淺談應用程式安全與 SIEM 之整合(下)

原文來源: HP

翻譯整理: 叡揚資訊 資訊安全事業處

應用程式安全監控(Application Security Monitoring)

第二個應用程式安全的關鍵為「應用程式安全監控」(請參考圖 1)。這表示當應用系統發生異常行為時，監控功能即會對系統管理員發出警示，其中異常行為包括：

- 駭客或未經授權使用者入侵的跡象
- 發生已知的攻擊手法，例如 SQL ingection、cross-site scripting、remote file inclusions
- 不常使用特定資料、要求異常資料量的使用者，意圖存取特定的安全資料

上述行為可以被紀錄，並且對系統管理者與資安人員發出警示。

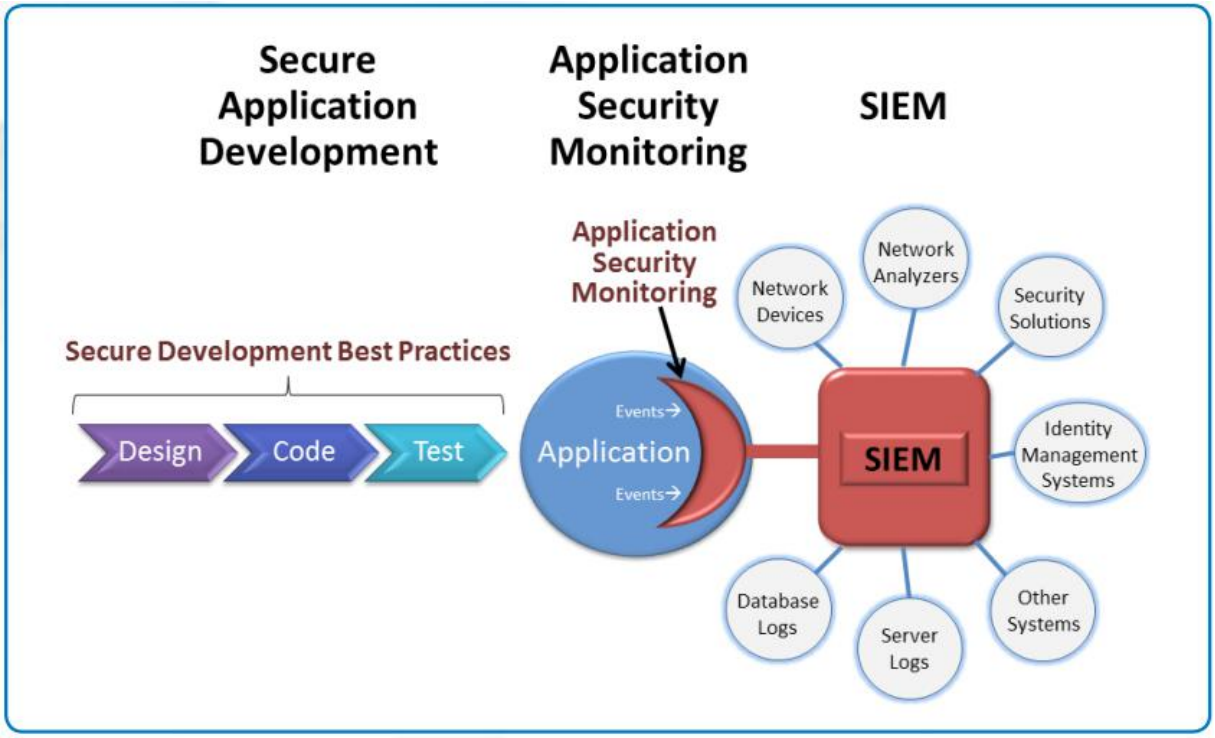


圖 1、應用程式安全三元件：安全的程式開發、應用程式安全之監控、資安事件管理

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

關於「應用程式安全監控」有兩種方式：將監控機制寫入每個程式的原始碼中、或建構一套應用程式安全監控(Application Security Monitoring)工具。

