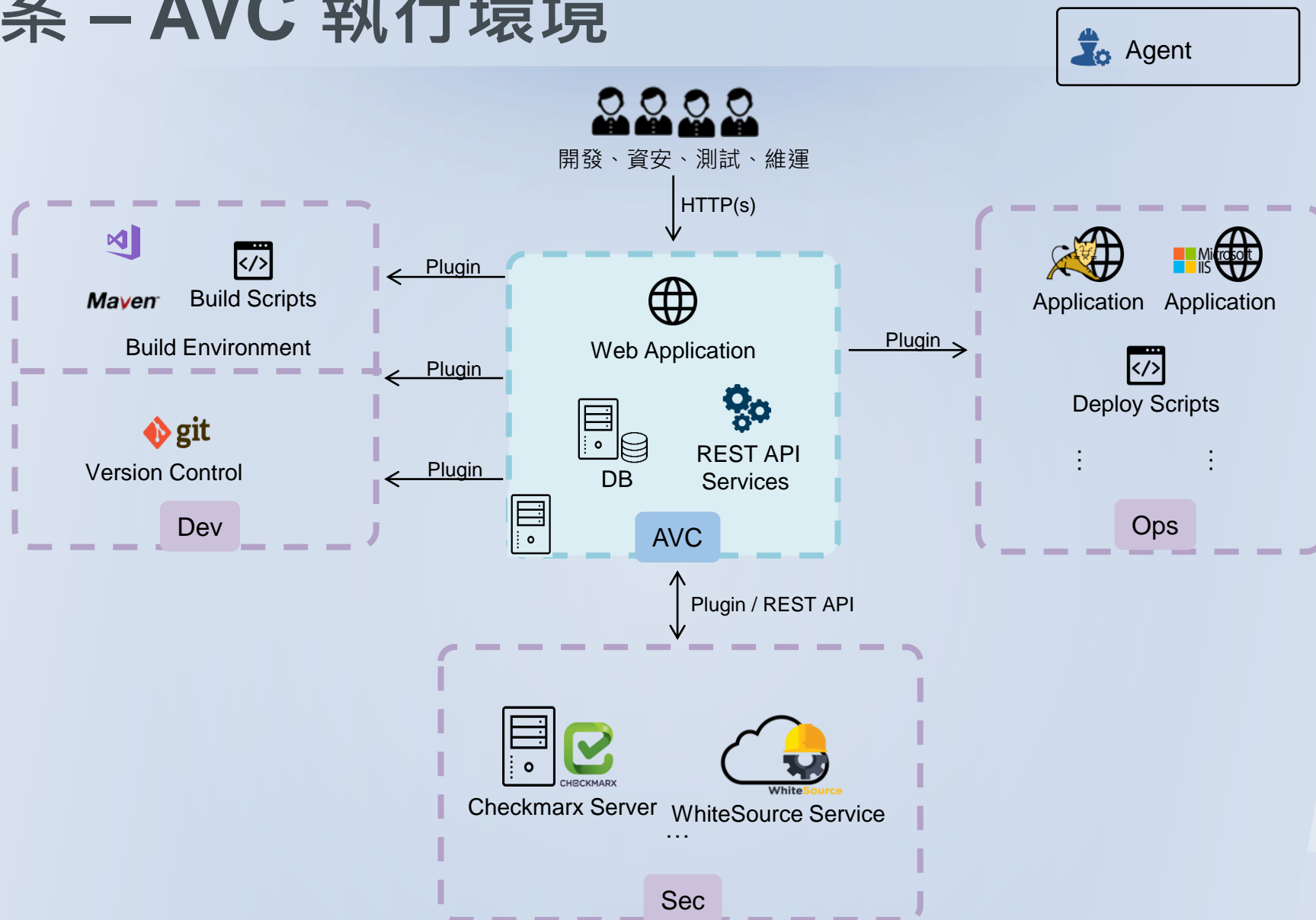
- › DevSecOps 觀念介紹
- › 實際案例與功能分享
- › 規劃/導入/建置 建議

