SANS 2012 年日誌和事件管理研究報告: Sorting Through the Noise (上)

資料來源：http://www.sans.org/reading_room/analysts_program/SortingThruNoise.pdf

翻譯整理：叡揚資訊 資訊安全事業處

Executive Summary

在 SANS 的第八屆年會日誌和事件管理的調查中，其中主要的發現是許多企業無法將正常的系統日誌從日常日誌事件中辨別出來。600 多名受訪者回覆，他們覺得最重要和最棘手的問題是，從自己的系統日誌中找出，並且檢測和追蹤可疑行為，以便可供司法鑑定分析和證明合乎法規性。隨著攻擊變得越來越複雜，IT 人員和資安工作人員必須知道他們要什麼才能維護資訊安全，不只是被動的針對已知弱點進行修補，也要能主動的對未知弱點進行防護。這個問題的關鍵是日誌管理。

根據每年一次的調查結果，本次調查的受訪者有著更多的資訊。今年的調查結果，由於日誌管理技術的不斷成熟，企業希望能從日誌數據中得到更多有意義和可運用的結果。現在幾乎所有的日誌管理產品，都有一個或多個的處理器來進行資料的擷取，分析和警報。

在本次調查中，有58%的企業報告表示，他們使用的日誌管理系統來收集和分析日誌。此外，37% 的受訪者表示，他們所使用的安全資訊和事件管理（SIEM）系統的部份功能，22% 表示他們完全使用到 SIEM 系統的所有功能。

有相當大比例的企業 – 22% 的受訪者表示，他們很少或根本沒有自動化日誌分析系統和沒有打算要採用的計劃。沒有自動化日誌分析系統的最常見的原因包括：缺乏時間和預算。受訪者認為，另外兩個原因：缺乏管理階層的支持和沒有足夠的時間來評估不同的 SIEM 和日誌管理產品。

如同過去兩年，今年的調查結果指出該企業正試圖從他們的日誌管理系統中盡可能取出可運用的數據，如果能用 SIEM/事件管理系統來進行關聯分析，會是一個很好的方法。然而他們仍然與新的威脅奮戰，並且從網路中過濾出可運用的數據。即使有 22% 的受訪者有使用 SIEM 系統來收集和分析資料，但有同樣比例的受訪者表示要透過 SIEM 來避免資安事件和偵測新的威脅是很困難的。

這樣的結果指出，當企業遇到網路危機時，不管是使用日誌事件管理系統或是以往的日誌管理方式，要找出事件主因有如大海撈針一樣。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

Why Collect Logs?

根據 2012 年的 Verizon 資料洩漏調查報告[1] ，對執法人員和管理者面臨的最大挑戰之一是無法識別駭客的攻擊，該報告顯示，在許多情況下，企業無法識別駭客的原因是因為沒有足夠的日誌資料。

