

HCLSoftware



無死角的應用安全檢測 打造完美 Secure DevOps

*Fast, Accurate, Agile
Security Testing*

Kevin Chia
Application Security Technical Advisor

應用程式中 嚴重弱點會產生後果

1.25億

新台幣

資料外泄平均成本
近三年增加15%

83%

的組織百分比
發生過一次以上資安事件

277

識別資料外泄的平均天數

51%

計畫增加資安預算

維護「應用安全」的複雜性不斷提高



容器 Container/ Docker
使用的普及化



Open API/ GraphQL
開發多樣化



攻擊目標與區域
深度與廣度



法令法規遵循
金融、政府、上市上櫃、ISO



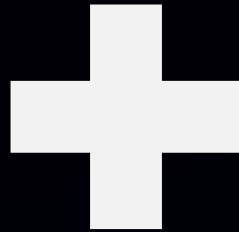
攻擊多樣化
第三方套件、伺服器服務、API Secret、等

僅靠「傳統的應用安全掃描」無法有效守護「應用安全」

從「技術」到「管理」—所需的安全措施

『技術』

網頁弱點掃描
原始碼檢測
Open API
API Secret
Fuzz Testing
第三方開源元件



『管理』

Secure DevOps
CI/CD整合
弱點追蹤與管理
生命開發週期整合
法令法規遵循

沒有超人這樣的「資安人員」...

資安超人



『技術』

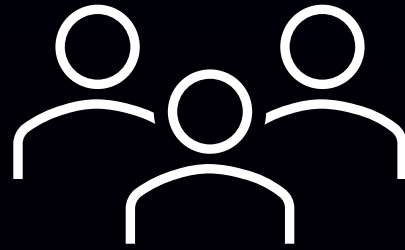
網頁弱點掃描
原始碼檢測
Open API
API Secret
Fuzz Testing
第三方開源元件

