利用 DevSecOps 自動化工具來融合資安、開發，與維運團隊的最佳實務

林皇興 Lambert Lin

VP / CISSP / 達友科技 Docutek Solutions

(Synopsys 新思科技/應用安全方案代理)

@臺灣資安大會 2024

2024/5/14

資安、開發與維運團隊的 DevSecOps 當今挑戰

軟體安全

問題：軟體與應用系統是駭客入侵活動的 #1 攻擊表面

目標：確保您所開發交付的軟體安全且可信賴

開發速度挑戰

問題：開發人員很討厭會拖慢開發進度的工具與資安檢查流程

目標：需要確保安全測試工具不會阻礙開發

合規&聚焦商業風險

問題：維運與開發團隊為漏洞修補而感到疲累不堪,無法聚焦真正風險

目標：需要識別並關注大量紀錄中的真正風險

SDLC 進階到 SSDLC，發展一個安全的，可靠的軟體

資料來源:
geeksforgeeks.org

軟體組建清單 SBOM 越來越受重視

- 因應層出不窮的資安危機，美國白宮發出行政命令，要求所有向聯邦政府出售的軟體都必須提供「軟體物料清單」（Software Bill of Materials，簡稱 **SBOM**）
  - 就像是食品標籤上的成分標示，載明軟體的組成、內部模組和完整的供應鏈
  - 軟體包數據交換（**SPDX**）已經成為一項國際標準（ISO/IEC 5962:2021）

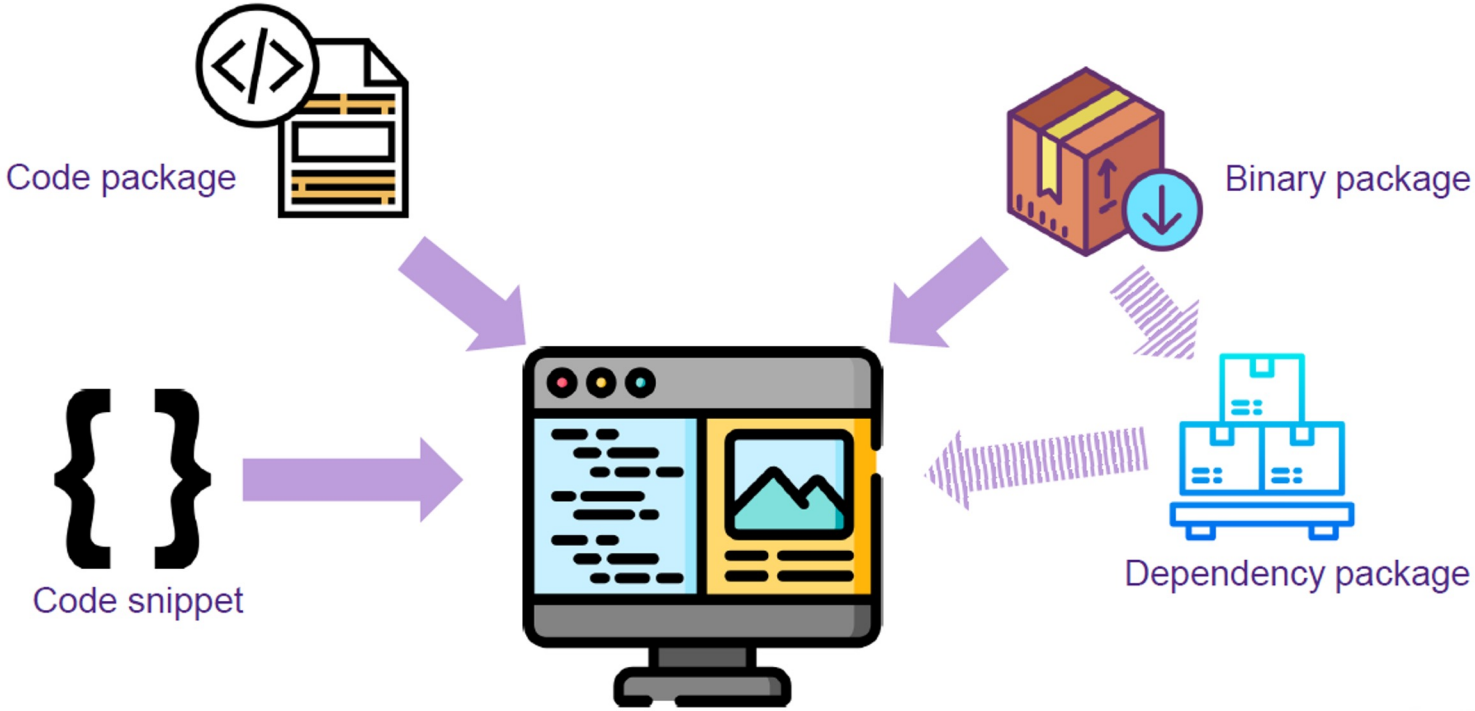
- **生成 SBOM 只是第一步**。正如 Log4Shell 向我們展示的那樣，當新的零日漏洞發生時，我們需要能夠**輕鬆地利用和搜索 SBOM**。
  - 使用**軟體組成分析工具（Software Composition Analysis, SCA）**生成 SBOM 很容易，但**管理**和**跟蹤**數百或數千個 SBOM 是一項艱巨的任務。

- 在交付應用程式之前掃描漏洞，掃描應用程式以識別組件和相關漏洞應該是一個持續的過程，不應該只運行一次，而應該定期運行。
  - 有新的安全漏洞被揭露時，優秀的SCA工具能夠**即時發出警告**，並提供更多的資訊協助修復。

