SandSphere

惡意程式檢測系統

應對第三方資源汙染風險的解決之道

在當前的軟體開發環境中，第三方套件和開源資源已成為加速開發的關鍵。然而，隨著第三方資源的普及，外部程式碼的安全風險也在逐漸增加，尤其是開源程式碼庫中的惡意程式碼和後門成為了新興的資安威脅。針對這些惡意程式汙染問題，SandSphere 惡意程式偵測平台為開發團隊提供了強大、精確的安全掃描解決方案。

SandSphere 惡意程式偵測平台

SandSphere 是一款專注於惡意程式偵測的安全平台，針對第三方元件及外部套件的潛在安全威脅提供了多層次的分析方法，涵蓋以下主要功能：

惡意程式與後門偵測

SandSphere 利用深層靜態和動態分析技術掃描第三方元件中的惡意程式、後門及可疑代碼。即使是變異或加殼的惡意程式，也能被平台的 AI 驅動相似度比對引擎識別出來，有效防止汙染程式碼進入系統中。

嵌入 URL 和外部連結掃描

除了惡意程式碼，SandSphere 能分析程式碼中是否包含惡意 URL、可疑的外部連結或不安全的 API 呼叫，避免不安全的外部資源被無意引入。

變種惡意程式檢測

隨著攻擊者利用不同方法變異惡意程式以躲避檢測，SandSphere 的 AI 技術能有效檢測出這些變異程式碼，並提供詳細的分析報告，協助團隊快速辨別程式碼中的安全性問題。

動態分析誘發惡意行為

針對一些未在靜態代碼中表現出惡意的程式碼，SandSphere 提供沙箱模擬執行環境，通過誘發機制誘使惡意行為表現，進一步提高偵測的準確性。

解決方案優勢

高精確度偵測

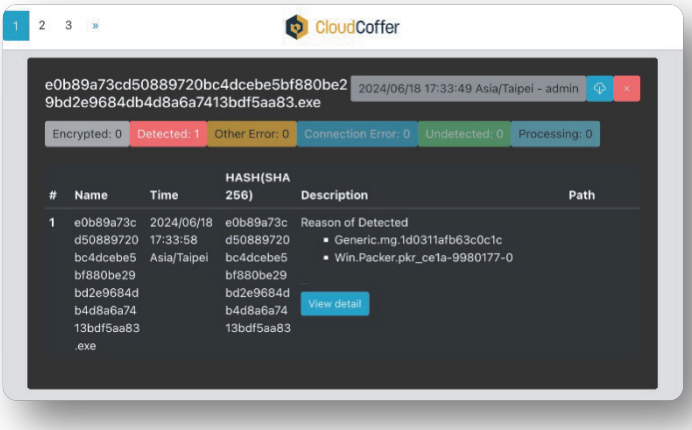
SandSphere 結合靜態與動態分析，並搭載 AI 技術，能更精確識別已知與未知的惡意程式、變異程式碼，並排除正常代碼誤報，適合嚴格控制版本質量的開發團隊。

迅速應對供應鏈風險

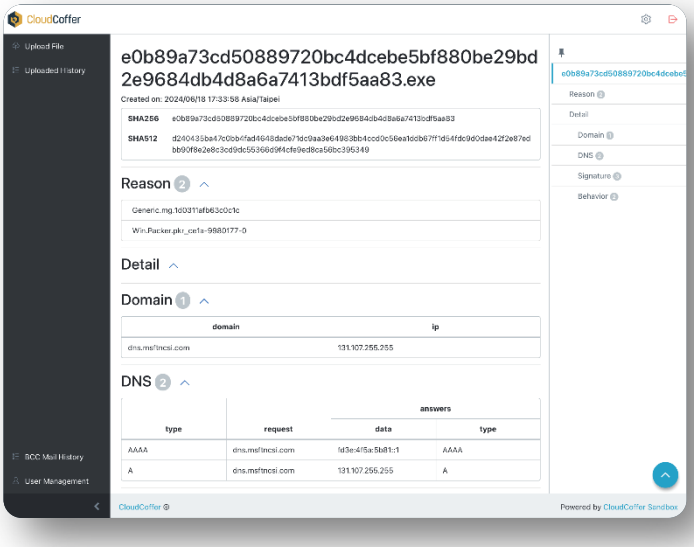
透過對第三方元件的徹底掃描，能提前識別外部代碼庫中的風險，有助於預防供應鏈攻擊的威脅，尤其適用於對供應鏈安全敏感的行業，如金融業、醫療業和電信業等。