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



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



應用系統合規流程
自動化集中管理平台

平台特色

簡易、彈性的流程設計

✓ 任務範本

定義標準上版流程

✓ 階段

定義各個子流程

✓ 任務

設定各階段中要進行的作業及環境參數

任務範本名稱	描述	管理
自動化測試上版	含源碼檢測、單元測試、壓力測試	訂定共用規範

階段- 檢測及佈署		
任務	描述	前置任務
+ Checkout(GIT)	1 版本控管：取得 Source Code	
+ Checkmarx	2 SAST：源碼檢測	Checkout(GIT)
+ WhiteSource	3 SCA：開放原始碼安全檢測	Checkout(GIT)
+ MSBuild	4 編譯/執行單元測試	Checkmarx, WhiteSource
+ IISDeploy	5 部署	MSBuild

階段- 黑箱測試與壓力測試		
任務	描述	前置任務
+ AppScan	6 DAST：黑箱測試	
+ VS Load Test	7 壓力測試	

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)

The screenshot displays the AVC platform interface, which is divided into several sections:

- Basic Information (基本資料):** Includes project details like name, version, and scan type.
- Task Execution (執行任務):** A table showing the status of various tasks (e.g., "重新啟動" - Restart) and their results (e.g., "成功" - Success).
- Report Management (檢測後報告自動帶回管理):** A section for managing reports generated by the scan.
- Summary (Summary):** A detailed view of the scan results, including a list of issues and their severity.

The **Summary** section is highlighted with a yellow box and contains the following data:

Issue Type	Number of Issues
Cross-Site Scripting	1
Link to Non-Existent Domain Found	1
Flushing Through URL Redirection	1
SQL Injection	4
Cross-Site Request Forgery	6
Inadequate Account Lockout	1
Link Injection (Facilitates Cross-Site Request Forgery)	6
Missing Secure Attribute in Encrypted Session (SSL) Cookie	1
Flushing Through Frames	7
Session Identifier Not Updated	1
Autocomplete HTML Attribute Not Disabled for Password Field	3
Body Parameters Accepted in Query	3
Catchable SQL Page Found	17
Cookies with Insecure or Improper or Missing SameSite attribute	2
Credit Card Number Pattern Found (Vuln)	4
Database Error Pattern Found	6
Direct Access to Administration Page	1
Enumeration Not Enabled	1
Insecure "OPTIONS" HTTP Method Enabled	2
Missing or insecure "X-Content-Type-Options" header	1
Missing or insecure "X-RSS-Protecton" header	1
Missing or insecure Cross-Framework Scoping Defense	1

平台特色

執行任務 – 功能測試

階段- 功能測試

管理	狀態	執行結果/報告	任務名稱	前置任務
+ 重新啟動	成功		Checkout(GIT)	
- 重新啟動	成功	SeeTest-SeeTest report.zip	SeeTest	Checkout(GIT)

參數	值
* 來源任務	Checkout(GIT)
指定的節點名稱	
* 程式語言	Java
* SeeTest標組	*****
* 測試瀏覽器	IE
* 測試網址	
通知模式	
通知方式	



型態：字串，描述：通知方式；範例：EMA



版更記錄與上版後服務品質確認

返回清單 | 範本執行次數統計 - APIM自動上版(完成)

專案名稱	範本名稱	狀態	申請單號	異動案號	申請日期	本次版號	管理
APIM	APIM自動上版	執行完成	T2021070203	H-109-0151_08828_B1001	2021/07/02	1.0.9	檢視 服務 交關
APIM	APIM自動上版	執行完成	T2021061811	H-109-0150_08828_B1001	2021/06/18	1.0.8	檢視 服務 交關
APIM	APIM自動上版	執行完成	T2021061811	H-109-0150_08828_B1001	2021/06/18	1.0.8	檢視 服務 交關