『管理』

Secure DevOps
CI/CD整合
弱點追蹤與管理
生命開發週期整合
法令法規遵循

你需要的是「工具」和「自動化」

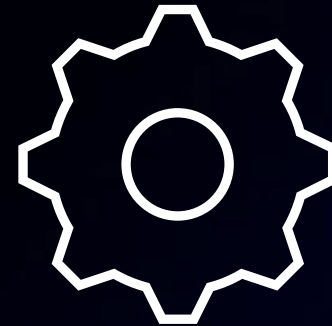
資安超人
一般資安人員



工具: HCL AppScan

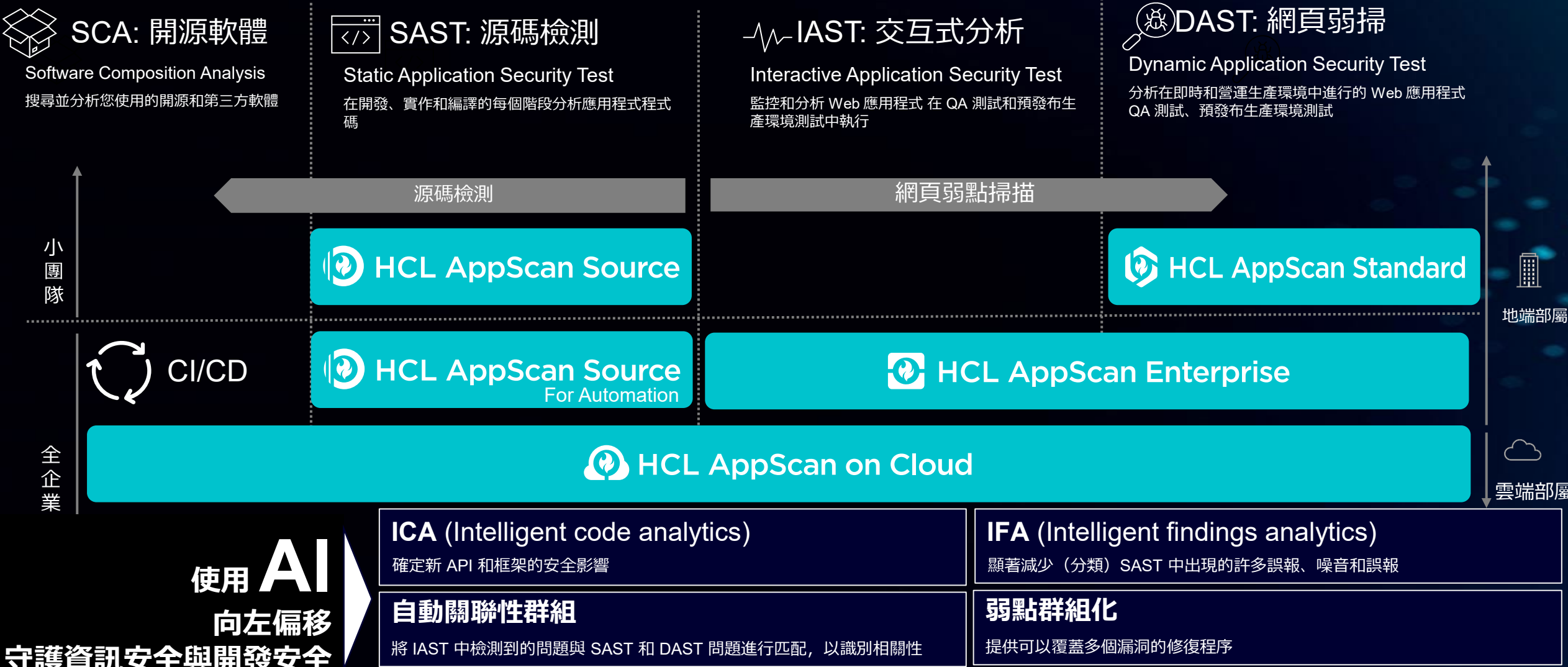


自動化: CI/CD整合



保護您的開發與應用 - HCL AppScan

使用AI測試應用程式從開發到營運的安全弱點



無死角的應用安全檢測 - 向左偏移 Shift Left

傳統的「開發」流程和「測試」 = 上版前執行網頁弱點掃描(DAST)



向左偏移=從「開發」的早期階段開始利用SAST（原碼檢測）和IAST(交互式分析)



該如何Shift Left 向左偏移

將應用安全檢測「整合」到您的開發流程中，**實踐**向左移動

Why?

Shift Left向左偏移的必要性

在早期發現弱點減少返工和延誤

未知弱點的風險，包括開源元件弱點

敏捷開發流程，實現CI/CD

困難：將不同工具進行整合

解決方法

Shift Left 「整合」到開發流程中

管理者

高成本效益

降低風險

開發者

提升程式品質

強化協同合作

打造完美 Secure DevOps

對使用者和管理員都「方便」的自動化

現狀(課題)

