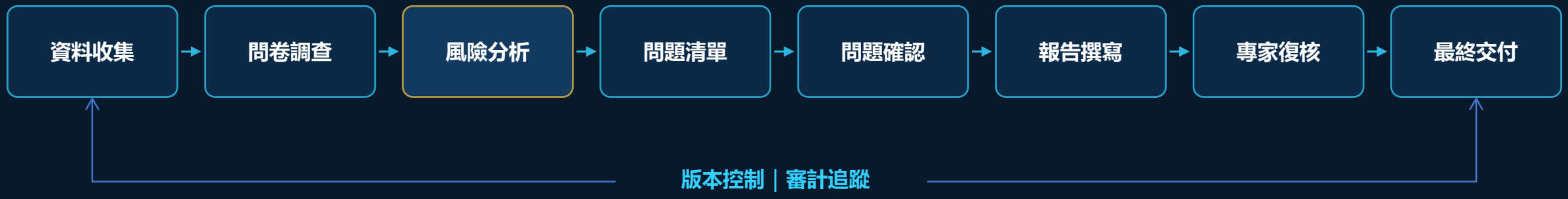
SCS | 开源服务

AI-SRAA Compliance Reporting Delivery System

System Objective

This system adopts AI large model technology, combined with an SRAA compliance knowledge base, standardised delivery workflows, evidence management and manual review mechanisms, to assist law firms, accounting firms, professional consulting companies and system integrators in platformising, standardising and automating their existing SRAA and compliance report delivery processes, thereby realising a more efficient, more cost-effective and more reliable compliance report delivery capability.

AI-SRAA System Delivery Process



核心技術：混合模型架構 + 本地化部署能力

硬體配置

本系統採用高密度 GPU 伺服器作為 AI 推理核心節點，構建集中式算力平台

計算資源配置：

- AMD AS-4125GS-TNRT準系統雙路AMD 服務器
- CPU：AMD EPYC 5代 9655 2.6C 96核 192線程（正式版無鎖） × 2
- 主板：AMD AS-4125GS-TNRT
- 內存：三星/SK/MU ECC DDR5 64G 5600 × 16
- 固態系統盤：三星480G 企業級 × 2
- 機械數據盤：希捷/西數 8T 3.5寸企業級機械硬盤 × 5
- 算力卡：RTX Pro 6000 Blackwell Server Edition × 8
- 網卡：全高INTEL藍標 X520 雙萬兆
- 散熱：機架式高效風冷

架構特點：

- 多 GPU 並行推理（Parallel Inference）
- 支持多模型同時運行
- 高吞吐 + 低延遲設計

輸出：

- 模型服務可调用
- GPU運行環境

專家復核機制：專業判斷保留機制

1

執行摘要

由 AI 根據項目範圍、主要風險、風險等級及整改重點生成初稿；顧問負責確認管理層表達、風險重點、語氣措辭及最終結論。

2

風險點發現及描述

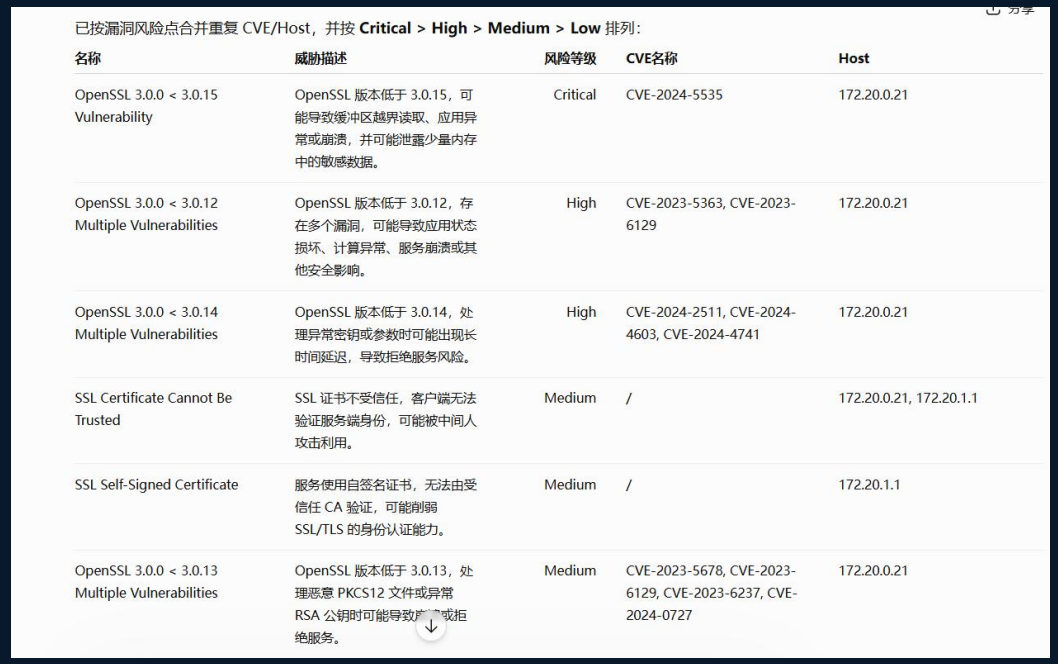
由 AI 根據證據鏈、Checklist 問題清單及風險分析結果生成風險描述、威脅說明、影響分析及整改建議；顧問負責確認事實準確性、風險評級、證據充分性及建議可行性。

