Feature

資訊安全持續監測解決辦法的實現—個案研究

Implementing an Information Security Continuous Monitoring Solution—A Case Study

作者：Tieu Luu

is a director of research and product development for SuprTEK, where he leads the development of innovative products and services for the company, including the PanOptes Continuous Monitoring Platform.

譯者: 黃淙澤，電腦稽核協會秘書長/ 網站服務委員會主任委員

美國政府問責局（GAO）引用了2006年至2012年間，美國電腦緊急應變小組（US-CERT）的報告表示，網路安全事件的數量增長從5,503至48,562，高達782%的增長[1]; 同時，由於網路攻擊技術的持續增長，以及越來越多人使用這些技術以獲取情報和進行破壞，政府部門的電腦系統和網路威脅將繼續增加。

為回應此日益嚴重的威脅，美國政府成立以建構持續監控的聯邦資訊系統為目標的跨部門機構（CAP）[2]，以便可持續且及時進行資訊安全風險評估，並做出快速因應，以支持組織的風險管理決策。在2013年11月，美國行政管理和預算局（OMB）發布了一份備忘錄M-14-03，要求所有聯邦部門和機構建立資訊安全持續監控（ISCM）機制[3]，美國國土安全部（DHS）被委以重任協助所有部門和機構，以幫助他們實施並通過此項目。

為遵守OMB任務，IT工程與服務公司SuperTEK承包一個大型美國政府機構工程專案，以建立一個持續監控系統，負責監控分佈於全球的百萬部設備。該系統能使客戶改善其風險和脆弱性管理之認可，以及管理流程之合規報告與安全配置，大大提高了其系統的安全狀態，此自動化程序比以往的人工流程節省無數時間。

ISCM之定義

何謂資訊安全持續監控（ISCM）？文獻說明這是一種“為保持持續的資訊安全，以及對於漏洞和威脅的認識，以支持組織的風險管理決策。”[4]這表示不斷地收集資訊，以提供部署在企業網路中對所有內容的全盤了解以及利用這種資訊評估進行安全策略和漏洞的合規性。此種資訊為IT經理提供一個全面且最新的財產清單，也讓他們明白如何對網路容易受到攻擊之處進行防禦配置。同時也可以幫助系統管理員可以考量企業的資訊治理而不只是根據漏洞來進行修補。此類資訊也提供每個系統的最新安全組態資訊，使管理員能夠正確地決定系統若有關鍵問題未解決前應否被准許上線。此類收集的資訊也有一套風險評估機制以來量化整個企業的安全狀況和需優先考慮解決的問題，讓企業管理階層可以決定如何配置IT資源。

實施架構

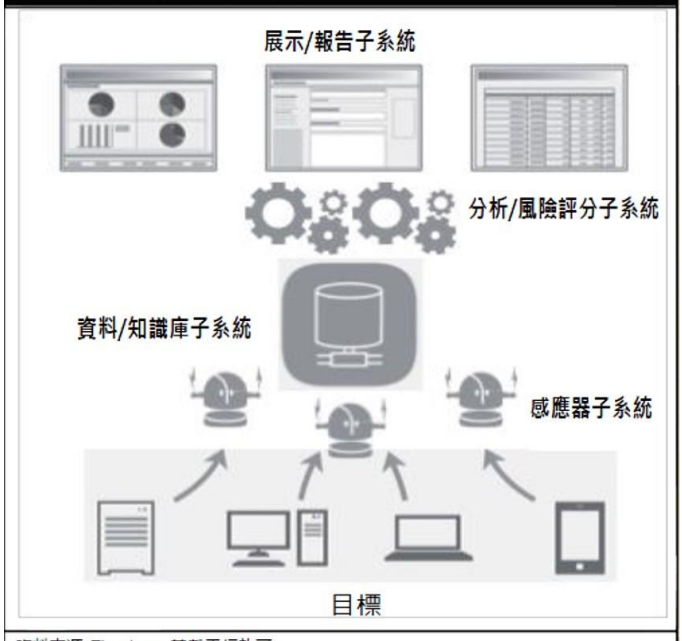
持續性監控系統基本上是一種資料分析應用程序，在圖1中是描述較高層級的持續性監控系統架構，類似於最典型的資料分析/商業智能（BI）的應用程序。美國國土安全部稱此持續性監控系統架構為持續資產評估，狀況認知和風險評分（CAESARS）參考架構[5], 目前已有美國國務院（DOS），美國國稅局（IRS）和美國司法部（DOJ）等三個美國聯邦機構已成功實施此持續性監控解決方案：