人工掃描耗人力、耽誤時間、易有疏漏

掃描基準不一致、弱點難管理

傳統管理方法的局限性



解決策

自動化

開發者

一站式自助服務

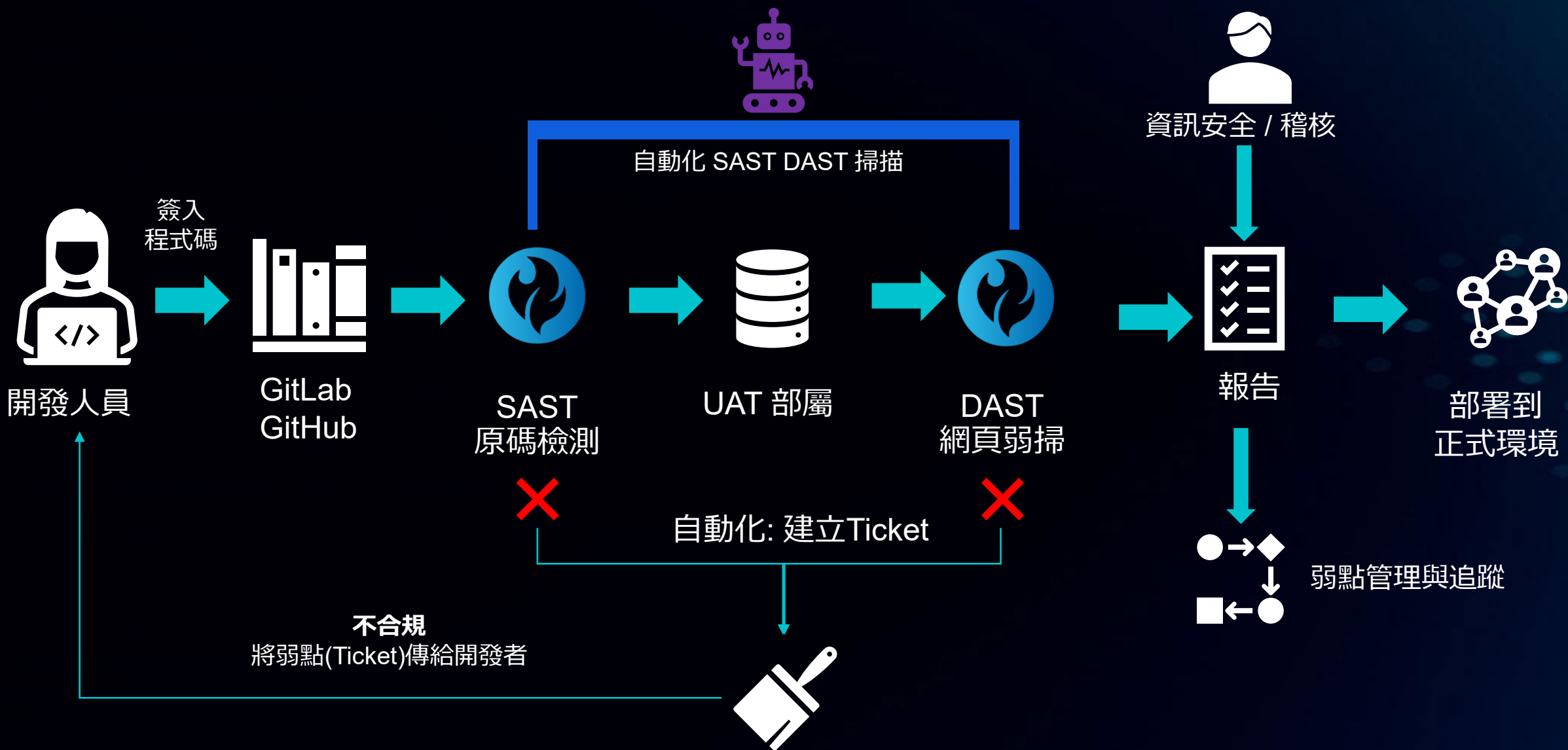
簡單、無須複雜設定

管理者

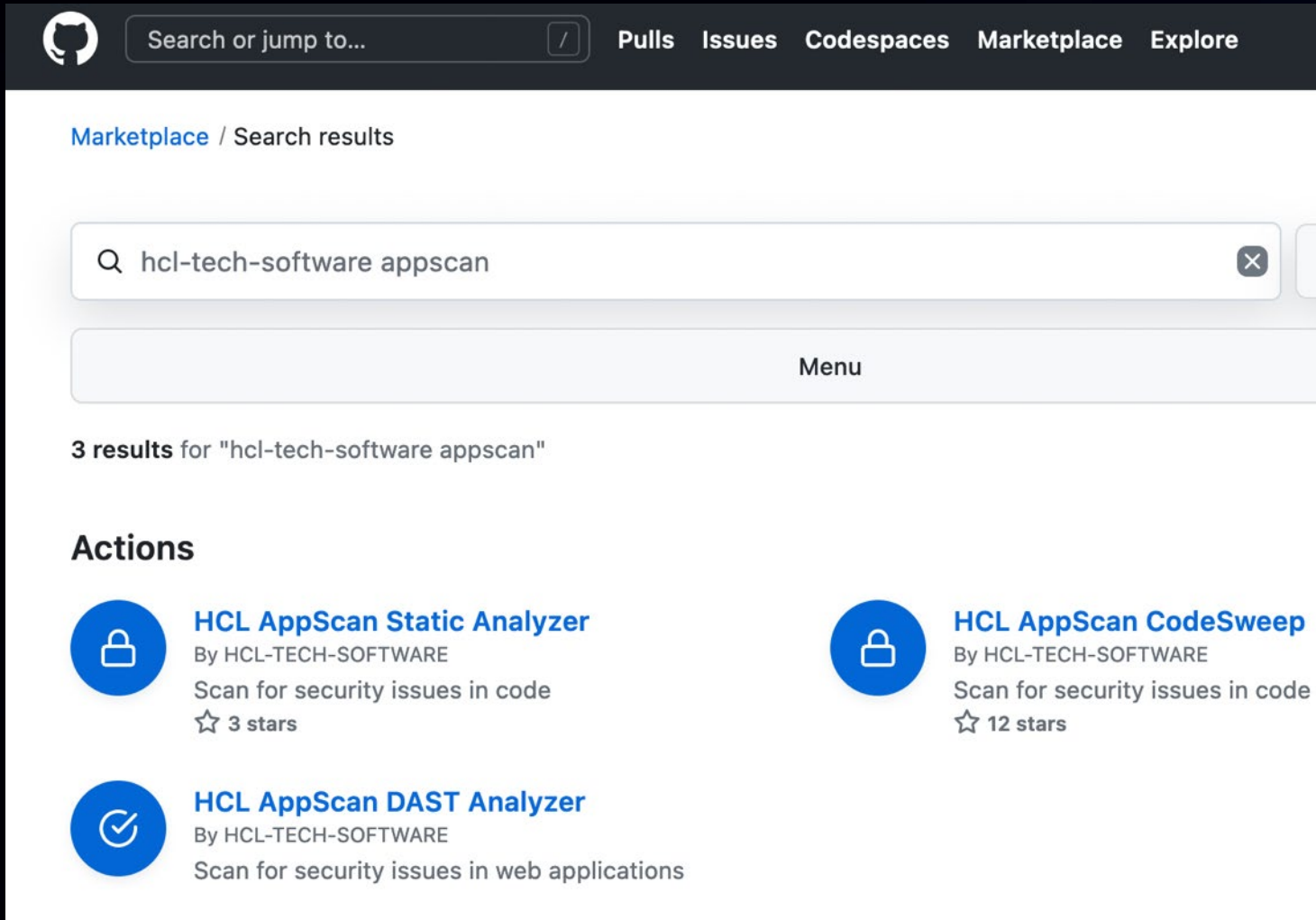
中央控管、追蹤

合規

自動化測試整合的開發流程

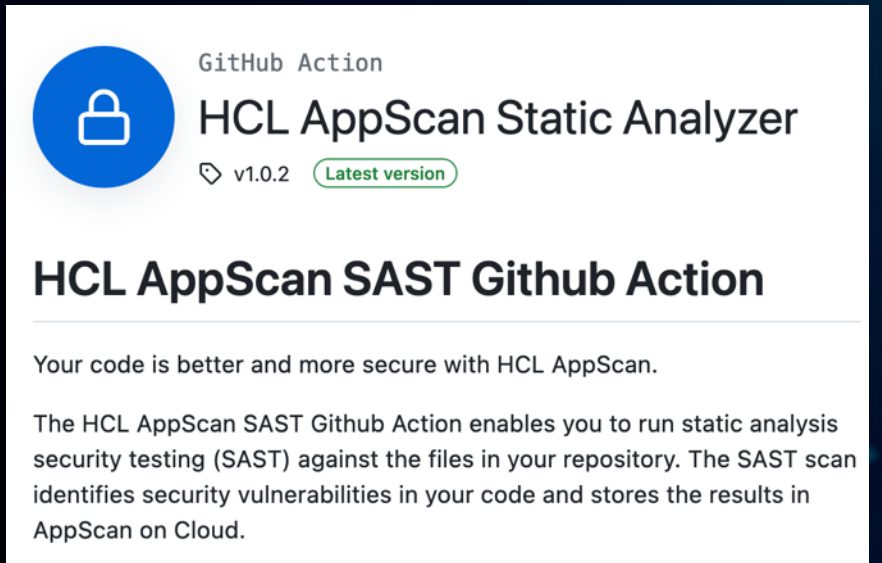


HCL AppScan @ GitHub Marketplace



The screenshot shows the GitHub Marketplace interface. At the top, there's a navigation bar with the GitHub logo, a search bar containing 'hcl-tech-software appscan', and links for Pulls, Issues, Codespaces, Marketplace, and Explore. Below