監控每個應用程式

有些單位將監控機制寫入每個應用程式中，這更進一步提供資訊將軌跡和監控跟各行業商業邏輯結合，然而這種做法實際上還是有很多缺點：

- 絕大部分軟體程式是為了處理一般使用事件，而非例外及非法妄用事件。開發者可能沒有相關經驗或知識，能先考慮所有可能的攻擊和妄用，或是編寫複雜邏輯來偵測刺探、未授權之資料存取以及其他各種攻擊。
- 大部分軟體發開人員使用的應用程式稽核機制，所能收集到資訊相較於資安監控所需的廣泛度而言，實屬太少。他們所紀錄的軌跡事件，通常非標準格式、並且難以跟其他的應用程式或系統軌跡作關聯比較。
- 大多數機關使用過時軟體或第三方套件，因此若要將此應用程式更新成有監控能力，將是非常不可能的事。

最後，很多精緻攻擊以及詐欺型態，單靠監控單一應用程式是無法被偵測出的，只能藉由關聯多個應用程式或橫跨應用程式、防火牆、入侵防禦系統和其他網路及資安設備。

應用程式安全監控工具

應用程式安全監控工具是「內嵌」於應用程式中，觀察應用程式以及使用者活動狀態，並可鑑別異常活動。

例如，應用程式安全監控工具可偵測：

- 網頁表格內之資料欄位，包含 SQL 語法
- 隱私資料被傳送到外部網路上
- 使用者從一個非屬於他的國家 IP 位置登入，且是在凌晨三點
- 在客戶帳號資料庫中，查詢並下載異常量的資料
- 業務人員存取含有機敏性資料的工程資料庫

一部分的可疑活動可以用純技術方式解析(如 SQL injection 攻擊軌跡)，而其他活動則須靠其是否違反商業邏輯行為(如銷售員突然存取工程文件)，這種使用商業邏輯判斷能力是無法獨立於應用程式監控資安工具之外。

應用程式安全監控工具相較將監控碼寫入個別程序中，具有一些主要優勢：

- 廣泛吸收軟體廠商以及其相關客戶被攻擊、妄用和偵測可疑活動的方法

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

- 可收集、正規化及紀錄各種類型應用程式資料，來補齊一般應用程式中的軌跡不足問題
- 可被派送至舊款及套裝應用程式，無須更動這些應用程式或是開發客製化軌跡
- 可使用事先設計好的方式來產生客製化規則
- 在一些案例中，可直接往外擴充與 SIEM 系統介接

結合應用程式安全監控(Application Security Monitoring)及資安事件管理(SIEM)

SIEM 系統從各地聚集資安及軌跡資料，包含路由器、 gateway(閘道)及其他網路設備，如防火牆、入侵防禦系統及其他資安方案元件；資料庫、主機及其他系統軌跡及位址清單、鑑別管理系統，SIEM 系統可以關聯這些巨量資料並且給予操作員警示以及保護個人資料被刺探、攻擊、資安政策違例，內部未授權活動，以及其他違反資安的指導。

應用程式安全監控工具能將資安事件導入 SIEM 系統，所以應用程式相關資料能夠與網路、資安事件及其他系統資料關聯(見圖 2)