CAESARS參考架構表示ISCM和風險評分系統的基本功能部件，如在圖1中所描繪CAESARS定義的4個子系統分別為

- **感應器子系統--** 負責從目標（即資產或設備，例如在企業的網路運算和移動設備）中收集諸如硬體和軟體清單，配置，合規性和漏洞的資料。感應器子系統是可以掃描設備和網路，並發送資料到資料庫/儲存庫子系統。

- **資料庫/儲存庫子系統--** 負責用於儲存由感應器子系統收集的結果。資料庫/儲存庫子系統還負責儲存和管理如何為目標配置技術安全策略和實施指導準則[6]。目標則是針對這些基準配置進行評估，以確定是否合規與安全。

圖1 -持續性監控系統架構



資料來源: Tieu Luu. 轉載需經許可.

資料整合挑戰

與大多數資料分析/商業智能應用程序一樣，資料的整合是持續監控系統的挑戰。大多數大型企業有多種工具所構成的感應器子系統，例如，他們可能會使用網路存取控制（NAC）解決方案來檢測設備，用漏洞掃描器來檢測設備，用代碼分析和掃描儀的漏洞來檢測軟體缺陷以及配置掃描儀評估對安全策略的合規性。因此資料的整合即成為典型的主資料管理（MDM）的問題，其中一個IT資產的完整全貌（例如，硬體，作業系統，軟體應用程序，程式漏洞修補等）必須從不同系統拼湊在一起。在圖2中將描述這些類型的工具所面臨到的的資料分析挑戰。

資料收集能力，是基於在資料庫/儲存庫子系統與安全內容自動化協議（SCAP）的介面下[7]，使用來自感應器子系統的資料。利用MDM技術之應用可以解決其他資料集面臨的挑戰。例如，交叉參考是MDM常用的技術，其中主表包含了跨越不同的系統的可能識別標誌。在這種情況下，交叉引用能力定義為設備的主要識別以及含有其它用於已使用的各種感應器工具的識別標誌（例如，MAC地址，IP地址，主機名）與其他感應器使用設備的結果比對至正確的設備。事實上並沒有靈丹妙藥可解決資料質量的完整性挑戰，從新的站點整合感應器資料，並與該站點的管理員工作就需要密切監控以及大量驗證。不同的系統報告也會用來檢查完整性和質量（例如，哪些站點是負責發佈資料，發佈了什麼資料）。應對不同的感應器重覆與衝突結果的問題，定義感應器信任模型（意即對於這種類型的研究內容，從感應器B中的結果信任來自感應器A的結果）。例如，對於脆弱性評估這項工作，由代理商執行且通過身份驗證的掃描結果會比無代理商執行，僅從網路的免費工具之的掃描結果更有可信度。