the navigation bar, the page title is 'Marketplace / Search results'. A search bar contains the text 'hcl-tech-software appscan'. Below the search bar, there's a 'Menu' button. The search results show '3 results for "hcl-tech-software appscan"'. Under the 'Actions' section, there are three results:

- HCL AppScan Static Analyzer**
By HCL-TECH-SOFTWARE
Scan for security issues in code
☆ 3 stars
- HCL AppScan CodeSweep**
By HCL-TECH-SOFTWARE
Scan for security issues in code
☆ 12 stars
- HCL AppScan DAST Analyzer**
By HCL-TECH-SOFTWARE
Scan for security issues in web applications



GitHub Action

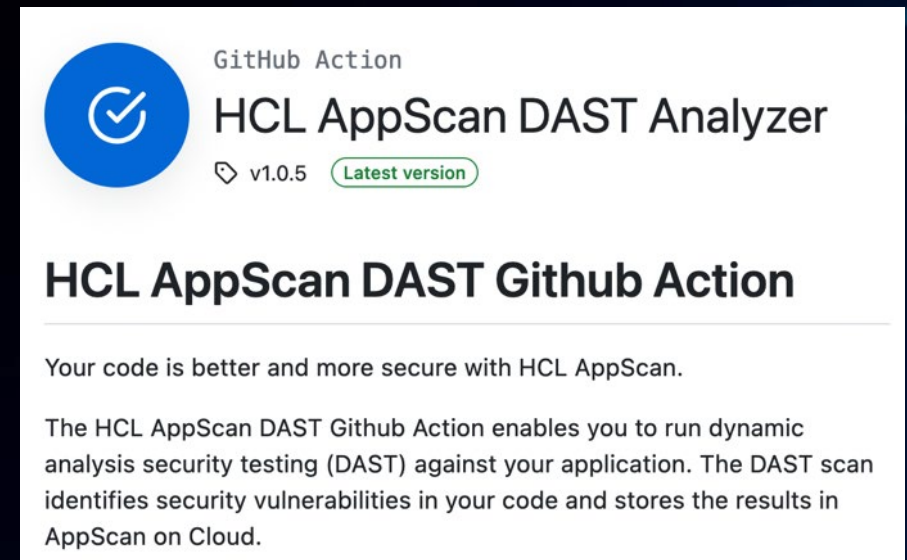
HCL AppScan Static Analyzer

v1.0.2 **Latest version**

HCL AppScan SAST Github Action

Your code is better and more secure with HCL AppScan.

The HCL AppScan SAST Github Action enables you to run static analysis security testing (SAST) against the files in your repository. The SAST scan identifies security vulnerabilities in your code and stores the results in AppScan on Cloud.