歐盟新法 網路韌性法案 Cyber Resilience Act / CRA

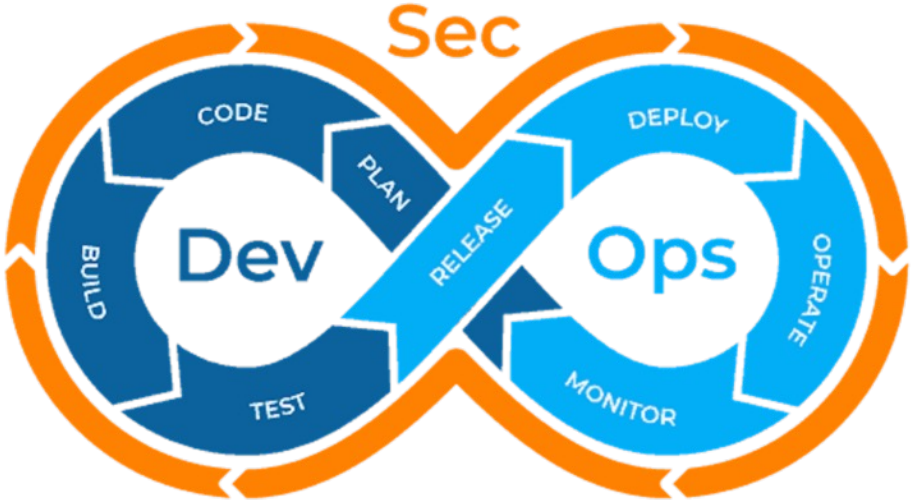
- 2024 年 3 月 12 日，歐洲議會以 517 票對 12 票贊成（78 票棄權）的多數票通過
- 標的: 具有數位元素的產品 (products with digital elements, PDE)
- 所有數位產品製造商、進口商和零售商需遵循
- 大幅改變產品的資訊安全規範和使用開源軟體的責任，違者恐面臨罰款甚至失去CE標誌的風險
- 違反CRA 處以最高 1500 萬歐元或上一財年全球年營業額 2.5% 的罰款（以較高者為準）

企業使用【開源軟體】方式 → Supply Chain 供應鏈風險



DevSecOps 讓安全活動無縫整合到軟體生命週期

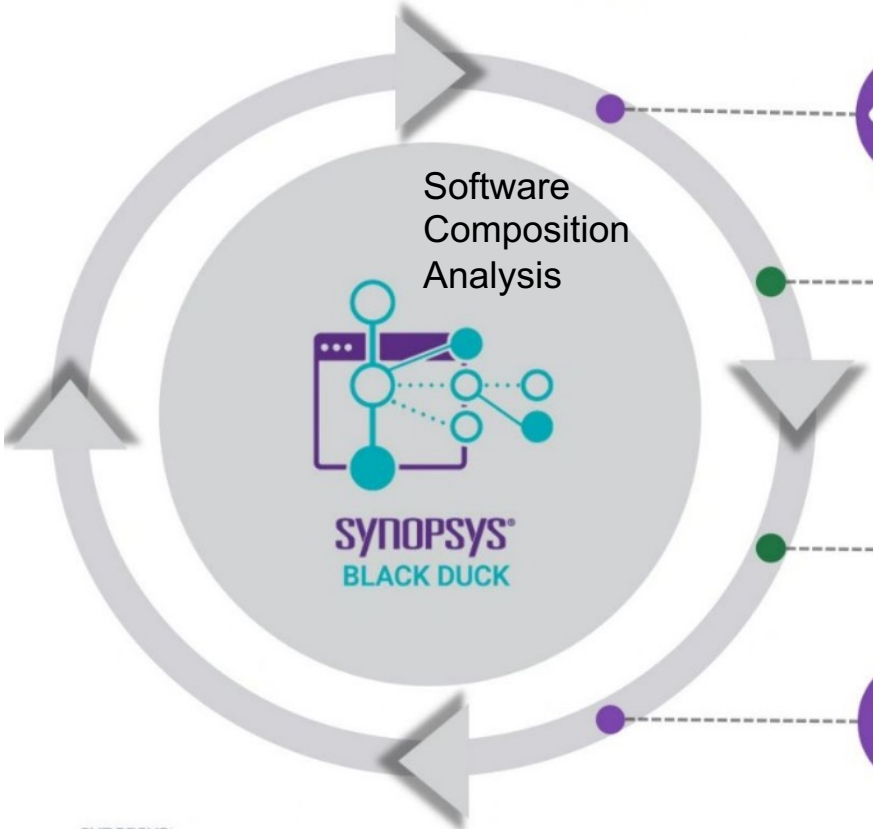
- 要有效的達成應用安全，是需要一些自動化工具的輔助
- AppSecTesting 工具融入 DevOps，打磨成適合自身的 DevSecOps 工具鏈
- 理想的 DevSecOps 工具鏈的應滿足以下特點：非侵入式、自動化、智慧能力、可視性及開放性



