有效管理軟體安全的保全計劃（上）
Fortify 軟體安全成熟度模組(SSA)

「保護一個企業的所有軟體的應用組合，包括公司內部、第三方套件、外包與開放源始碼。您需要評估每一個應用系統，並建立一個以風險為基礎的清單以及定義每個環節的安全活動。Fortify 的 SSA 管理模組自動執行此流程，針對整個企業環節提供視覺化的過程與軟體安全狀態。」

--Jim Routh, Chief Information Security Officer, Depository Trust & Clearing Corporation

大綱

一、摘要

軟體安全成熟度(SSA)快速的成為解決軟體安全風險的首選方法。事實上，也是唯一針對軟體安全的方法，提供數位資產最大安全成熟度的保證。為了達到這點，SSA 規定一系列的活動，包括廣泛的定義與移除軟體的安全弱點與加強安全因素於企業現有開發流程與採購流程。

將 SSA 程序納入整個企業對安全團隊來說充滿著許多挑戰。隨著專案增加時，安全團隊在與開發團隊、查核人員、專案經理進行需求討論會議時會經歷許多難處。第一個用來控制情勢的必要步驟為導入與實施安全開發生命周期(SDL)。然而，若沒有有效的自動化交付與追蹤 SDL 中安全活動，安全團隊仍然無法管理所有情況。

為了持續追蹤多個 SSA 專案，Fortify 360 提供 SSA 的解決方案，直接於 Fortify 建立 SSA 管理模組。它提供一個稽核品質、資產、活動與結果等與整體企業 SSA 成果的資訊。對於個人發展專案，SSA 管理模組提供了方便的網頁入口，當進行降低風險活動時，可以查閱、記錄與對談。

對於企業中每一個專案，SSA 管理模組以適合活動為基礎，自動的指派專案具體風險項目。 安全團隊可根據完成或未完成的里程碑警示追蹤專案成果。先進的報告與儀表版可提供快速統整所有專案的成果，並確定施行等級與改善項目。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3 TEL:(07)586-6195
海外據點：上海、北京、東京

有了這些功能，安全團隊可以開始走向例外管理辦法來達成 SSA，節省時間去執行其他更重要的活動。此外，若企業正在尋找快速推行 SDL 的方法，Fortify 提供了 SDL 樣板與最佳實例供參考。這些樣版提供有效且立即可用的 SDL 實作。若參照這些樣版，可以大大減少開發 SDL 所需的額外付出。

二、軟體安全成熟度(SSA)程序的四項挑戰

安全團隊的許多挑戰是面對整個企業 SSA 程序的部署與管理，多數的案例中，因為安全團隊很小，但卻要確保許多大型的、複雜的且不同類型的軟體環境。

許多企業擁有數百，甚至上千個正在發展中的專案；有些分散於不同的地點。從安全的角度來看，有一些專案是重要的，如有些會接觸到敏感的資料，有些則否。專案或專案元件有許多不同的來源，如內部發展的、外包、採購或採購開放原碼軟體。其中一些專案已經部署於線上作業，必需立即處理，其他尚在發展階段的都可以適用於安全改善工作。

為了讓安全團隊可以確保所有的安全。發展應用程式與安全的人員比應為 150 比 1，但實際上多數的比例遠高於 300 比 1。

在這些情況下，一定要有排定優先順序的能力。企業常常透過安全開發生命週期(SDL)做為開始。SDL 確保軟體專案在各個階段考慮安全的部份，如此將需求併入發展計劃中。

當採用 SDL 可以確保專案的安全關鍵問題，但他並未考量完整的 SSA。為此，專家建議風險排名的方法來管理 SSA，包括維護應用程式的清單與元件；以風險分析為基礎，為每個應用程式建立一套政策，並舉出具體的活動。這些活動也許是根據企業的 SDL，或是透過外包完成。