GitHub Action

HCL AppScan DAST Analyzer

v1.0.5 **Latest version**

HCL AppScan DAST Github Action

Your code is better and more secure with HCL AppScan.

The HCL AppScan DAST Github Action enables you to run dynamic analysis security testing (DAST) against your application. The DAST scan identifies security vulnerabilities in your code and stores the results in AppScan on Cloud.

GitLab Runner – Pipeline

appscan_onprem / GitLab_AltoroJ / Pipelines / #1077917889

Update .gitlab-ci.yml file

✓ Passed

Tech Advisor KC created pipeline for commit `a1f054c7` 5 months ago, finished 5 months ago

For `master`

2 jobs

13 minutes 21 seconds, queued for 0 seconds

Pipeline

Needs

Jobs 2

Tests 0

scan-sast

✓ scan-sast-job

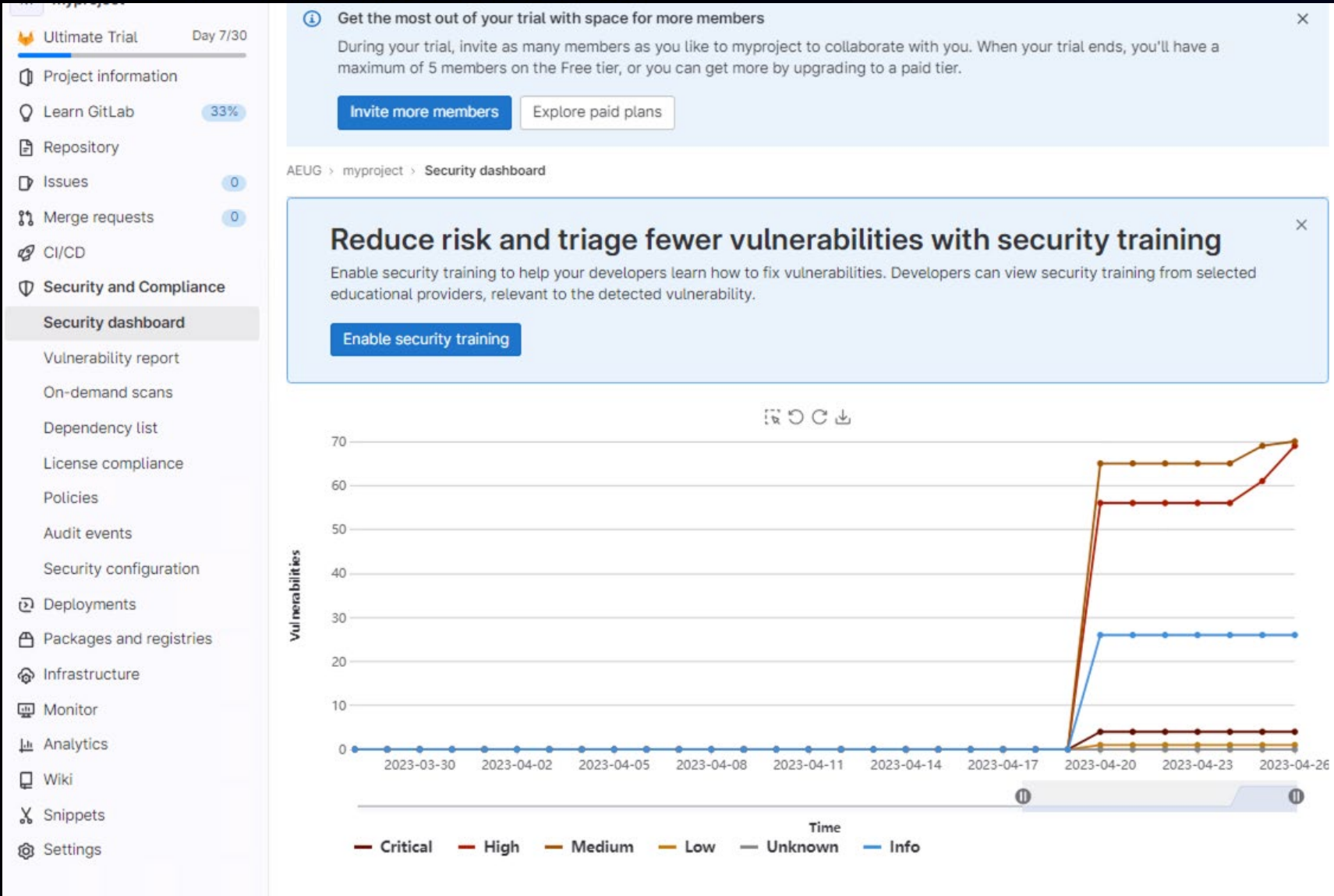
scan-dast

✓ scan-dast-job

HCLSoftware
Copyright © 2024 HCL Technologies Ltd.

18

GitLab Security Dashboard



GitLab 弱點管理

Vulnerability report

+ Submit vulnerability

Export

The Vulnerability Report shows results of successful scans on your project's default branch, manually added vulnerability records, and vulnerabilities found from scanning operational environments. [Learn more.](#)