自動產生 Software BOM (Bill of Material) 組件清單與風險

Component	Source	Match Type	Usage	License	Security Risk
Apache Ant 1.10.8	2 Matches	Exact Directory	Dynamically Linked	Apache-2.0	2
Apache Commons BeanUtils 1.9.3	4 Matches	Direct Dependency, Transitive Dependency	Dynamically Linked	Apache-2.0	2
Apache Commons Codec 1.10	11 Matches	Transitive Dependency	Dynamically Linked	Apache-2.0	1
Apache Groovy GROOVY_2_5_12	64 Matches	Exact Directory	Dynamically Linked	Apache-2.0	1
Apache Groovy 2.4.15	225 Matches	Transitive Dependency	Dynamically Linked	Unknown License	1
Apache HttpClient 3.1	2 Matches	Direct Dependency	Dynamically Linked	Apache-2.0	5
Apache HttpClient 4.5.6	85 Matches	Direct Dependency, Transitive Dependency	Dynamically Linked	Unknown License	1
Apache HttpClient 4.5.10	1 Match	Exact Directory	Dynamically Linked	Apache-2.0	1
Apache PDFBox 1.8.16	2 Matches	Direct Dependency	Dynamically Linked	Apache-2.0	1
Apache Tomcat 8.5.34	17 Matches	Direct Dependency, Transitive Dependency	Dynamically Linked	Apache-2.0	1 5 11
Apache Tomcat Embed 8.5.34	4 Matches	Transitive Dependency	Dynamically Linked	Apache-2.0	1 5 11
Axis (Java) 1.4	275 Matches	Direct Dependency, Transitive Dependency	Dynamically Linked	Unknown License	3 2
Bouncy Castle 1.46	2 Matches	Direct Dependency	Dynamically Linked	MIT	1 2 12 1
Bouncy Castle 1.56	2 Matches	Transitive Dependency	Dynamically Linked	MIT	1 2 2
Bouncy Castle 1.55	7 Matches	Transitive Dependency	Dynamically Linked	MIT	1 2 11 1
Bouncy Castle 1.38	2 Matches	Transitive Dependency	Dynamically Linked	MIT	1 2 12 1
Bouncy Castle 1.64	2 Matches	Exact Directory	Dynamically Linked	MIT	1

Black Duck SCA 協助控制引用開放原始碼帶來的可能風險



Detect

識別與追蹤App或Container有用到開源的元件

Protect

找到與建議如何修復已知開源的弱點 (開發中/已發布)