3

附錄

由人工手動上傳附錄材料

AI模型準確性對比



已按漏洞风险点合并重复 CVE/Host，并按 **Critical > High > Medium > Low** 排列：

名称	威胁描述	风险等级	CVE名称	Host
OpenSSL 3.0.0 < 3.0.15 Vulnerability	OpenSSL 版本低于 3.0.15，可能导致缓冲区越界读取、应用异常或崩溃，并可能泄露少量内存中的敏感数据。	Critical	CVE-2024-5535	172.20.0.21
OpenSSL 3.0.0 < 3.0.12 Multiple Vulnerabilities	OpenSSL 版本低于 3.0.12，存在多个漏洞，可能导致应用状态损坏、计算异常、服务崩溃或其他安全影响。	High	CVE-2023-5363, CVE-2023-6129	172.20.0.21
OpenSSL 3.0.0 < 3.0.14 Multiple Vulnerabilities	OpenSSL 版本低于 3.0.14，处理异常密钥或参数时可能出现长时间延迟，导致拒绝服务风险。	High	CVE-2024-2511, CVE-2024-4603, CVE-2024-4741	172.20.0.21
SSL Certificate Cannot Be Trusted	SSL 证书不受信任，客户端无法验证服务端身份，可能被中间人攻击利用。	Medium	/	172.20.0.21, 172.20.1.1
SSL Self-Signed Certificate	服务使用自签名证书，无法由受信任 CA 验证，可能削弱 SSL/TLS 的身份认证能力。	Medium	/	172.20.1.1
OpenSSL 3.0.0 < 3.0.13 Multiple Vulnerabilities	OpenSSL 版本低于 3.0.13，处理恶意 PKCS12 文件或异常 RSA 公钥时可能导致[illegible]或拒绝服务。	Medium	CVE-2023-5678, CVE-2023-6129, CVE-2023-6237, CVE-2024-0727	172.20.0.21

ChatGPT 5.5 （80%）

开源服务AI助手

+ 新会话

运行设置
gpt-oss:120b · 自动技能

会话 ID
session-1782550601056

模型
gpt-oss:120b

技能
自动识别技能

- 自动匹配技能
- 启用工具调用
- 启用多步骤 Planner
- 高风险工具执行前确认

Planner 确定性　思考模式 开启

历史会话 5
请你整理出这个表格的漏洞风险… 2 条消息
你是一名hk Security Risk Asses… 6 条消息

请你整理出这个表格的漏洞风险点，从高到低进行排列，只列出名称、威胁…
gpt-oss:120b · 自动技能

test-3　API Key　退出

Low; CVE: CVE-1999-0524; Host: 172.20.0.1
3. Same for host .21 (also Low). Since same risk, order maybe same risk but keep both. So list both low entries.
Thus final answer a table sorted.

以下是从 **风险等级高到低** 排列的漏洞要点（仅保留 **名称、威胁描述、风险等级、CVE 名称、主机（Host）**）：

序号	名称 (Name)	威胁描述 (Synopsis)	风险等级 (Risk)	CVE 名称	主机 (Host)
1	HTTP TRACE / TRACK Methods Allowed	Debugging functions are enabled on the remote web server.	Medium	CVE-2003-1567	172.20.0.21
2	ICMP Timestamp Request Remote Date Disclosure	It is possible to determine the exact time set on the remote host.	Low	CVE-1999-0524	172.20.0.1
3	ICMP Timestamp Request Remote Date Disclosure	It is possible to determine the exact time set on the remote host.	Low	CVE-1999-0524	172.20.0.21

说明

- 该 CSV 中只有 **Medium** 与 **Low** 两个风险等级，未出现 **High**。因此表格先列出唯一的 Medium 项，随后按出现顺序列出两个 Low 项。
- “威胁描述” 采用 CSV 中的 **Synopsis** 列内容。

+ 添加附件　未选择附件

输入消息　发送

ChatGPT 4.0 （60-70%）

效率對比


一小時 vs 八小時的差別
AI-SRAAA 系統大幅提升效率，讓專家專注於專業判斷與風險確認
傳統人工方式
1 資料收集與整理
人工逐份閱讀、分類、歸檔
2 證據查找與關聯
手動查找證據並建立關聯
3 風險分析與判斷
人工分析控制缺口與風險
4 撰寫報告初稿
撰寫風險描述、建議與結論
5 格式調整與檢查
調整格式、檢查內容一致性
VS
一鍵生成報告
1 資料自動整理與分類
系統自動提取、重整並建立關鍵結構
2 證據自動關聯與檢索
系統自動關聯證據並控制與鍵項目
3 風險分析與草稿生成
AI 根據證據生成風險描述與建議
4 報告初稿自動生成
生成結構化報告初稿與問題清單
5 專家審核與最終確認
專家專注於專業判斷與內容確認
專家花費大量時間在重複性文檔處理與整理，可投入專業判斷與客戶溝通的時間有限。
系統自動處理重複性工作，專家專注於風險判斷，大幅提升工作效率與品質。
流程從 8 小時縮短至 1 小時，效率提升 87%，讓專業價值最大化！


SCS | 开源服务
THANKS