這個原因直接呼應到我們調查的受訪者所認為的最大問題。當問到以下 12 個收集日誌資料的重要理由(圖一)時，最被重視的都是與內部與外部的資安相關問題。

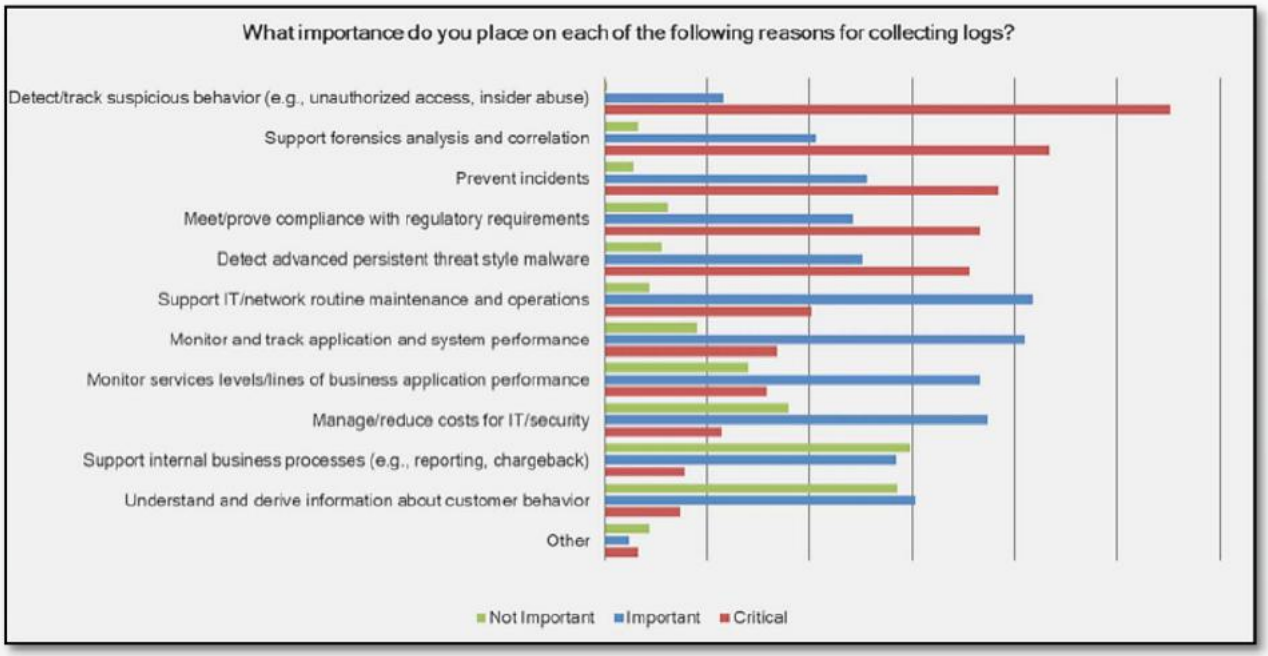

Figure 1. Why Collect Logs?

預先的威脅偵測也很重要（54%），使用日誌資料，以符合法規性要求（55%）。這些結果與和我們先前的調查的一致。今年的問題已經有改變，避免與上一年的問題類似。

許多受訪者還收集日誌資料來幫助公司運營和業務的改進，包括IT運行和證據保全、應用程式和系統效能來監測服務水準和其他業務。這是 24%~30% 的受訪者認為是重要的。

從我們在 2005 年開始調查收集日誌資料的原因，其中之一就是為了符合各式各樣的政府的法令法規要求。

今年，一個收集日誌資料理由的調查，有 55% 的人表示，符合政府的法令法規要求是非常重要的，36% 的受訪者表示是重要的，其餘 9% 的受訪者表示並不重要。幾乎所有的受訪者（除為 0.3%）表示，檢測和追蹤可疑的行為是非常重要的。這是在 2008 年的調查中，日誌資料收集的首要原因。

1 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z037

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

Changes in Log Collection and Analysis

同年 SANS 進行了第一次日誌管理調查（2005年），創造了 SIEM(Security Information and Event Management) 的名詞[2] 。「SIEM」包括收集的日誌數據，以及從各種來源不同的日誌事件的相關性，再加上可疑的事件訊息，透過特定廠商導入的功能，如儀表板，即時報警，報告和圖表，可從這些資料找出關連。

在 2005 年，受訪者是利用手動或自動運行的 script 來不斷的收集日誌資料。這些年來，我們預測日誌管理系統最終會具有完全自動化的關聯，分析和報告功能。今年的調查顯示，企業正在建置日誌系統安全和事件管理系統，使其能有更好的分析的能力和更詳細的報告。

今年，我們試著找出傳統日誌分析工具的比例和使用 SIEM 的比例。當然，這兩個產品是有明確的定義，因為這些工具之間的有功能是重疊的。例如，如果一個企業收集日誌系統是使用 script 來計算連入或連出的網路端口的數量， 並且可以顯示所對應的應用程式，是否會被認為是 SIEM？也許不會，但如果有更好的自動化和智能化功能，有可能會被認定為是 SIEM。