圖 2 -資料整合關鍵挑戰釋例

Challenge挑戰	Examples釋例
資產確認	進行資產確認時，需有一致的識別方法，因為不同的資產會有其識別方法，例如MAC位址，IP位址，主機名，內部標識符號等。
不完整和/或不準確的資料	在建置ISCM系統的初期階段，來自感應器資料的品質與完整性並不穩定。許多部門剛開始只做檢測並不會立即針對硬體漏洞進行配置和符合性評估。另外，缺乏經驗的系統管理員也可能會執行錯誤的程序致使報告結果失真。
矛盾的結果	有些大型企業同時有不同的漏洞掃描工具，這些工具對於不同的脆弱性暴露與危害程度有時會有不同的解讀，以致在檢測報告上會有重疊或衝突的資料產生。
具有多個資料存取機制和格式	使用多種工具意味著資料存取及格式的多樣化。有些工具提供良好的資料存取應用程式編碼介面(API)；有些則僅允許以手動輸出。有些系統係以批次方式傳送資料，有些則以事件驅動模式傳送。而且資料格式的差異也很大，以日誌文件為例，即有CSV格式與XML格式。
不同的解釋標準	越來越多的工具採用NIST的SCAP，用於自動評估程序以及標準化的資料內容和格式。但大多數的系統開發人員都知道，採用相同標準並不一定能保證可以支援不同版本相互操作性標準的解釋差異。

資料來源: Tieu Luu. 轉載需經許可.

資料結構之挑戰

資料庫/儲存庫子系統需要一個可支援多種交互模型，從感應器子系統大量寫入批次和即時處理提取資料以支持分析，以及來自用戶端即時查詢的強大結構。此外，它必需能夠容納關於企業的IT資產豐富及不斷收集的資料。例如，美國國土安全部前述的發展專案初始階段之重點是硬體和軟體資產管理，組態配置，已知的漏洞和惡意軟體。要支持這些用途所需的資料包括設備，軟體應用程序，程式補丁，組態配置資料，系統漏洞和操作元件資料（例如，擁有/管理機構，位置，支援的系統）。該計劃的後續階段加入其他使用案例，如審計，事件檢測，權限管理，端點/協議/服務，進而大量拓展資料庫/儲存庫子系統所必須支援的資料集。通過這些要求所提出的加密金鑰資料結構的挑戰將在圖3中描述。

此系統剛開始是單一資料庫結構，但後來演變成一個三階段的資料結構以支持多樣化與相互衝突的要求。第一階段的目的是提供一個倉庫或收集區可快速編寫感應器的資料，重組的所有資訊，並與儲存庫中的現有記錄對帳。資料轉換的存取點很可能會產生瓶頸，所以第一階段的結構設計成類似資產報告格式（ARF）[8]和資產彙總報告（ASR）[9]所使用的資料模型。

第二階段是對資料進行存取，變換和加載

（ETL）的優化分析工作，並支援展示與報告子系統資料庫。第三階段則是建立可支援快速匯總多層次儀表板和資料探勘分析工作的線上分析程序(OLAP)。

圖 3—關鍵資料架構之挑戰

Challenge挑戰	Examples 釋例
合併多個來源的資料	在大型企業中，資料庫/儲存子系統可能來自數百個感應器的資料。在此子系統中，資訊的取得來源不僅多樣且常常並非同時取得，也有可能是無用的資訊。資料庫/儲存子系統需要所有資料整合成可適用於分析和風險評估之模型。
衝突的資料模型	資料庫/儲存庫子系統需要一種資料模型，可讓系統快速編寫從感應器接收到的資訊。在此系統中，資料庫/儲存庫子系統以符合ARF和ASR標準的感應器接收資料。ARF主要用於傳送硬體資源和業務的資料。ASR則用於傳送感應器實際發現的結果。但在ARF與ASR間存有架構設計上的衝突。
有效支援儀表板資訊和報告等多樣化的分析結果	在ARF和ASR的高效能模式不一定表示在分析資料或是在使用儀表板和報告系統時也能高效處理。此外，分析不同的部分可能需要不同的模型。例如，預先計算的OLAP多面向資料集可以聚焦於企業風險，並提供組織層級或深入到具體部門以儀表板呈現風險評估結果。

