onward SECURITY
a DEKRA company

DEKRA

HERCULES

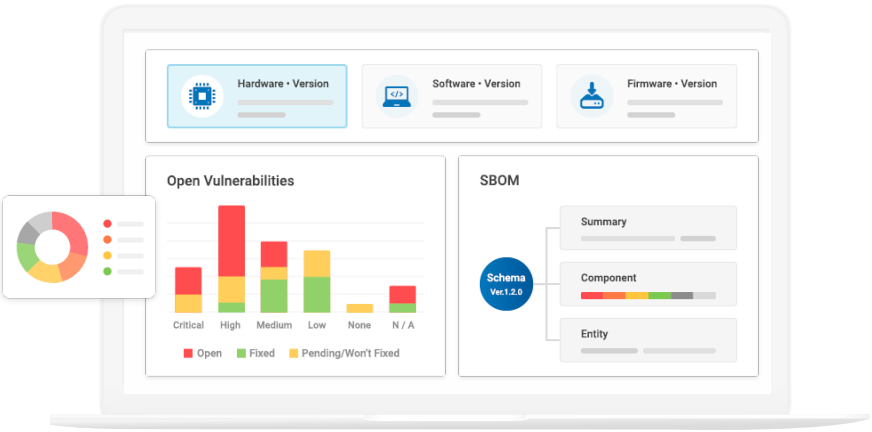
SecSAM 開源軟體風險管理系統

輕鬆找出產品中開源軟體之潛在風險

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

2023 Cybersecurity Excellence Awards
開源軟體安全金獎

HERCULES SecSAM 開源軟體風險管理系統可有效管理開源軟體 (Open Source Software, OSS) 之風險，透過分析產品組成並建立軟體物料清單 (SBOM)，藉此找出並管理專案 (產品) 中第三方元件之弱點、授權等問題，並提供建議的弱點修復方案。



如何選擇安全的 Open Source 元件

美國政府針對軟體供應鏈安全已下達行政命令。未來透過軟體物料清單進行供應鏈管理已勢在必行，其中開源軟體組成複雜的特性，使其成為軟體供應鏈管理中極為重要的一環。

Gartner

不久的將來，軟體購買者在購買產品時，會要求廠商提供軟體物料清單 (SBOM)

找出開源弱點並提供修補建議

透過持續性的弱點分析、警示，協助團隊提早發現所需處理的資安風險及授權問題，在設計階段初期即可處理弱點，或使用更安全的第三方元件，降低後續修補時間及成本。

分析開源元件授權

透過韌體掃描自動分析產品中第三方元件的授權類型，例如：GPL、Apache、LGPL 等，協助客戶避免授權爭議，保護企業智慧財產權。

onward SECURITY a DEKRA company

DEKRA

SecSAM 六大功能

韌體掃描

透過韌體掃描進行軟體溯源、分析軟體供應鏈組成，無須原始碼即可分析軟體中之第三方元件組成。

OSS 清單管理

持續性的管理產品專案中之 OSS 清單，透過 SecSAM 之安全元件選擇功能，協助開發者選用安全、合適的元件進行開發。

CVE 弱點追蹤

藉由 SBOM 的建立與維護，分析 CVE，協同每日自動更新弱點情資、測報管理及追蹤審核機制，有效監控產品與開源元件弱點。

弱點分析

與國際 NVD 同步的弱點資訊，超過 240, 000 個以上 CVE 弱點情資，內容涵蓋 1,200,000 個元件，可提供完整的產品弱點比對。

CI/CD 整合

透過問題追蹤文件或提供標準 API 介接等模式，進行產品的持續開發整合流程，讓使用者不需花費過多時間進行繁瑣的操作。

SBOM 格式轉換

支援市面上主流 SBOM 格式的匯入匯出，包括 SWID, SPDX 等；讓企業匯入可接受的格式資料，並匯出所需的格式檔案。

輕鬆進入安全開發的正向循環

1 建立專案

透過韌體掃描辨識協力廠商元件與開源元件組成，建立產品開源元件清單。

2 安全設計評估

- 開源軟體元件選用
- 開源軟體弱點風險評估
- 開源軟體授權風險評估

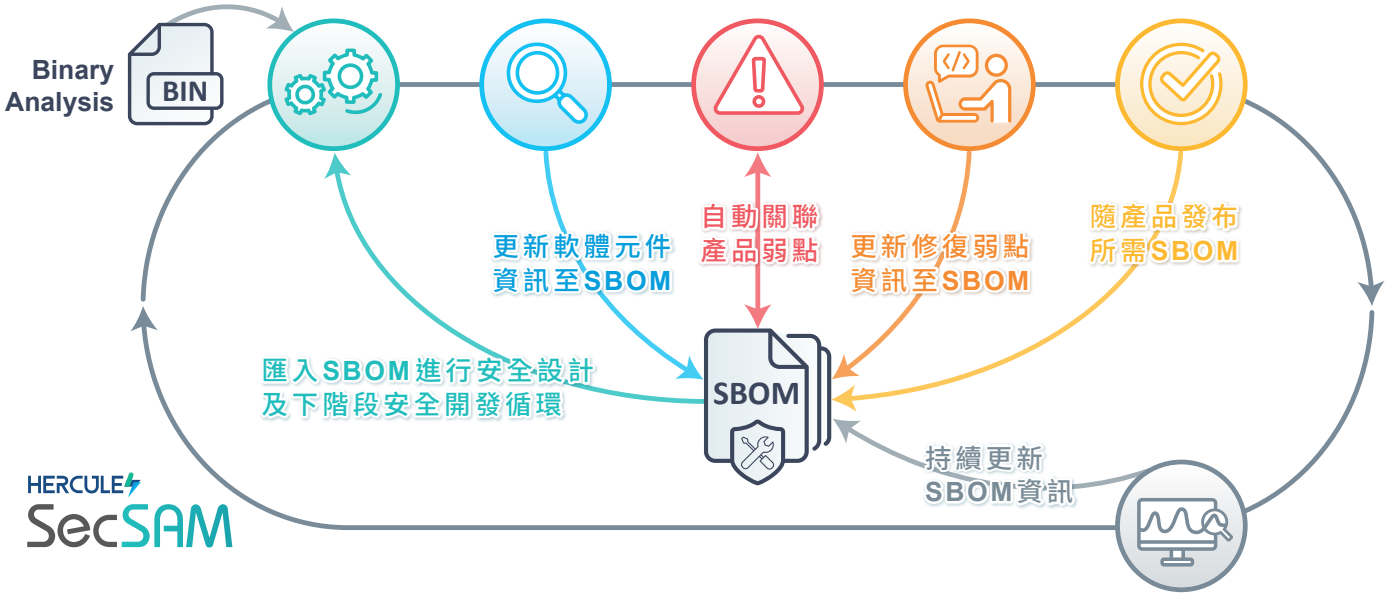
3 開發流程整合

CI/CD 弱點修復&追蹤

mantis BUG TRACKER　Jira　X

4 專案發布

- 專案報告
- SBOM 發布



安華聯網科技 (DEKRA 德凱集團成員)

Contact Us - contact.onward@dekra.com　Learn more at - www.onwardsecurity.com