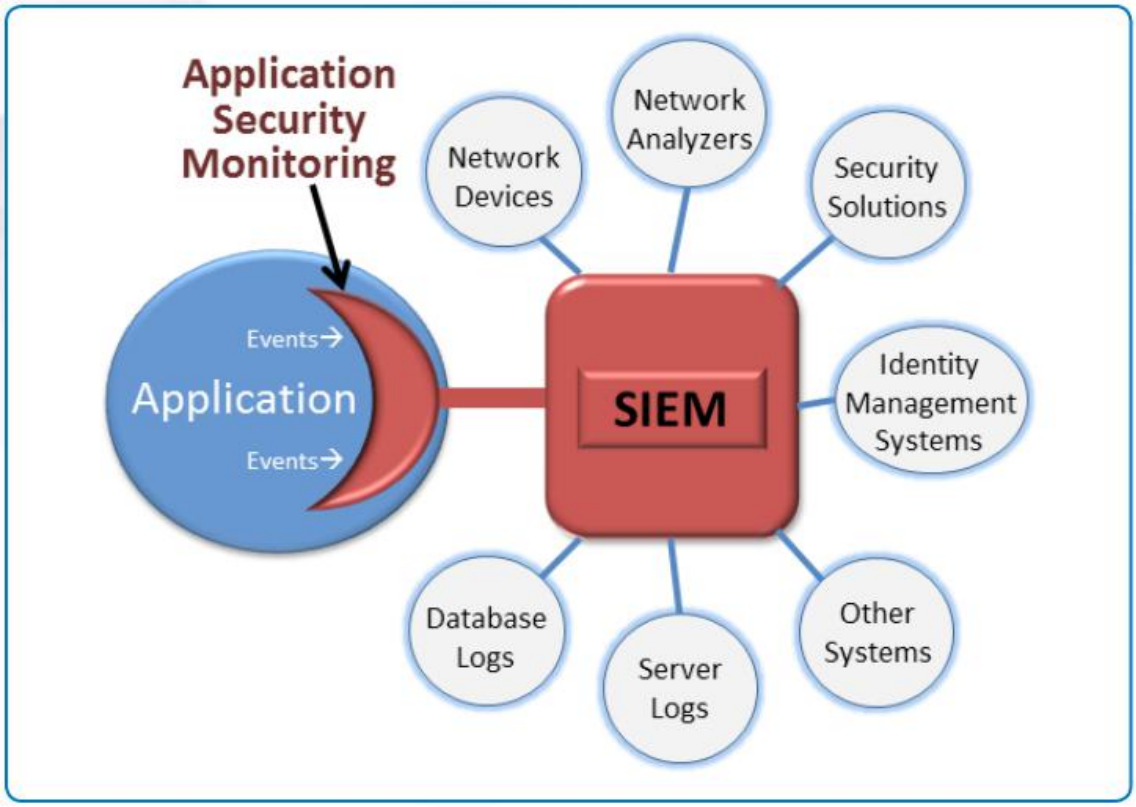


圖 2、應用系統安全監控工具可以匯集事件資料到 SIEM 系統，做關聯分析

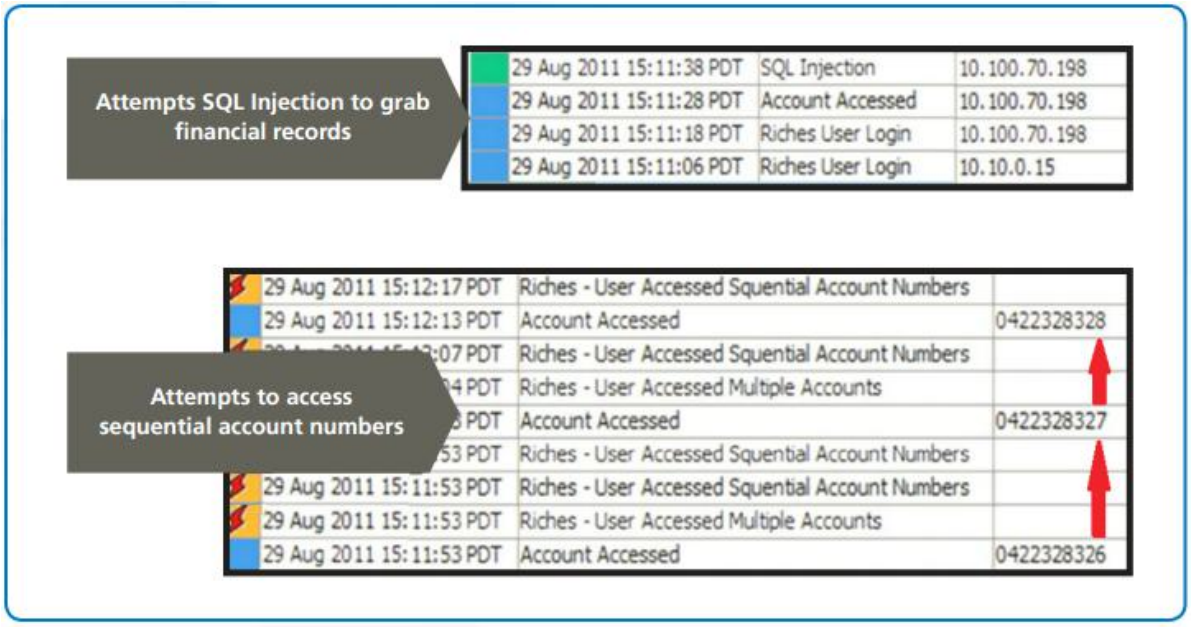
GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