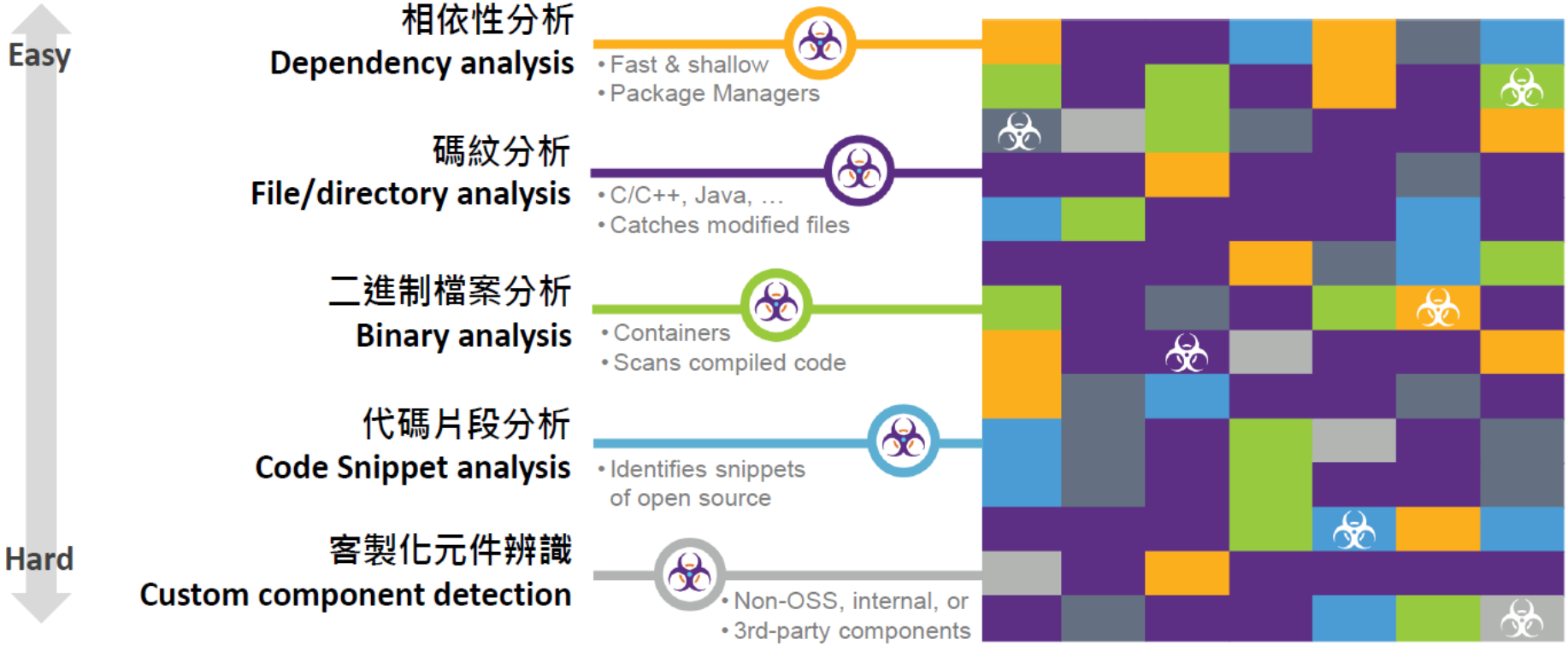
Comply

檢查、確認這些開源組件的授權條件，確保沒有授權違規

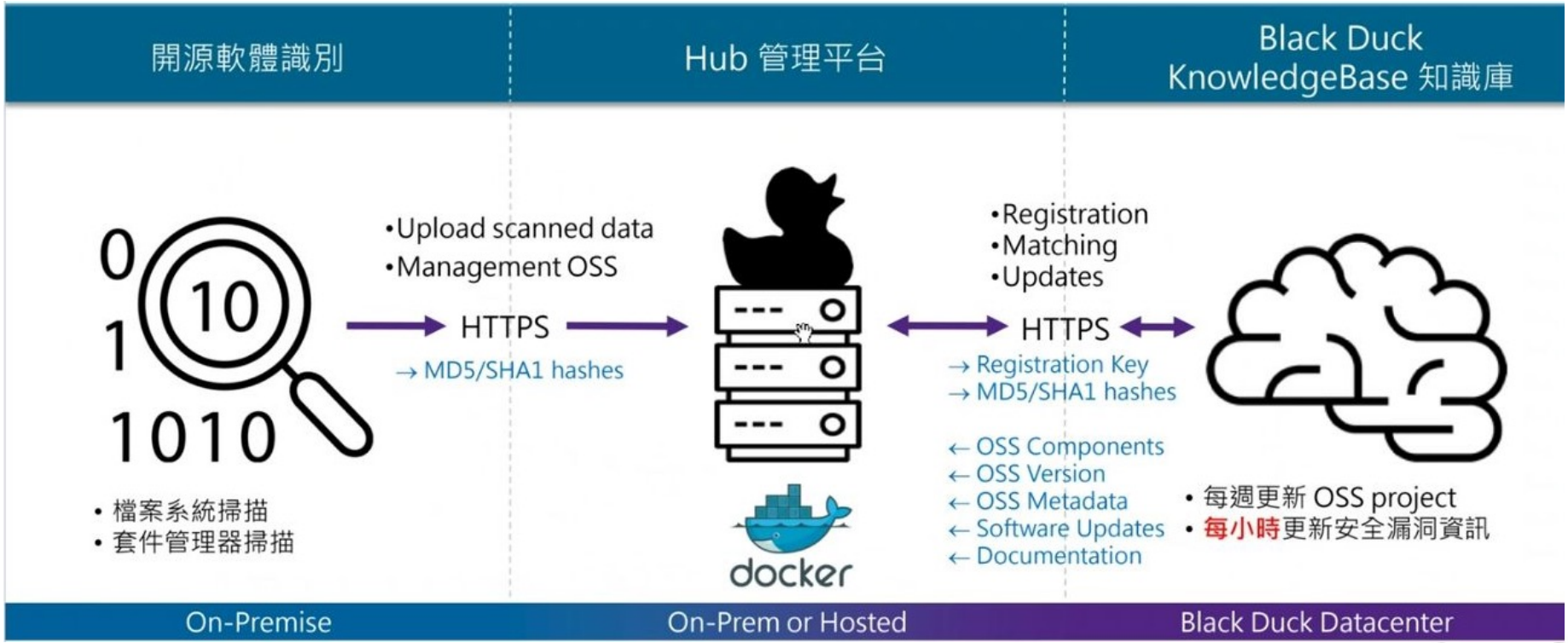
Manage

整合與自動化的落實開源組件引用帶來的風險，以遵循法規