資料來源: Tieu Luu. 轉載需經許可

分析之挑戰

在持續監控解決方案所需的主要類型分析包括相關性，融合和感應器發現衝突排解;符合性評估;風險評分;歷史趨勢;和立即查詢。這些分析能力除了幫助識別企業暴露在漏洞和潛在影響的範圍，也幫助企業評估以及如何實施其政策，如SANS定義的20個主要安全控制風險評分[10]，可讓組織應用於將這些評估進行量化，並優先解決最糟的問題。不同類型的缺陷/調查結果，嚴重性，威脅和相關資產的衝擊度等風險評分算法可說是相當複雜。此外，該組織需考慮評估結果是否可修復，減輕和接受，還是風險可以轉移到其他組織。此種分析和風險評分從個別資產或設備，到網路層面，部門級，最後到企業層面都可應用。

這可使最需識別的地區可先進行比較分析，並使管理員能夠深入到特定資產進行修復。在圖4中將描述實施這些分析功能時可能遇到的挑戰。

以工程學科結合快捷的開發方法是克服分析計算複雜性，持續修正發展的分析，以及跟上作業環境的變化時所帶來的挑戰。這將可確保該組織未來將如實發布在他們感應器資料。並確保資料可以從整個企業的多個站點進行收集，最後用於組成資產報告分類標準的定義。儘管如此會部份限制各站點彈性定義自己的分類，然而可以正確可靠地聚集資料的能力將可彌補此缺點。

圖 4—重點分析挑戰之釋例

Challenge 挑戰	Examples 釋例
跨部門間不一致的資料	正如資料品質和完整性對於資料庫是一種挑戰，目前在進行分析功能時也有更大的挑戰。不同的部門有可能無法持續提供所有必要的計算分析資料，以進行跨部門分析。例如在風險評分措施的要件之一是防病毒特徵資料庫是否一直保持在最新狀態，但有些部門缺乏檢查某些平台的能力。而且很多時候是在完成佈建後才發現有這些問題。
多面向的分析結果	要導入應用和具備多面向的分析能力是極具挑戰性。經常有多個層級（例如，目錄結構，組織結構，IT系統/程序的結構，位置，指令鏈）在正反兩極間進行匯總。而在大企業中，這些挑戰還會一步步在不同部門與站點間加劇，結果將難以凝聚整個企業。
感應器發現事項之及時性	為整合不同的感應器在不同的時間對同一套設備所產出之報告，會變得具有挑戰性；由其是在大型企業中更形顯著。另外，對於某些結果（例如，軟體清單），有些感應器僅報告當前數量而沒有其他差異資料（例如，那些軟體已加入或那些軟體已刪除）。其結果就是需要在分析發現事項時，需要以更為合理的分析，以了解何者為最新資料。
因應不同之需求與變化所做的分析	產官學研各界都在不斷確定新的指標和風險評估計算，以跟上新的網路威脅出現的速度。例如，DOS 定義一個良好的基本模型 iPost[11] 和國土安全部正在擴大其 CDM 評分模型。不同的部門也有自己的一套指標和模型，如能源部（DOE）對能源產業網路安全能力成熟度模型（C2M2）[12]。結論是在系統中的分析功能必須能夠跟上這些不斷變化的速度。

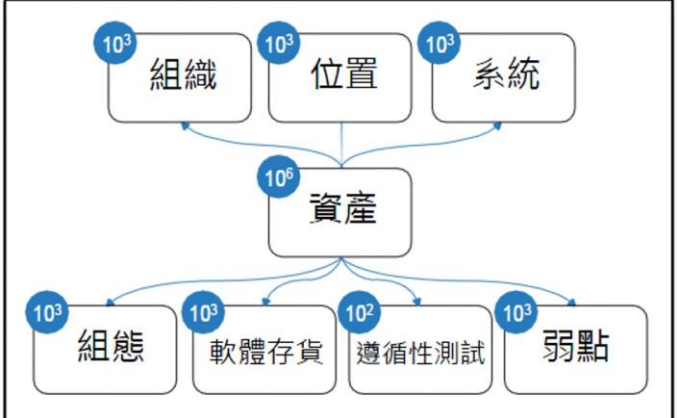
資料來源: Tieu Luu. 轉載需經許可.