✓ 上版後服務品質確認
整合Dynatrace查看上版前後的服務品質變化

平台特色

深度整合資安檢測工具，自動控管合規性

任務	前置任務	管理
+ Checkout(GIT)		編輯
- Checkmarx		編輯

Checkmarx放行門檻

參數	值
高風險數	\${high-risk-standard}
中風險數	\${medium-risk-standard}
低風險數	
未達門檻狀態	
通知方式	

WhiteSource放行門檻

參數	值	型態
高風險數-弱點	\${high-risk-standard-vulnerabi...}	型
中風險數-弱點	\${medium-risk-standard-vulne...}	型
低風險數-弱點	\${low-risk-standard-vulnerabili...}	型
高風險數-授權	\${high-risk-standard-dueDilig...}	型
中風險數-授權	\${medium-risk-standard-dueD...}	型
低風險數-授權	\${low-risk-standard-dueDilige...}	型
未達門檻狀態	\${status-when-job-fails}	型
通知方式	\${notifcation-type}	型

管理	狀態	執行結果/報告	任務	前置任務
重新啟動	未通過	ACL-WhiteSource_report	WhiteSource	Checkout(GIT)

參數	值	型態
* 產品名稱	APIPM	型態：字串，描述：WhiteS
* 專案名稱	ACL	型態：字串，描述：WhiteS
高風險數-弱點	0	型態：數字；描述：通過此
中風險數-弱點	0	型態：數字；描述：通過此
低風險數-弱點		型態：數字；描述：通過此
高風險數-授權	0	型態：數字；描述：通過此
中風險數-授權	0	型態：數字；描述：通過此
低風險數-授權		型態：數字；描述：通過此
未達門檻狀態	未通過	型態：字串；描述：未達通
通知模式	TICKET COMPLETE	型態：字串，描述：通知模

平台特色

輕鬆追蹤稽核軌跡

返回清單 | 申請單明細 - T20210810002 : AVC_DEMO_SERVICE-AVC測試系統

所有申請單 待審核(77) 已審核

基本資料 項目 簽核紀錄

+	重新啟動	成功		GitPush-程式碼	腳本執行-建置	是	admin	實際執行: 2021/08/1 實際完成: 2021/08/1
+	重新啟動	成功		GitTag-程式碼	GitPush-程式碼	是	admin	實際執行: 2021/08/1 實際完成: 2021/08/1
+	重新啟動	成功		GitPush-目的碼	GitTag-程式碼	是	admin	實際執行: 2021/08/1 實際完成: 2021/08/1
+	重新啟動	成功		GitTag-目的碼	GitPush-目的碼	是	admin	實際執行: 2021/08/1 實際完成: 2021/08/1

執行人員及時間

階段-應用系統佈署

管理	狀態	執行結果/報告	任務名稱	前置任務	必要執行	啟動人員	實際執行時間
+	重新啟動	成功	Checkout(Git)-目的碼		是	admin	實際執行: 2021/08/10 13:30:53 實際完成: 2021/08/10 13:31:06
+	重新啟動	成功	Checkout(Git)-佈署腳本	Checkout(Git)-目的碼	是	admin	實際執行: 2021/08/10 13:31:13 實際完成: 2021/08/10 13:31:16
+	重新啟動	成功	腳本執行-佈署	Checkout(Git)-佈署腳本	是	admin	實際執行: 2021/08/10 13:31:23 實際完成: 2021/08/10 13:31:42

執行狀態及Log

檢測報告

管理	狀態	執行結果/報告	任務名稱	前置任務
+	重新啟動	成功	Checkout(Share Folder)	
+	重新啟動	成功	Checkmarx	Checkout(Share Folder)
+	重新啟動	成功	WhiteSource	Checkout(Share Folder)

上版次數統計



工作

功能(範本執行次數統計)

報表

設定

sandra_yang

範本執行次數統計

請選擇任務範本

請選擇專案

查詢

匯出

任務範本名稱	已完成次數	未完成次數
+ ChangeChecker上版	0	2
+ WebSphere完整更新	0	3
+ 一般上版B (Git)	7	10
+ 一般上版G	0	2
+ 一般上版M	3	25
+ 一般上版P	0	
+ 入庫申請		
+ 出庫申請		
+ 安管上版-上傳		