採用這種方法，安全團隊可以確保企業大幅降低風險(還有其他的好處，將進一步討論)。

此外，對於許多企業而言，風險與安全要求遵循如 PCI、FISMA、HIPAA、SOX 與 NERC 等法規。遵循這些法規帶來新的挑戰：如何快速的讓企業證明符合這些條件。

這一切聽起來合乎邏輯，但很難想像的是這方面的工作完全沒有有效率的自動化。事實上，導入 SSA 有四項主要營運的挑戰：

挑戰一：維持一個考量所有專案與應用程式狀況所需的觀點。

正如前述，安全團隊必需處理內部與外部不斷增加數量、規模與複雜度的應用程式。在 SSA 程序中必要的元素是能維護一個精確的應用程式清單其中包含關鍵商業邏輯與技術。企業採用後可以發現到有一個精準的軟體清單可以快速評估威脅等級、排定優先順序、滿足法規遵循、舉證與制定回應計劃。

許多企業的挑戰是持繼更新清單。多數的安全團隊依據表單與電子郵件去發展追蹤清單。但這些工具的功能無法跟上發展專案更新的速度。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3　TEL:(07)586-6195
海外據點：上海、北京、東京

在其他案例中，安全團隊嘗試不透過開發團隊自行佈建系統，但由於缺乏控制導致難以管理。這些都可能導致缺乏能見度、無法有效安排安全人力與定義優先順序。

挑戰二：建立適合的安全政策並貫徹執行。

除了一個廣泛的應用程式清單外，安全團隊必需建立一套安全政策，決定在部署前的清理應用程式時應執行什麼活動。例如威脅模型文件、結構檢討或移除已知的弱點。

建立這些政策可以說是個耗時的工作，需要實際的研究與溝通協調企業內部。採用 SDL 可以處理企業內部的發展項目，但對於外包或開放原始碼的專案，也需制定一套軟體的發展政策，因為這些專案也有可能將弱點帶入企業內部。

活動的指派也是一項有挑戰性的任務。正確的決定專案的活動需要專案經理與安全團隊持續地溝通。為了確保稽核的結果，指派作業必需一致，在該專案中相同的風險分類需指派相同的活動。每個專案的活動被定義後，安全團隊必需能追蹤這些活動直到專案完成。

挑戰三：回應質詢

安全團隊定期收到管理階層、企業主與稽核員的質詢像是完成了什麼？還需要做什麼？何時能完成或是即將完成？在稽核時安全團隊可能被要求重現應用系統曾發生的活動，並提供相關的文件。同時也要求證明符合一致的程序。

挑戰四：識別趨勢

要達到真正有效，安全團隊必需保有領先的優勢，並且極積主動。是否有特別專案持續在苦鬥？可以透過訓練改善嗎？某些開放原始碼的軟體元件造成延遲？是否被其他開放原始碼的軟體使用？

三、Fortify SSA 管理模組介紹

Fortify 已制定了全方位的解決方案，幫助企業改善 SSA 計劃，提供一套強大且可重複施行的 SDL，具有安全相關活動追蹤與管理程序。Fortify SSA 管理模組提供五大關鍵功能：

功能一：建立與管理應用程式的詳細清單

SSA 管理模組提供了一個集中的介面可用來定義與搜集應用程式的前後相關資訊。提供安全團隊在單一系統中可取得所有專案的記錄。SSA 管理模組介面可完全客製化，且允許安全團隊建立他們需要的專案項目。根據 Fortify 設計/發展超過 400 個具體專案的經驗，SSA 管理模組透過問卷即可立即建立。問題可分為三類：

1. **專案屬性**
   a. 列出所有專案與元件、函式庫間的關係。使用者可以透過現有的系統做選擇。
2. **企業屬性**
   a. 專案的風險等級為何：高、中、低？