全面覆蓋與彈性部署

支持多種作業系統（Windows、Linux、macOS、Android、iOS）和多種文件格式的檢測，並能透過 API 與現有開發環境整合，方便應用於不同規模和需求的組織。



SandSphere 分析摘要說明



SandSphere AI 沙箱分析報告

適用場域

開源軟體開發團隊

適合大量使用開源程式碼的開發團隊，SandSphere 能有效檢測 GitHub、GitLab 等開源平台上的程式碼汙染風險，確保上版安全。

供應鏈管理和第三方依賴

對於依賴第三方模組、外部 API 的企業，SandSphere 能幫助這些企業定期檢查套件庫，確保外部依賴的安全性。

高敏感度行業（如金融、醫療、公共機構）

適合需要強化應用程式安全性的行業，SandSphere 提供的 AI 和大數據分析能更好地應對高安全需求，特別是金融和醫療行業中的數據安全合規需求。

SandSphere 惡意程式偵測平台是一款強大且多功能的安全解決方案，針對第三方程式庫及共享平台上普遍的汙染問題提供了針對性應對措施。藉由結合 AI 驅動的相似度分析技術、沙箱動態分析、及大數據情資庫，SandSphere 不僅能協助開發團隊在上版前識別惡意程式碼及外部依賴的潛在風險，更能加強組織的整體供應鏈安全性。對於需要強化供應鏈管理和確保應用程式安全性的各類企業，SandSphere 是值得信賴的合作夥伴。

	功能	說明
SandSphere 惡意程式檢測系統	惡意行為偵測種類	• 惡意程式與後門偵測：深層靜態和動態分析技術掃描惡意程式、後門及可疑代碼。 • 嵌入 URL 和外部連結掃描：分析程式碼中是否包含惡意 URL、可疑的外部連結或不安全的 API 呼叫。 • 變種惡意程式檢測：SandSphere 的 AI 技術能檢測變異程式碼。 • 動態分析誘發惡意行為：提供沙箱模擬執行環境，通過誘發機制誘使惡意行為驅動。

	偵測作業系統與檔案類型	• Windows
		  • exe, dll, doc, docx, xls, xlsx, .ppt, .pptx, pdf, one, asp, aspx, php, py, zip, .mp3, .mp4, .avi,…etc
		• Linux
		  • sh, .pl, .py, .c, .cpp, .h, .o, .so, .bin, .elf, .deb, .rpm, .tar, .gz, .bz2, .zip, .mp3, .mp4, .avi, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf…etc
		• macOS
		  • app, .dmg, .pkg, .zip, .mp3, .mp4, .avi, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf…etc
		• Android
		  • apk, .obb, .zip, .mp3, .mp4, .avi, .jpg, .png…etc
		• iOS
		  • ipa, .app, .zip, .mp3, .mp4, .avi, .jpg, .png…etc

	系統管理功能	• 具備 TLS V1.3 之 SSL 圖形化加密網頁管理介面。 • 具備多種帳號分權管理群組，系統管理者可依據不同的管理帳號及群組對象套用特定管理權限。 • 提供管理帳號登入管理稽核事件記錄、查詢及匯出功能。 • 具備管理設定檔備份及還原等管理功能。
	型號	**說明**
SandSphere 產品型號	SandSphere-Platform	CloudCoffer SandSphere 原始碼惡意程式檢測系統一年期訂閱服務，內含掃描檔案數量至多3萬個。
	SandSphere-AD2W	擴增模組: CloudCoffer SandSphere 原始碼惡意程式檢測系統一年期 20,000 個檔案掃描增購授權。
	說明	
硬體規格需求	系統運行硬體需求：實體機，VMware 虛擬化系統	
	CPU：X86　32核含以上	
	RAM：64GB 含以上	
	SSD：2TB 含以上	
	實際硬體需求規格數量會因擴充模組增加而提高	