事實上，應用程式安全監控工具與 SIEM 系統是非常強而有力的組合，因為結合此二者能夠鑑識一般技術上難以捉摸的行為模式。且這種組合對於各行業以及產業別的商業邏輯特別有效及具優勢。

金融業相關範例

以下是特定產業的 scenario 介紹：應用程式安全工具正監控著客戶帳號管理程序。在捕抓客戶登入證明時，工具偵測到 SQL injection 攻擊 (圖 3 上)，之後又發現一位使用者使用這些登入證明來查詢帳戶資料庫(圖 3 下)。

這些事件被導入 SIEM 系統後，關聯規則偵測到這位使用者行為違反其正常模式，並且這些帳戶正被依帳號號碼順序被逐筆存取，SIEM 系統的 customer rule 指出這是高可疑性活動，因為單個客戶不會有接續編號的帳號。所以 SIEM 系統把此使用者列入高可疑份子清單，並且通知金融機關防詐小組。管理者同時先封阻此使用者的資金流動，防止網路犯罪者將資金移至海外。



圖三、應用程式安全監控工具偵測到 SQL injection 及不正常的帳戶登入，SIEM 系統可以辨識這些複雜的攻擊手法並通知系統管理者

這個案例展示 Application Security Monitoring 工具和 SIEM 系統能夠一起運作，並使用特定行業的商業邏輯規則，來偵測使用迂迴閃躲、複雜、多層次攻擊。

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

結論：應用程式安全監控及 SIEM 案例

強化應用程式監控的趨勢，正不停被以下狀況所推進，包括被傳統區域聯防及主機安全產品、與日俱增精緻的駭客攻擊及內部威脅、當某部分架構位於 SaaS 以及雲端運算端點所產生的資安挑戰。

但也反映出其加值行為當使用此新技術 Application Security Monitoring，特別是與 SIEM 系統結合時。

其優勢包含：

- 對於犯罪攻擊者及內部資安危脅，提供更佳的防護
- 透過更好的監控應用程式及使用者行為，來簡化政府法規及各行業標準的遵循複雜度
- 更有效率的使用客製化商業邏輯及商業情境，來偵測特定產業及公司的詐欺和精密攻擊

HP Enterprise Security：應用系統安全監控的最佳選擇

HP Fortify RTA 的優勢包括容易部屬、偵測廣泛攻擊種類、可製作複雜的商業邏輯、並客製化被攻擊時的反應。

HP ArcSight ESM 為領先業界的 SIEM 平台，能將多種系統及 device 的大量資料收集，進行關聯分析。

被 HP Fortify RTA 偵測到的資安事件可以匯入 HP ArcSight ESM，並將資料與 ArcSight ESM 於其他系統收集到的資料進行關聯分析，不需另外特別進行整合。

若有任何問題，歡迎參考：

http://www.gss.com.tw/index.php/rta

http://www.gss.com.tw/index.php/arcsight-esm

www.hpenterprisesecurity.com.

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