申請單一覽表

所有申請單 待審核(20) 已審核

請選擇專案

申請單號

查詢

一般上版M

申請起始日期

申請終止日期

申請中

執行失敗

執行不通過

執行中

專案名稱	範本名稱	階段	狀態	申請單號	申請人	申請日期	申請單位	申請原因	管理
AVC測試系統	一般上版M	測試區-建構項目...	執行中	T20210831...	sandra_yang	2021/08/31	ISVD2		檢視 刪除
AVC測試系統	一般上版M	測試區-建構項目...	申請中	T20210805...	admin	2021/08/05	Tony	.PDF test	檢視 刪除
AVC測試系統	一般上版M	測試區-建構項目...	執行失敗	T20210226...	admin	2021/02/26	gss		檢視 刪除
API流程管理平台	一般上版M	測試區-建構項目...	申請中	T20210108...	sandra_yang	2020/10/08	FPS	公文系統更新	檢視 刪除
AVC測試系統	一般上版M	測試區-建置(人工)	執行中	T20210106...	sandra_yang	2020/10/06	ISVD2		檢視 刪除
AVC測試系統	一般上版M	測試區-建構項目...	執行中	T20210105...	sandra_yang	2020/10/05	ISVD2		檢視 刪除
AVC測試系統	一般上版M	測試區-建構項目...	執行失敗	T20210105...	sandra_yang	2020/10/05	ISVD2	Master Slave ...	檢視 刪除
AVC測試系統	一般上版M	正式區-佈署及運...	執行中	T20210103...	sandra_yang	2020/10/03	ISVD2	測試checksum	檢視 刪除

整合GitLab Webhook提升自動化作業效率

› 自動觸發檢測作業



Menu

ISBG > gssdlc-acl > Commits

master gssdlc-acl

14 Jan, 2022 10 commits

 **george_chou** authored 2 days ago





工作(申請單一覽表) 功能 報表

[返回清單](#) 申請單明細 - T1110114003 : ACL-權限控管系

所有申請單 待簽核(0) 已簽核

基本資料 項目 簽核紀錄

專案資料

專案名稱

權限控管系統

前次版本

階段- 源碼檢測(Git、WS、CX)

管理	狀態	執行結果/報告	任務名稱	前置任務	必要...	啟動人員	實際執行時間
+	成功		Checkout(GIT)		是	george_chou	實際執行 : 2022/01/14 09:39:18 實際完成 : 2022/01/14 09:39:32
+	未通過	 ACL-Checkmarx_re...  ACL-Checkmarx_re...	Checkmarx	Checkout(...	是	george_chou	實際執行 : 2022/01/14 09:39:43 實際完成 : 2022/01/14 09:54:40
+	未通過	 ACL-WhiteSource_r...  ACL-WhiteSource_p...  ACL-WhiteSource_p...	WhiteSource	Checkout(...	是	george_chou	實際執行 : 2022/01/14 09:39:43 實際完成 : 2022/01/14 09:42:57



[Testing!] AVC 任務執行結果未通過通知

2022年1 月14日 上午 9:54

寄件者: noreply@gss.com.tw

收件者: Sandra Yang (楊佳穎) George Chou (周孚陽)

您好:
申請單號 T1110114003下列任務執行結果未通過, 請至系統進行確認, 謝謝!
專案: ACL
階段: 源碼檢測(Git、WS、CX)
任務: Checkmarx
[http://\[redacted\]/avc/page/tickets#/ticketId/71](#)