要了解受訪者如何分析和關聯系統日誌和安全訊息，我們請他們勾選以下選項，以確定他們的日誌收集活動，根據以下類別：

- 直接從主機中收集日誌資料到日誌事件管理主機
- 從 syslog (UDP/TCP) 收集日誌資料到日誌事件管理主機
- 使用 agent 從來源設備中收集日誌資料到日誌事件管理主機
- 使用 Security Information Event Management (SIEM) 對其它設備 (e.g., log server) 收到的日誌資料進行關連分析
- 使用 SIEM 來收集日誌資料，並對其進行關連分析
- 以上皆非

收到的回覆中，包括直接或透過 syslog 或 agent 發送多種日誌資料到一台日誌事件管理主機。

有 22% 表示，他們使用 SIEM 收集和分析日誌數據。有 58% 仍然使用日誌事件管理主機，比例是很高，如圖2 所示。

[2] http://en.wikipedia.org/wiki/SIEM

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

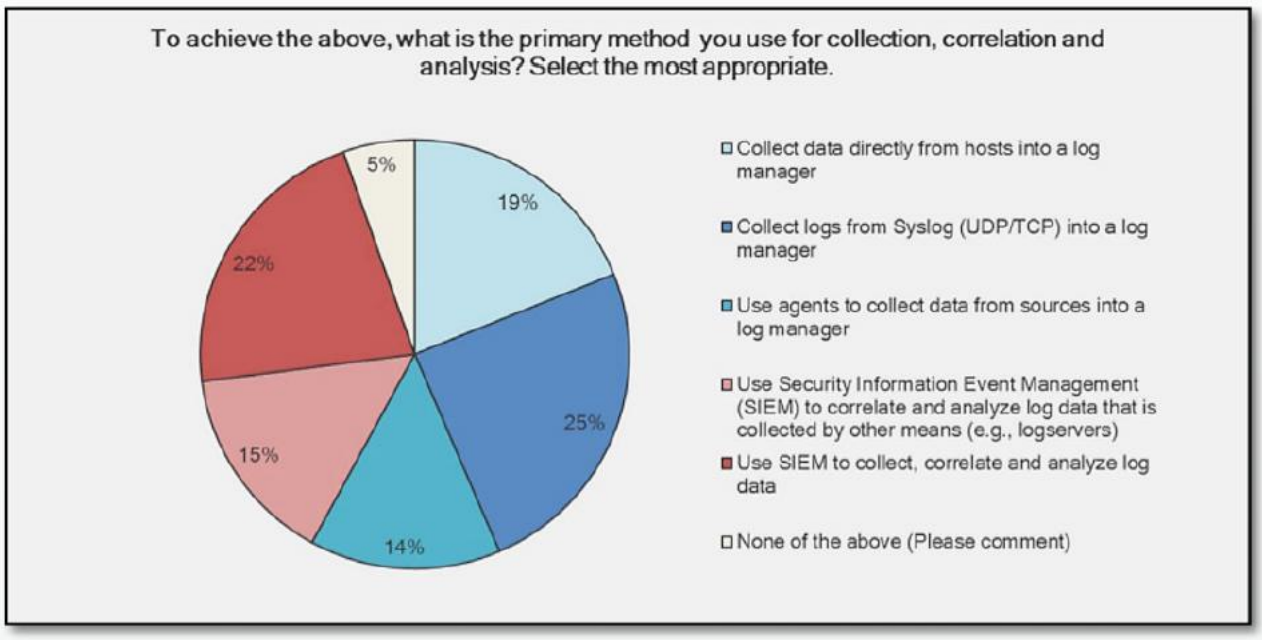

Figure 2. Methods of Collecting and Analyzing Log Data

在另一個問題中，問到有關於日誌事件管理軟體的種類，我們發現許多受訪者使用自行開發的軟體和商業版軟體，所以有一些重覆的受訪者選擇了這些選項。

前三個選項（如圖中的藍色色調）與日誌管理，第四個選項是一個混合的 15%，第五個選項（暗紅色），是都使用 SIEM。在未來幾年內我們將看看這些數據如何改變。

<下期待續>

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓　TEL：(07)586-6195
海外據點：上海、北京　營業範圍：兩岸三地及日本　www.gss.com.tw