Development vulnerabilities 124

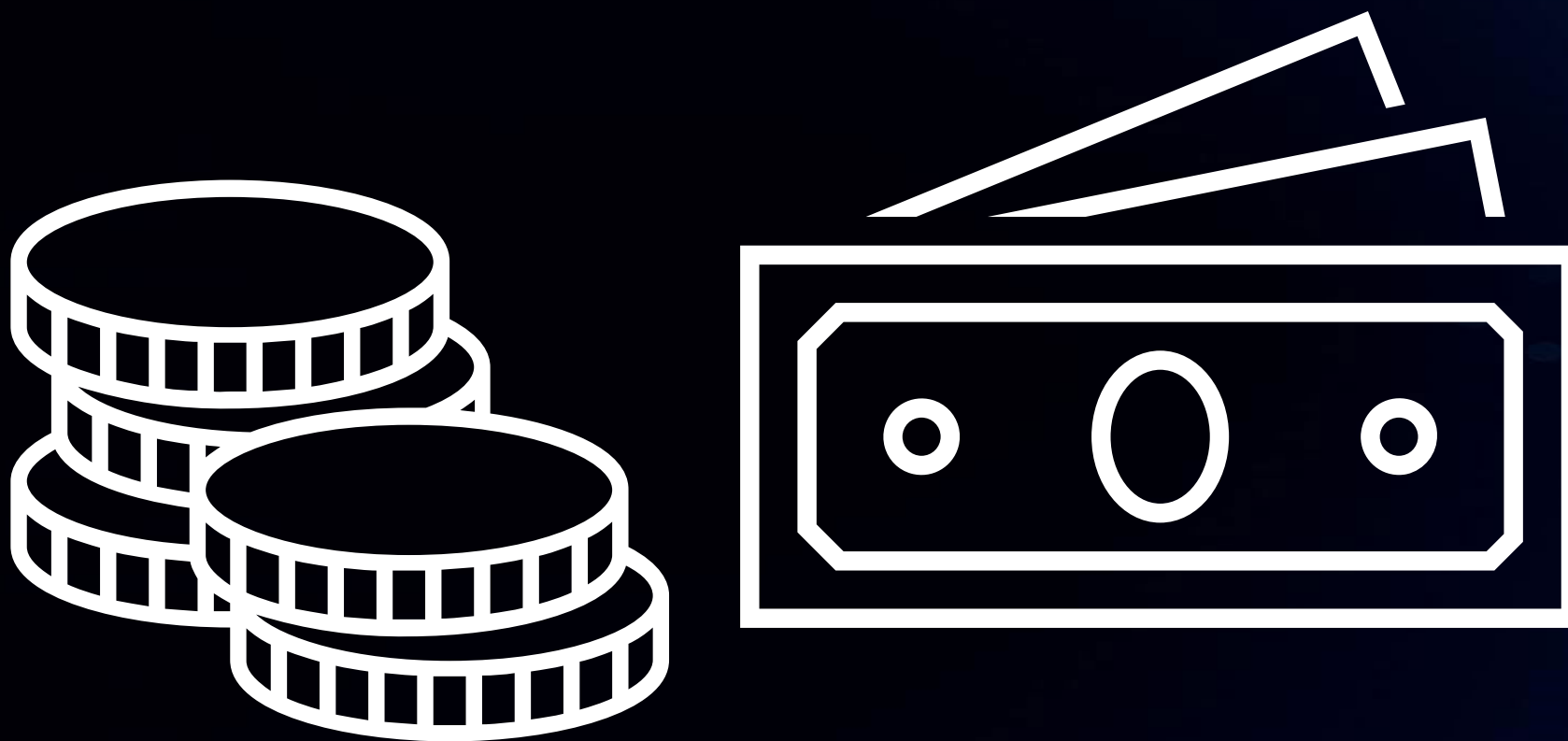
Operational vulnerabilities 0

Last updated 42 minutes ago #852260078

<div>Critical</div> <div>0</div>	<div>High</div> <div>86</div>	<div>Medium</div> <div>35</div>	<div>Low</div> <div>1</div>	<div>Info</div> <div>2</div>	<div>Unknown</div> <div>0</div>
----------------------------------	-------------------------------	---------------------------------	-----------------------------	------------------------------	---------------------------------

Status		Severity		Tool		Activity	
Needs triage +1 more		All severities		All tools		All activity	
<input type="checkbox"/>	Detected	Status	Severity	Description	Identifier	Tool	Activity
<input type="checkbox"/>	2023-04-28	Needs Triage	High	Reflected Cross Site Scripting in /index.jsp	CWE-79 + 1 more	DAST HCL	
<input type="checkbox"/>	2023-04-28	Needs Triage	High	Drupal Remote Command Execution without authentication (CVE -2018-7600) in /index.jsp	CWE-78 + 1 more	DAST HCL	
