使用 Lucent Sky AVM 來排除靜態安全檢測的不足

企業如何使用 Lucent Sky AVM 來做得比檢測更多，修正應用程式層的安全弱點。

LUCENT SKY

摘要

應用程式層的安全與安全的程式碼是一體的兩面。然而，許多企業和組織將靜態安全檢測結果視為可被忽略的背景噪音，在安全應用程式開發週期（SSDLC）中不斷被拖延。這是因為開發團隊了解傳統的 SAST 工具著重在分析，無法對他們的安全規劃提供實際的影響。而分析本身是無法讓程式碼變得安全的。

分析不能修正任何弱點

我們可以說人可以修正弱點，但是所有的研究都顯示企業修正已知弱點的速度改不上新弱點產生的速度。對絕大多數的企業來說，這不是因為流程不佳所導致的問題：它們的開發團隊多半都已經有報告能指出安全弱點在哪裡。然而，極少數的團隊在不斷持續的軟體開發週期中有時間能夠安排來修正弱點。

這代表傳統的 SAST 工具廠商提供的基本上就是一份報告，來滿足資訊安全流程的要求。SAST 工具所產生的報告，既無法提供關於程式碼安全品質的細節，也沒有實際上提升安全的行動。程式碼的安全品質和應用程式的安全必須同步進行，以跟上 SSDLC 的步調。Lucent Sky AVM 補足了傳統 SAST 工具和快速的開發流程之間的不足 - 沒有時間人工修正弱點。

要確保安全問題無法被忽略，資訊安全工具必須有實際加強安全的能力，而非僅是產生報告。Lucent Sky AVM 在功能上比傳統 SAST 工具做的更多，提供能修正被識別弱點的程式碼 - Instant Fix。Lucent Sky AVM 在一次掃描中，能自動修正多達 90% 的弱點，大幅度降低弱點的數量以及避免在新增程式碼時也跟著新增弱點。

安全分析的結果應該是一個份更安全的程式碼，而不是一份漂亮的報告。使用 Lucent Sky AVM 來幫助開發團隊做的更多。

一個 Lucent Sky AVM 找到的弱點，包括所產生使用參數化查詢來修正 SQL injection 的 Instant Fix。

藉由做的更多，Lucent Sky AVM 也有更完整的報告：包含發現以及**修正**的弱點。報告的重點是已經完成的工作，而非工程師還需要做的工作。

降低報告中的雜訊，同時提高安全性

Lucent Sky AVM 不需要依賴資訊安全專家，就能如傳統 SAST 工具一樣，提供相同的整合、管理與報告功能。

由於 SAST 工具是設計來讓資訊安全顧問所使用，它們在掃描時通常會產生盡量多的結果，儘管其中僅有少部分是真實的弱點。要評估這些結果的風險以及相關的後續處理，依賴專業與時間來排除例如誤報等問題。這種高度依賴資訊安全專家以及人工複查時間的流程，對於大部分的開發團隊來說，都是難以接受的。

Lucent Sky AVM 是針對開發者的需求所設計。它能輕易地和各種開發流程（例如瀑布式開發、敏捷開發等）整合，並且被設計來加速提升安全的作業時間以及降低不必要的雜訊。

符合企業所需的高安全性且支援複雜的佈署環境

要把 SAST 產生的報告轉化為修正過的安全程式碼是一份全職的工作。也因此沒人有空處理它。Lucent Sky AVM 的弱點檢測和修正都是透過既定的規則進行，且可由開發與資訊安全團隊進行集中控管，代表開發者或資訊安全人員能夠完全掌握弱點何時被從程式碼中移除。

- 檢視並與允許 Instant Fix。
- 依照 SSDLC 的最佳方式佈署 - 在建構腳本中、透過 API 或是使用網頁介面。
- 中控的弱點修正：開發者和管理者能更完全控制 Instant Fix 是否被植入程式碼中、何時被植入，以及所使用的安全函式庫，讓他們可以有系統的大規模修正弱點。這也能確保所使用的安全函式庫符合任何適用的法規遵循要求。

結論

Lucent Sky AVM 是一個針對弱點修正所設計的產品，在第一次掃描中就能協助開發者完成他們的工作。弱點分析本身無法讓程式碼變得安全：SAST 工具的報告受限於無法提供任何有意義、實質上的弱點修正。藉由透過既定的規則來偵測和修正弱點，並與 SSDLC 整合，Lucent Sky AVM 能夠在應用程式的根源就將弱點移除，有效提升應用程式的安全性。

關於 LUCENT SKY

Lucent Sky 新開發的應用程式安全科技能在集中控管的環境下，透過自動化的方式將應用程式層的弱點從程式碼中實際移除。

透過整批的移除弱點，僅須一次掃描就能快速提升既有應用程式的安全等級，讓傳統的應用程式能符合最新的資訊安全標準。對於新的應用程式，Lucent Sky AVM 讓開發者能在開發程式碼的同時就確保程式碼的安全性，且透過在根源就移除常見的弱點，有效降低弱點的累積。

與開發同步，Lucent Sky AVM 與 SSDLC 結合，快速又有效率。