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

The screenshot displays the 'AVC 申請單' (AVC Request Form) interface. On the left, a sidebar contains navigation links: '所有申請單', '返回清單', and '基本資料'. The main content area shows a table with columns for '指定的節點名稱' (Specified Node Name) and '狀態' (Status). The table lists several nodes: 'Checkmarx 帳號', 'Checkmarx 密碼', 'Checkmarx 預設集合', '高風險數', '中風險數', '低風險數', and '未達門檻狀態'. The '未達門檻狀態' row shows '執行成功' (Execution Successful). Below the table, a red box highlights the '通知模式' (Notification Mode) and '通知方式' (Notification Method) settings, with a red arrow pointing to them from the text '設定通知方式及模式' (Set notification method and mode). To the right of the table, four example notification emails are shown, each with a yellow bell icon and a title: '簽核通知' (Approval Notification), '申請單完成通知' (Request Form Completion Notification), '任務失敗通知' (Task Failure Notification), and 'AVC 申請單簽核通知' (AVC Request Form Approval Notification). The emails are from 'noreply@gss.com.tw' and sent to 'sandra yang'. The '任務失敗通知' email includes a link to 'FetchJenkinsConsoleLog.txt (1.3 KB)' and a list of failed tasks.

簽核通知

AVC 申請單簽核通知
寄件者: noreply@gss.com.tw
收件者: sandra yang

您好:
申請單號 20190408012 已
<http://172.16.5.180:8084/g>

申請單完成通知

AVC 申請單執行完成通知
寄件者: noreply@gss.com.tw
收件者: sandra yang

您好:
申請單號 T20190904-1 已執行完成。請至系統進行確
專案: ISVD1
<http://localhost>

任務失敗通知

AVC 任務執行失敗通知
寄件者: noreply@gss.com.tw
收件者: sandra yang

[FetchJenkinsConsoleLog.txt \(1.3 KB\)](#) [下載](#) | [公事包](#) | [移除](#)

您好:
申請單號 T20190904-5 下列任務執行失敗，請至系統進行確認，謝謝！
專案: ISVD2_APP_2G
階段: WhiteSource 掃描 (指定路徑)
任務: WhiteSource(離線掃描)
<http://localhost:8084/avc-portal-web/page/tickets#/ticketId/6>