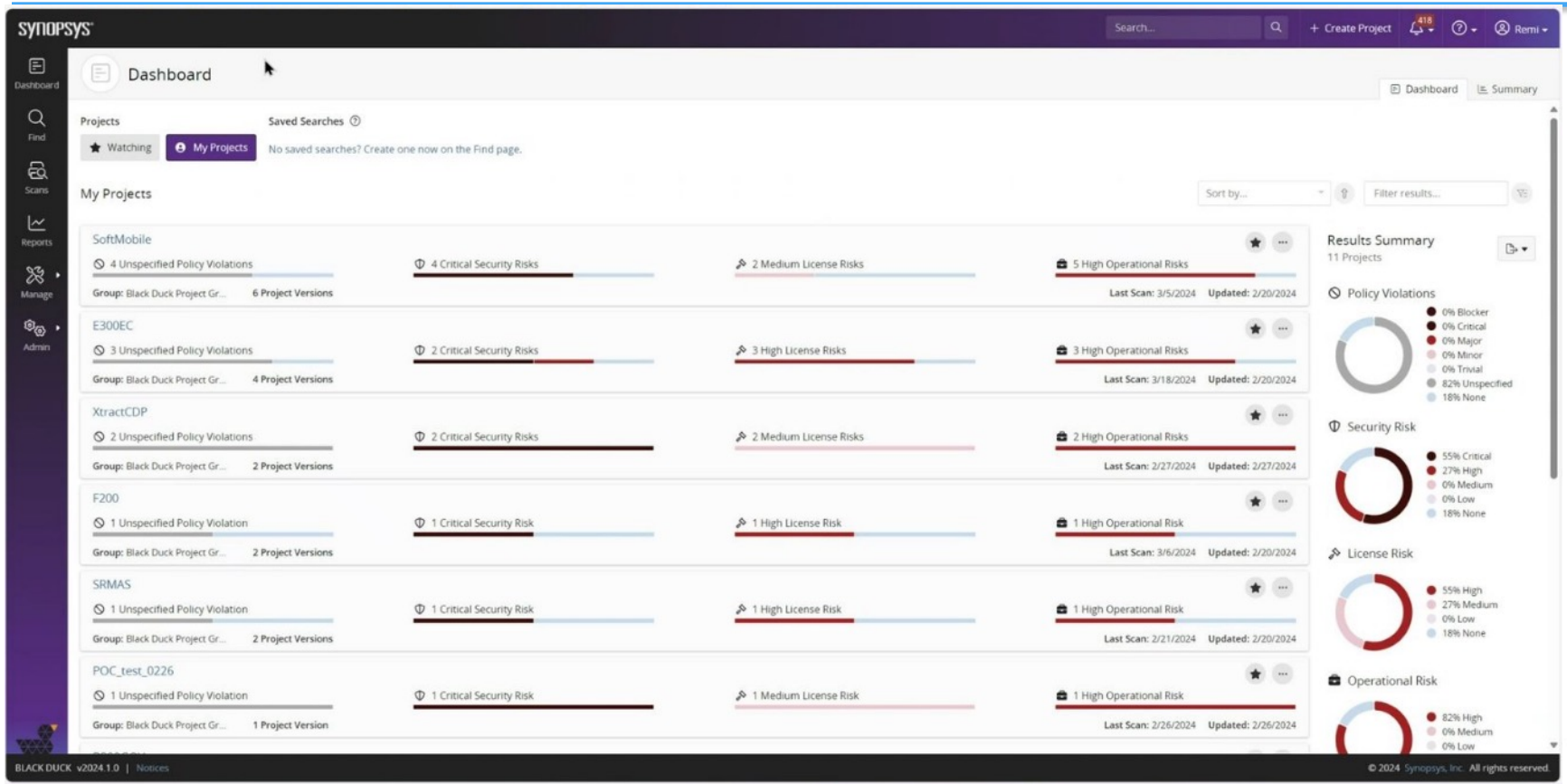
Black Duck 開源弱點比對 & 合法授權工具之分析技術



SCA : Black Duck – 系統架構

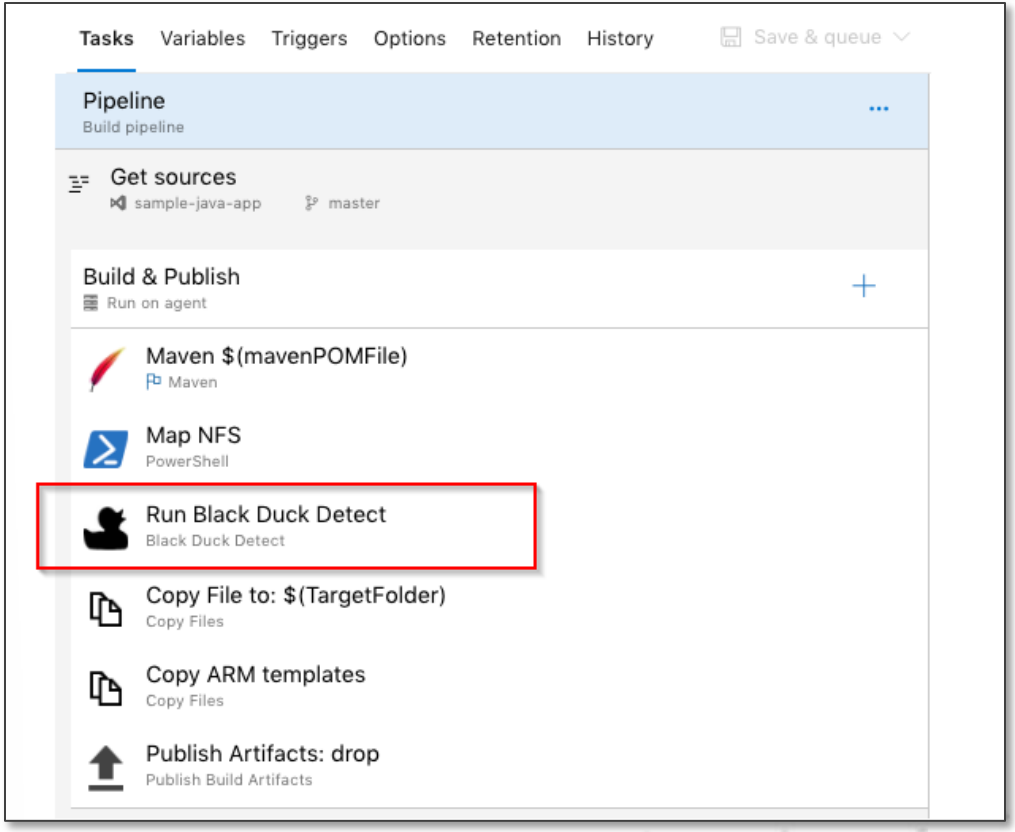


報告儀錶板

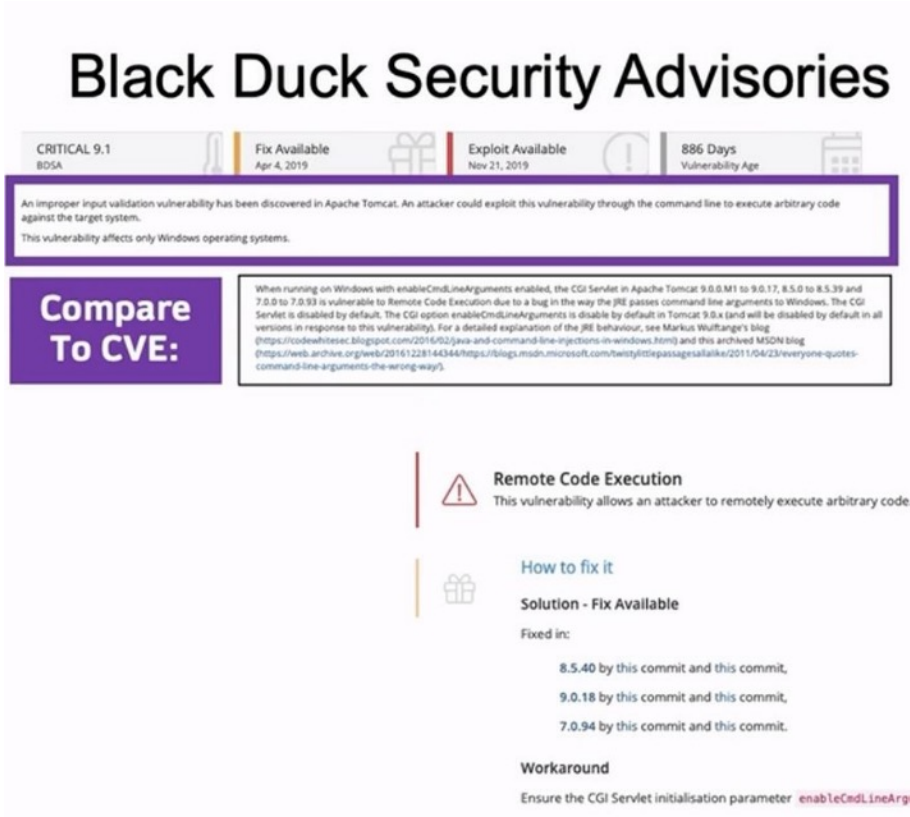


