淺談應用程式安全與 SIEM 之整合(上)

原文來源: HP 提供

翻譯整理: 叡揚資訊 資訊安全事業處

摘要

本文中將簡述 **安全的程式開發(Secure Application Development)**，進而深入 **應用程式安全之監控(Application Security Monitoring)**，最後討論 **應用程式安全之監控(Application Security Monitoring) 如何與資安事件管理(SIEM)結合**，提供最高層次的應用程式監控與攻擊偵測。

資訊安全為什麼必須轉移焦點到應用層?

傳統區域聯防已被打破

大多數資訊安全專家認為，server、endpoint、network 區域聯防的舊模式，出現了幾個趨勢：

1、**區域聯防已出現太多漏洞：**駭客可以利用 mobile 設備、遭入侵網站、社交網路應用程式、以及其他尚未受到完整保護的路徑，進入企業網路。

2、**網路犯罪分子已經變得更複雜、更具針對性、且更有耐性：**他們利用網路釣魚和社交工程來擷取用戶憑據，然後利用技術逃避傳統檢測的網路和主機安全產品，來提取機密數據如信用資料。

3、**企業已無法再一手掌握全部的資訊架構：**越來越多企業都在導入及使用 software-as-a-service (SaaS)等虛擬化系統以及雲端架構，導致難以直接監控和管理。

越來越多的威脅只能被業務邏輯層面偵測到

因此還有第四項因素須考慮：

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

4、極多的潛在資安危脅只能從業務內容及業務邏輯面去分析了解：內部威脅、詐欺以及來自商業對手的攻擊，並無明顯及簡單的徵兆可被傳統區域聯防資安設備偵測，這些徵兆僅可能透過行為模版以及樣本來辨識，而大多時候這些行為模版僅可用於某些相關類似產業，甚至於是單一特定組織。

將注意轉移到應用程式(application-level)安全

對於上敘趨勢合乎邏輯的反應是：不僅要使用傳統的安全工具繼續深入防禦戰略，也要轉移更多的資源及注意力到 application level 安全上。事實上，加強 application level 安全有許多好處：

- **對於犯罪及詐欺攻擊提供更佳的防護：**依據近來資安統計顯示，主要之資安弱點存在於應用程式以及網頁軟體的漏洞，但大部分組織僅花費極少比例的經費在監控及保護軟體上。
- **法規遵循更簡單：**極多政府法規及產業標準，均有規範各別之業務機敏性資料防護準則(如客戶帳號、健康狀態、持卡人訊息等)，應用程式之資訊安全措施更能夠直接顯示法規遵循的狀態。
- **將商業標準、營運政策、資安政策緊密結合的機會：**當有人違反相關法規及標準時，應用程式資安措施能給予管理者警示。

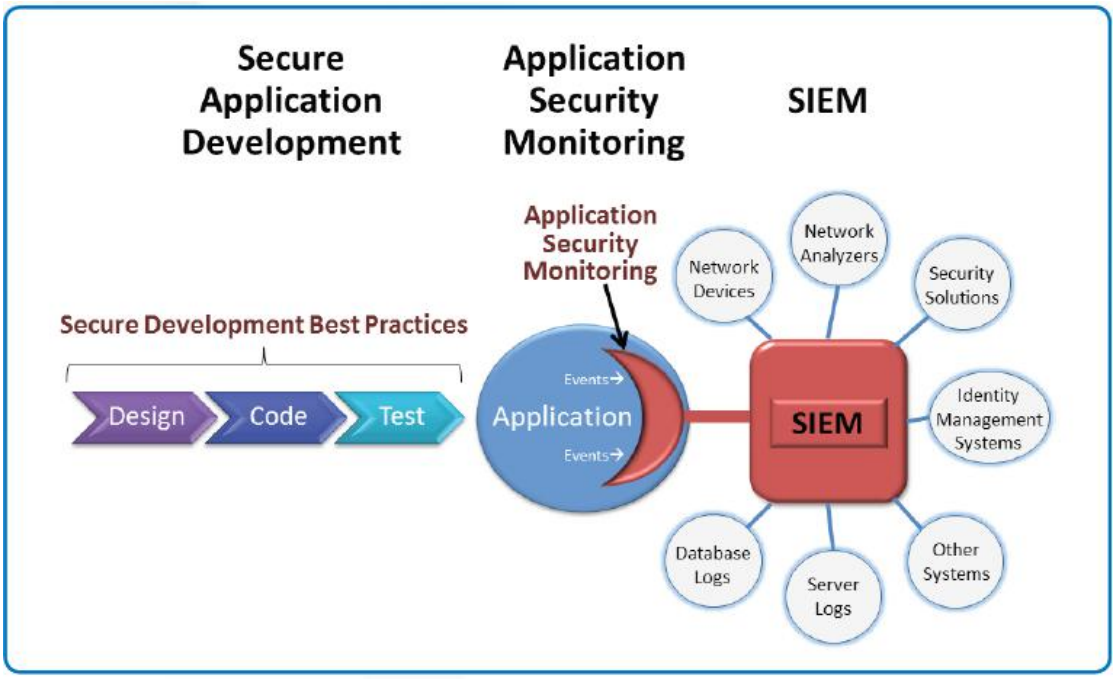
簡而言之，越好的監控及對應用程式層級的安全保護，將達成更少的資料外洩、更快的稽核效率、以及更多可預期性的運作狀況。

應用程式安全之三元件

應用程式安全的三元件主要為：安全的程式開發(Secure Application Development)、應用程式安全之監控(Application Security Monitoring)、及資安事件管理(SIEM , Security Information and Event Management)，如圖一所示。

在本文中將簡述安全的程式開發 (Secure Application Development)，進而深入應用程式安全之監控(Application Security Monitoring)，最後討論應用程式安全之監控(Application Security Monitoring)如何與資安事件管理(SIEM)結合，提供最高層次的應用程式監控與攻擊偵測。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787



圖一：應用程式安全三元件：安全的程式開發、應用程式安全之監控、資安事件管理

安全的應用程式開發(Secure Application Development)

軟體開發生命週期的最佳實踐

安全的應用程式開發(Secure Application Development)為建構安全最佳作法之程序，並融入軟體開發生命週期(SDLC, software development life cycle)的每個步驟，以縮減程式源碼中的弱點。

此包含：

- 於 SDLC 收集資安要求的階段，分析安全要求並執行威脅模式
- 於設計階段，遵循訂定之資安標準
- 於開發階段，執行並實施安全程式碼撰寫，及以安全為導向的程式碼複審
- 於測試階段，執行靜態程式碼分析，及動態 web 掃描測試
- 於部署階段，執行以安全為導向的實際部署審查

組織亦可以善用資源，例如 OWASP TOP 10、美國國防部及國防資訊系統局發布的內容、PCI DSS 及 HIPPA 等標準，或其他已知的常見弱點及應用系統安全實踐方式。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

安全應用程式開發之限制

然而，組織也須了解安全應用程式開發之限制：

- **適應過程較慢：**一般而言，訓練架構師、程式設計師、品管測試者，並且將程式安全融 SDLC 各個階段，將花費數年時間。
- **委外開發的程式碼：**組織無法將自訂之安全程式開發標準，實踐於軟體供應商。
- **舊有的應用程式：**對於原有的應用程式，通常已經無法加改安全性語法、以及套用新的安全開發標準。
- **不斷變化的威脅：**面對新出現的威脅和攻擊，需要新的對策，但往往無法納入既有的應用程式。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787