狀態：字串，描述：通知方式；範例：EIM

設定通知方式及模式

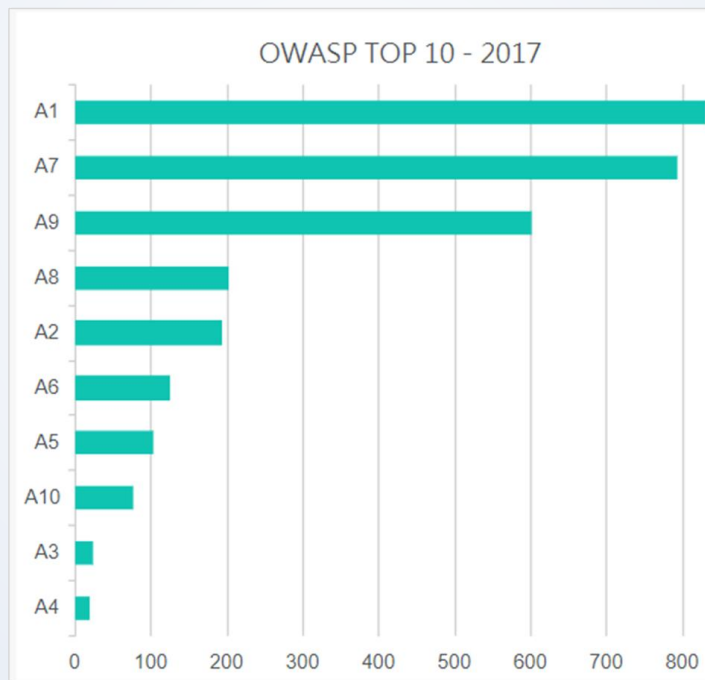
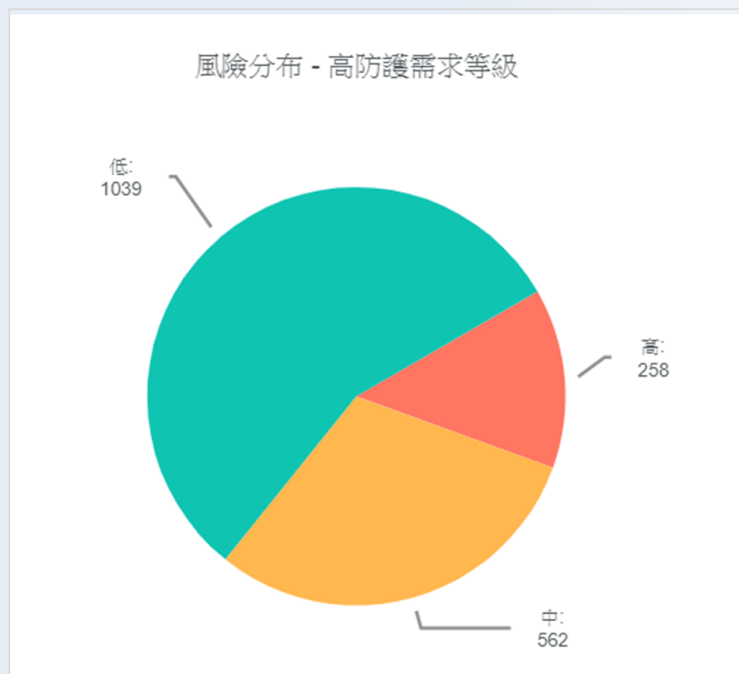
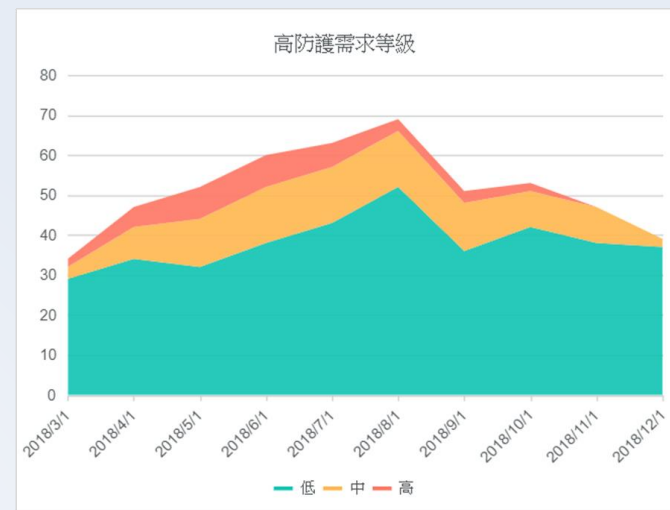
指定的節點名稱	狀態
* Checkmarx 帳號	admin@
* Checkmarx 密碼	*****
* Checkmarx 預設集合	OWASP
高風險數	0
中風險數	0
低風險數	0
未達門檻狀態	執行成功
通知模式	JOB_FAILED
通知方式	EMAIL