自動化 Pipeline 整合到 CI/CD 流程

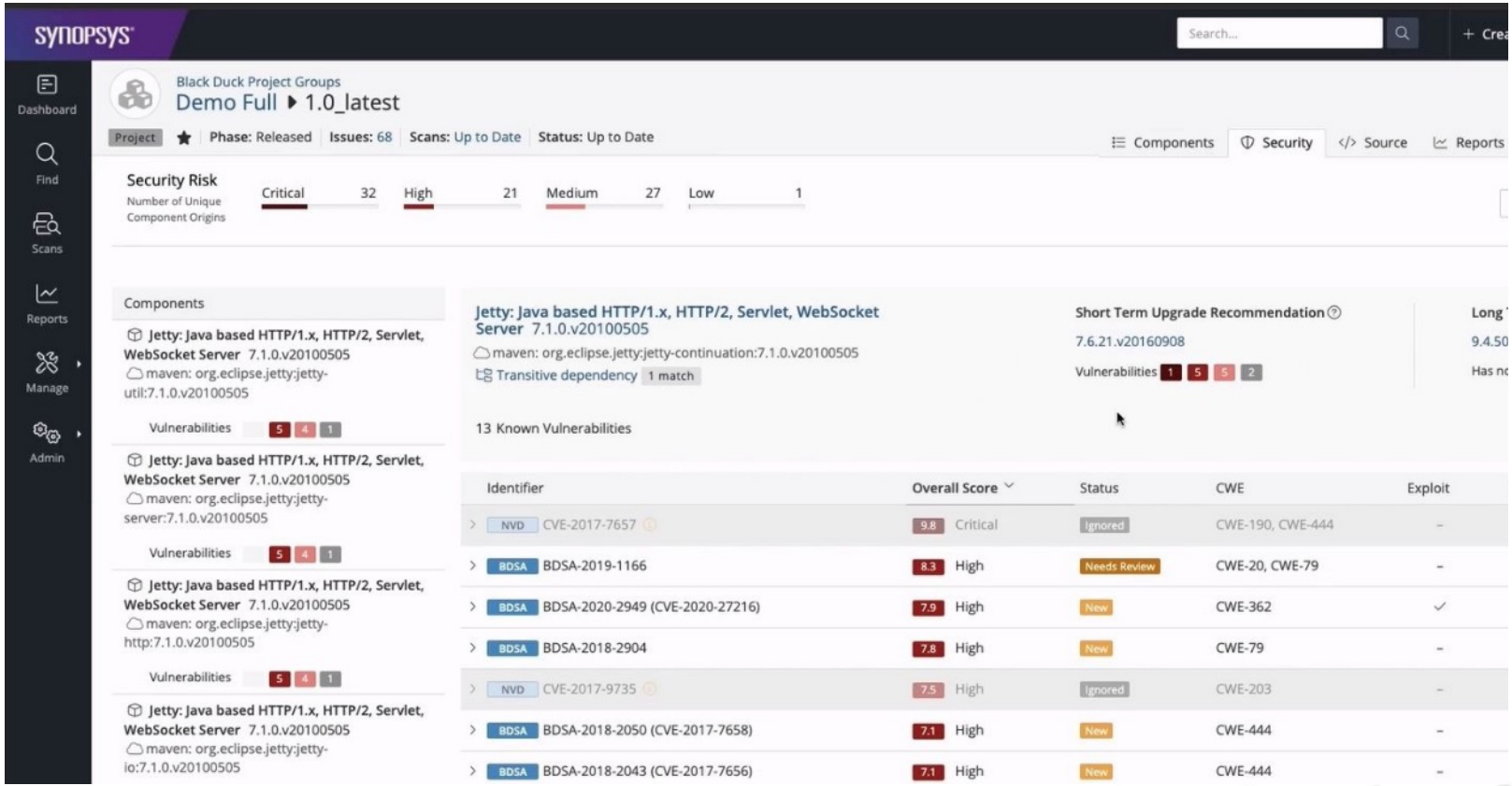
例如 GitHub, 微軟 Team Foundation Server (TFS), Azure DevOps
在 Build & Release Pipeline 中可自動整合 SCA 分析工具