性能和擴展性之挑戰

一般情況下，當大型網路公司面臨其應用系統並非在同一規模之下，一個持續監控方案所儲存和處理大量的資料，同樣有性能和擴展性的挑戰。例如，某公司有500萬和1千萬之間的資訊資產，包括成千上萬的應用軟體和補丁，成千上萬的合規性和配置設置，以及數以千計的漏洞，每天都要對這些資產是否有所衝突進行評估。圖5描繪了這些關鍵資料集以及所收集的記錄順序。

SCAP採用的標準如ARF，ASR和可擴展性組態清單描述格式（XCCDF）是相當冗長的XML格式，並且是CPU式的密集型處理。此種系統在每晚有固定的批次作業時間處理所有從感應器收集的資料。在專為支援資料儲存的分析中所進行的多種優化格式，通常只要預先處理都可以加快反應時間（例如，利用預先計算的結果驅動OLAP儀表板）以增加擴展性。

圖5 - 關鍵資料集的記錄數量



資料來源: Tieu Luu. 轉載需經許可.

結論

ISCM解決方案適用於許多從資料分析，商業智能和MDM應用網路安全等複雜領域的技術。因此，可能會遇到許多同樣圍繞著資料結構，分析性能和可擴展性應用程序之挑戰，特別是在網路安全的使用情況下，不管是案例、資料集和標準都會引發額外的複雜性。

在大型企業推行ISCM是一項複雜的工作，從考量需求的部署，營運和管理方面的問題皆是挑戰。例如，所述部署方法需要確保感應器中，提供了一個企業的IT風景全覆蓋這樣的方式展開。從執行的角度來看，ISCM的解決方案具有廣大的利益關係人員（如資訊長[CIOs]，資訊安全長[CISOs]，專案經理，系統管理員），都需要接受培訓，以正確操作和使用這些功能。管理人員如資訊長官和資訊安全長需知道如何解釋顯示在儀表板的資訊結果，而系統管理員需要知道如何正確地掃描他們的資產，並公佈調查結果。在這麼多需要執行的項目之中，治理是首要工作，先要求所有的部門依據企業安全政策開始盤點資訊資產，才能進行後續的評估與處理。

ENDNOTES

[1] Government Accountability Office, Report to Congressional Committees, “High-Risk Series: An Update,” USA, February 2013, www.gao.gov/assets/660/652133.pdf

[2] Performance.gov, “Cross-Agency Priority Goal—Cybersecurity,” www.performance.gov/content/cybersecurity#overview

[3] Office of Budget Management, “M-14-03. Enhancing the Security of Federal Information and Information Systems,” USA, www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

[4] National Institute of Standards and Technology, Special Publication 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” USA, http://csrc.nist.gov/publications/ nistpubs/800-137/SP800-137-Final.pdf

[5] Department of Homeland Security, “Continuous Asset Evaluation, Situational Awareness, and Risk Scoring(CAESARS) Reference Architecture Report,” USA, www.dhs.gov/xlibrary/assets/fns-caesars.pdf

[6] Ibid.

[7] National Institute of Standards and Technology, “The Security Content Automation Protocol (SCAP),” USA, http://scap.nist.gov/

[8] National Institute of Standards and Technology, “ARF—The Asset Reporting Format,” USA, http://scap.nist.gov/specifications/arf/

[9] National Institute of Standards and Technology, “ASR—The Asset Summary Reporting,” USA, http://scap.nist.gov/specifications/asr/

[10] SANS Institute, “Top 20 Critical Security Controls,” USA, www.sans.org/critical-security-controls

[11] Department of State, “iPost,” USA, www.state.gov/ documents/organization/156865.pdf

[12] Department of Energy, “Cybersecurity Capability Maturity Model (C2M2),” USA, http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model- c2m2-program/cybersecurity

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 1, 2015 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：
ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2015,Volume 1中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Copyright

版權聲明：

Disclaimer:
The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：
ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每

年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。