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

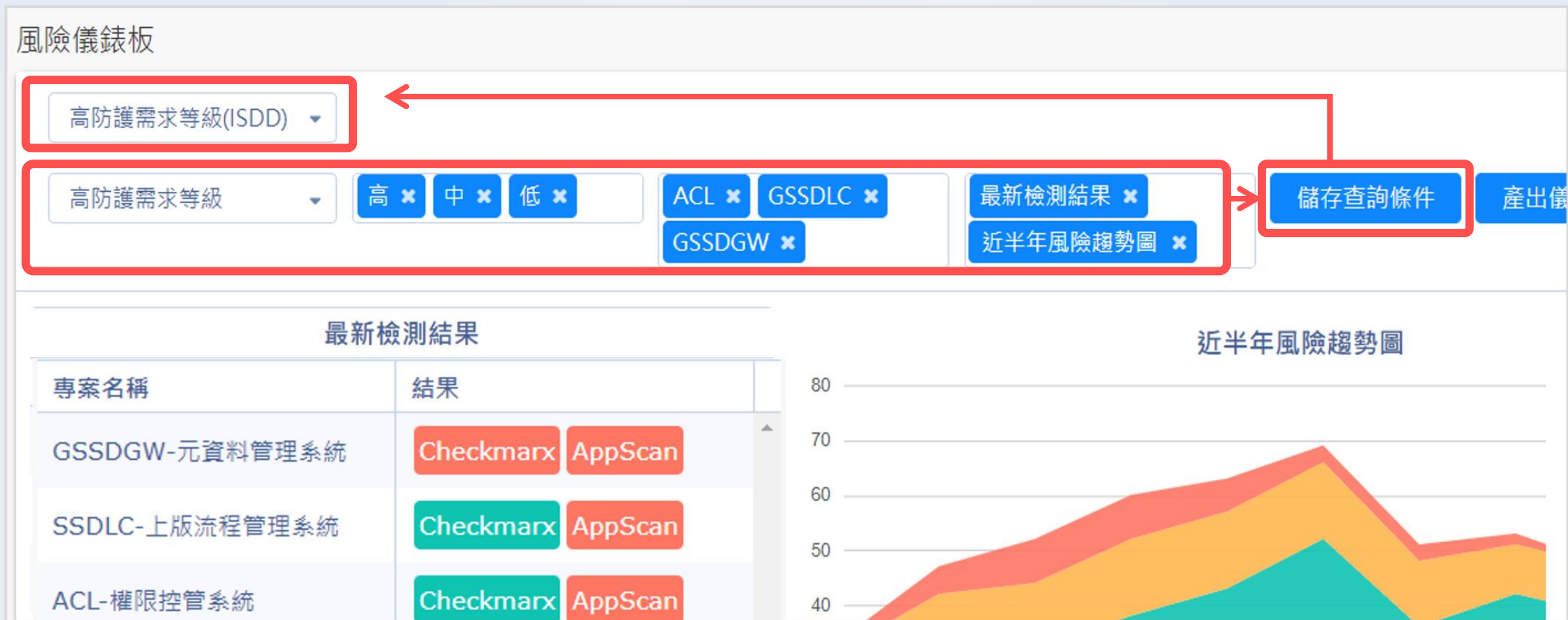
專案名稱	最新檢測結果
GSSDGW-元資料管理系統	Checkmarx WhiteSource
SSDLC-上版流程管理系統	Checkmarx WhiteSource
ACL-權限控管系統	Checkmarx WhiteSource
SHIELD-屏蔽系統	Checkmarx WhiteSource
NewRadar-HR系統	Checkmarx WhiteSource

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



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

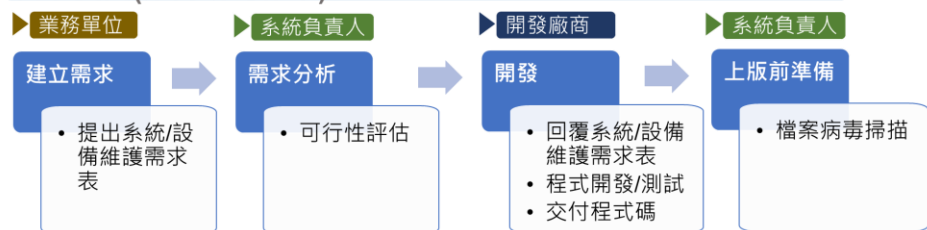
- 稽核紀錄一目瞭然
- 常用 Report 可在一個平台同時取得，不需登多個產品下載

建置專案實績 - 政府

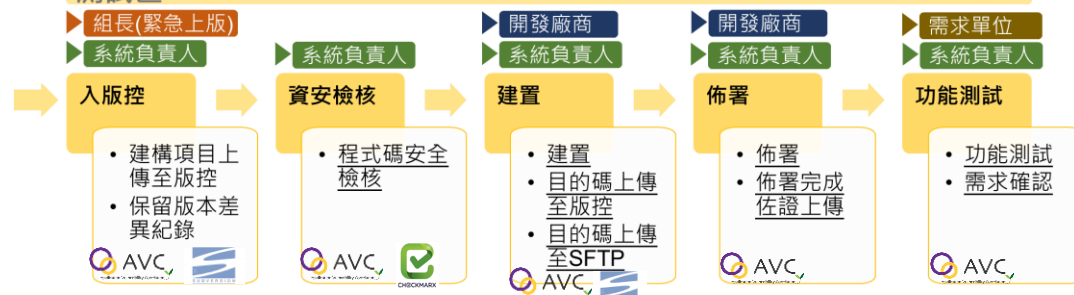
- 改善程序以符合稽核規範
 - 程式碼前後不一致
 - 上版程式碼未經資安檢測