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3　TEL:(07)586-6195
海外據點：上海、北京、東京

b. 專案處理什麼類型的資料：客戶資料、員工資訊、企業 IP？

c. 專案是屬於內部或外部使用？

d. 什麼業務單位開發此專案？

e. 什麼法規是一定要遵守的？

3. **技術屬性**

a. 專案的類型：函式庫、元件或完整的應用程式？

b. 專案是內部開發、外包還是授權？

c. 此專案處於何階段：部署中、開發中、新開發

d. 專案屬於什麼平台？

e. 用什麼語言開發的？

對於企業而言，已有一個清單管理系統，SSA 管理模組可以透過 Web Services 介面輕鬆的存取與使用。SSA 管理模組具有延展性，在系統間容易達到資訊的搜集與推播。

功能二：建立一致的安全政策與實行

以風險分析基礎建立，SSA 管理模組提供 10 種不同的樣版，每組需遵循不同的安全活動。這些樣版除了提供可立即使用的安全政策範例外，也可以完全的客製。有了這些樣版企業可以針對不同的應用系統使用一致的安全政策。

10 個樣版對應不同類型的應用系統：

1. 新開發專案具有高風險
2. 新開發專案具有低風險
3. 開發中專案具有高風險
4. 開發中專案具有低風險
5. 第三方的開發專案具有高風險
6. 第三方的開發專案具有低風險
7. PCI 法規
8. 開放原碼軟體
9. 第三方
10. 基本安全檢查

每個樣版包含多達 40 個不同的安全活動。若組織已有一個標準樣版，可以更輕鬆的加到此系統。

以下是各樣版皆會出現的特定活動：

- 上傳 abuse case 文件
- 上傳威脅模型文件
- 上傳架構檢討後文件
- 上傳程式碼分析文件
- 移除程式碼中高風險弱點問題

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3　TEL:(07)586-6195
海外據點：上海、北京、東京

- 上傳滲透測試結果
- 移除 OWASP TOP 10 弱點
- 部署應用系統防火牆

功能三：構通與追蹤

SSA 管理模組提供 Web-Based 介面，讓各個開發團隊與安全團隊做為管理入口。開發團隊可以登入，找到自己應用系統，查閱被指派的工作並可下載相關文件如威脅模型等。當指派完成時，開發團隊可以在 SSA 模組中記錄並上傳相關文件。

當安全團隊開始清查的過程中，SSA 管理模組具有探索部署專案的能力。個人開發團隊可以註冊並回答關於該專案的問卷。SSA 管理模組可藉由此資訊產生符合專案風險或儲存資訊的活動，並可透過 360 Server 進一步的分析。

因為他使用標準網際網路的技術，並包括一個強健的安全模型，外包夥伴也可用同樣的方式部署。

安全團隊或開發團隊的領導者可以以管理者身份登入，檢視所有/部份的應用系統。他們可以決定是否要簽核結果。他們還可以看到安全活動是否已完成與目前階段。

功能四：回應質詢

SSA 管理模組提供了一個安全團隊的功能，開發團隊的領導與資訊長(CISO)可以快速回應任何質詢關於現在或過去專案效能與專案狀態。呈現結果的儀表版允許安全團隊快速的回答問題。舉例來說：

- 有多少應用系統是必需遵守 PCI 標準？持續多久？有多少的外包應用系統是屬於高商業影響？應用系統中已完成何種安全活動來確保安全性？
- 我們從軟體供應商獲得什麼應用系統？那些是已經上線作業？對已針對那些應用系統進行什麼評估？

功能五：收集資料並產生趨勢報告

SSA 管理模組提供具有時間趨勢的報告給管理者。舉例來說：

- 外包的應用系統需要花多少時間達到完全的安全？
- 內部開發的應用系統需要花多少時間達成？
- 那一個團隊產生最高的弱點比率？
- 那種弱點是各個隊團都會發生的？

下期待續...

GSS 叡揚資訊 Galaxy Software Services
台北總公司：台北市 10461 中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：高雄市明華路 315 號 13 樓之 3　TEL:(07)586-6195
海外據點：上海、北京、東京