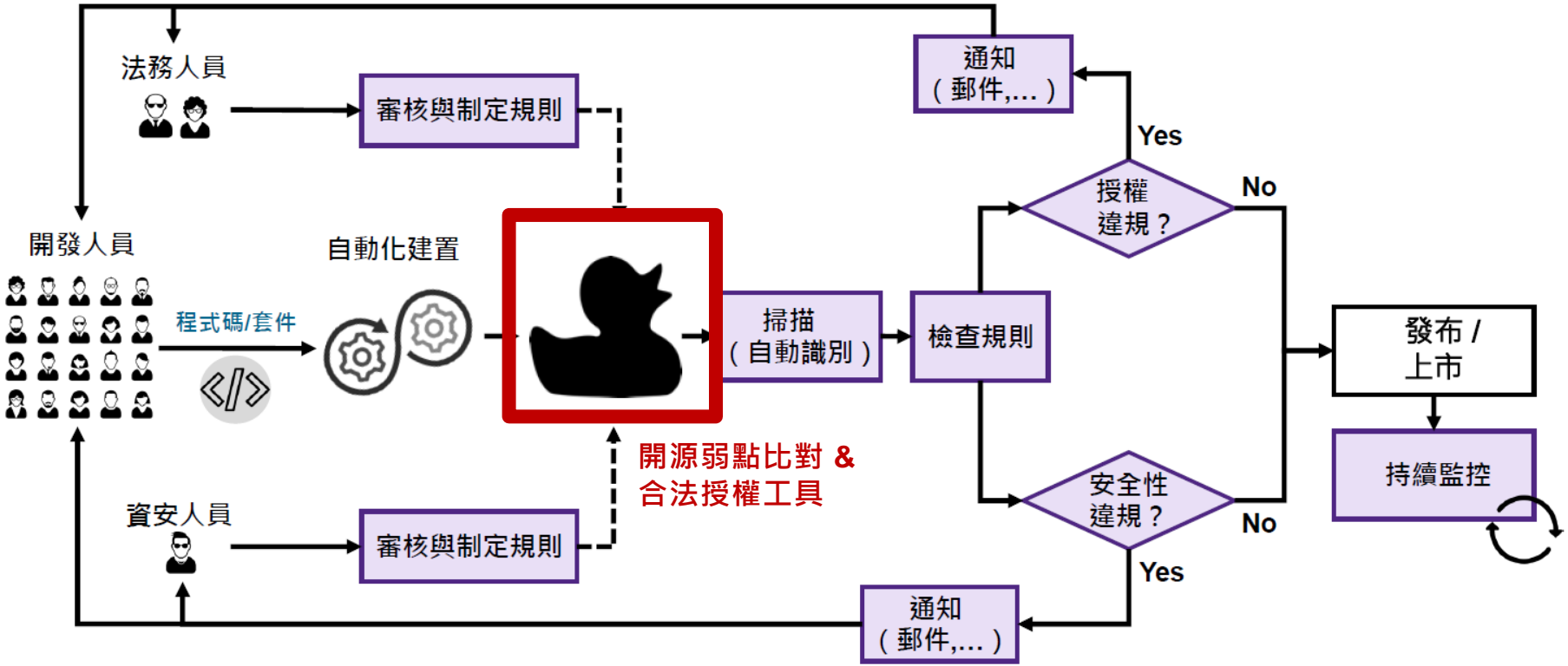
提供軟體風險的消弭建議



可追蹤弱點修正的軌跡



開源弱點比對 & 授權合法性分析之流程



在應用安全測試領域，是廣受認可的領導者

Gartner®

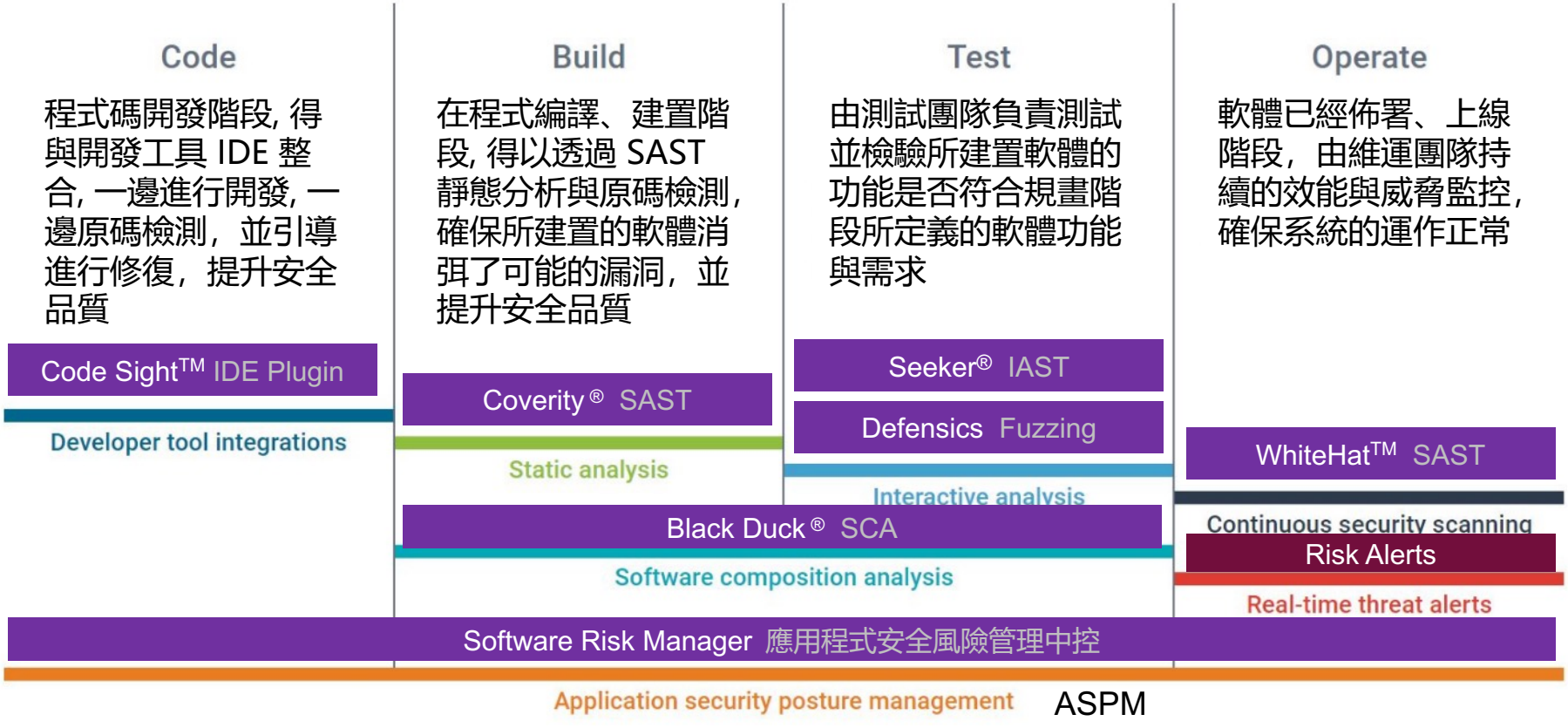
Magic Quadrant for Application Security Testing

FORRESTER

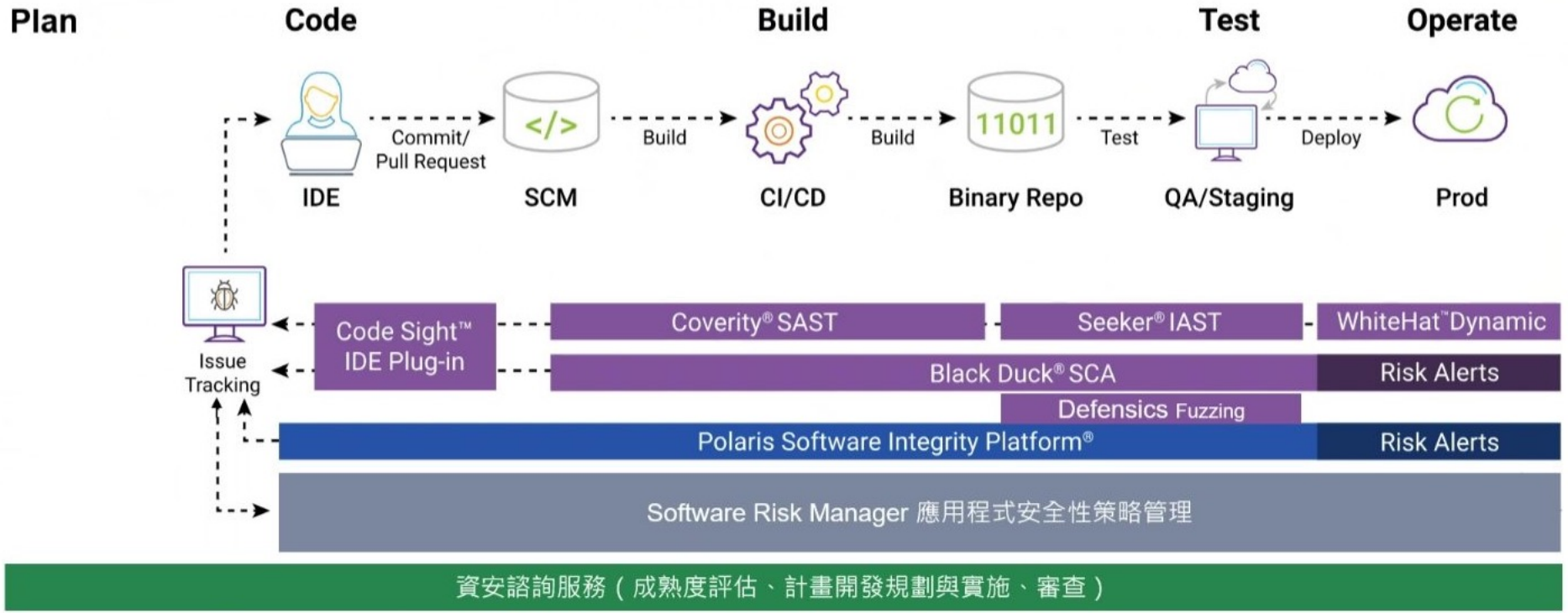
Forrester Wave™: Static Application Security Testing

Forrester Wave™: Software Composition Analysis

Synopsys 的 DevSecOps 應用安全完整方案



Synopsys 的應用安全方案，智慧地將資安融入 DevOps 中



達友科技代理的主要品牌與應用

利用 DevSecOps 自動化工具來融合資安、開發，與維運團隊的最佳實務

林皇興 Lambert Lin

VP / CISSP / 達友科技 Docutek Solutions

(Synopsys 新思科技/應用安全方案代理)

@臺灣資安大會 2024

2024/5/14