- 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

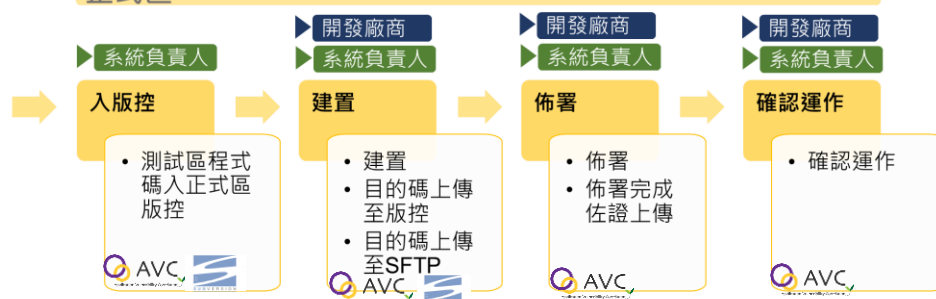
需求變更(維持既有作業)



測試區



正式區



- ✓ 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

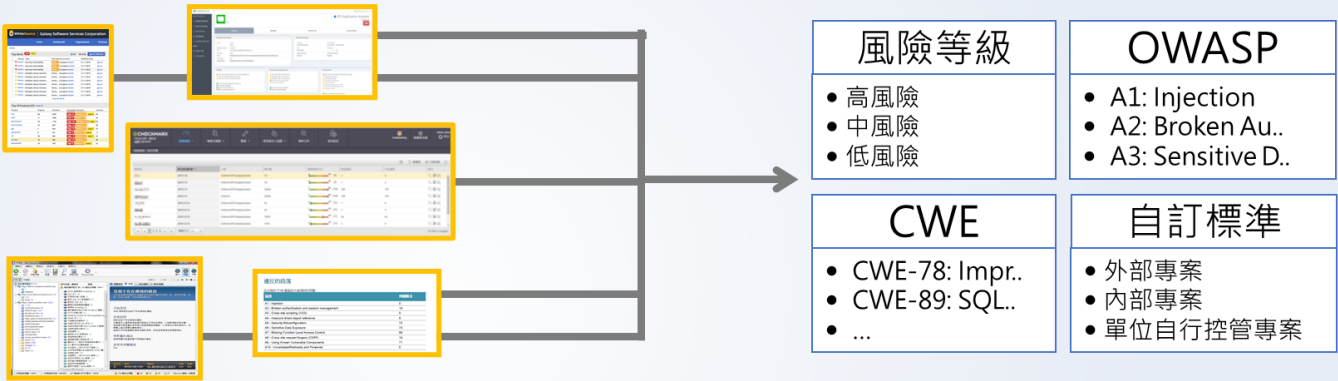
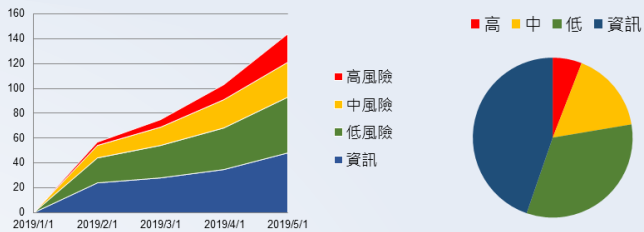
規劃/導入/建置 建議

AVC整合運作平台

多角度
多維度
分析與管理

彙總
檢測結果

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 叻揚資訊
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



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