<input type="checkbox"/>	2023-04-28	Needs Triage	High	Link to Non-Existing Domain Found in /index.jsp	ASE: attnxdomain + 1 more	DAST HCL	
<input type="checkbox"/>	2023-04-28	Needs Triage	High	Injection in C:\gitlab\bin\builds\NNu-yABs\0\hclappscanta\AltoroJ\WebContent\util\serverStatusCheck.html(25) C:\gitlab\bin\builds\NNu-yABs... t\util\serverStatusCheck.html:25	CWE-699 + 1 more	SAST HCL	

能否同時實現「應用安全」與「降低成本」？



高度使用 DevSecOps

可以節省成本

4.8億

新台幣

整合安全測試在 2023 年
顯示出可觀的投資報酬率

700

年省

萬新台幣

DevSecOps最有效降低資料外洩成本

#1

27 個因素對資料外洩平均成本的影響。

22.8%

與未導入DevSecOps 資料外洩成本差異

(Cost of Data Breach Report 2023, IBM)

無死角的應用安全檢測 打造完美 Secure DevOps



HCL AppScan

- ✓ 網頁弱掃與原碼檢測**無法互相取代**
- ✓ 別遺忘**第三方套件、Open API**
- ✓ 開發生命週期**整合應用安全檢測**
- ✓ CI/CD自動化**提升效率**
- ✓ **技術**解決**管理**問題
- ✓ **管理**解決**技術**問題
- ✓ 合規 合規 合規

HCLSoftware

Contact Your Technical Advisor

Kevin Chia

Application Security Technical Advisor

kaijye.chia@hcl-software.com

HCLSoftware

Contact Your Product Specialist

Eric Hsu

Application Security Product Specialist

eric.hsu@hcl-software.com

HCLSoftware

hcl-software.com