資通訊安全偵測控制-對於威脅的監視到識別與回應

Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats

作者: Fredric Greene, CISSP,

Is an experienced IT auditor specializing in technology infrastructure in the financial services industry. His main areas of focus are information and cybersecurity, IBM platforms (mainframe z/OS, AIX Power Systems), databases (DB2, Oracle), and a spectrum of systems and network technology. Another area of focus in recent years is cloud and virtualization technology including VMWare, Citrix and IBM cloud products and services. Greene worked for the legacy organization Bank of Tokyo (prior to its merger to form MUFG Union Bank), Depository Trust & Clearing Corporation (DTCC), and KPMG.

譯者: 陳政龍, 國家實驗研究院副研究員，CISA、CGEIT、PMP、CEH、ISO 27001 LA、電腦稽核協會監事

偵測控制是資通訊安全方案中，對於企業的 IT 環境提供能透徹瞭解惡意活動、破壞和攻擊的重要部分。這些控制包括了對事件與相關日誌記錄的監視和警報，以促進有效的 IT 管理。稽核人員於稽核企業資通訊安全作業時，應對這些關鍵控制措施進行確認與評估。依照 COBIT®5 框架中的資通訊安全轉型，這是一個朝著以系統化方式改變其資通訊安全的出版物，關鍵的資通訊安全目標是「攻擊和破壞能即時以適當的方式被識別與處理」。[1]

COBIT 5 提供相關的稽核目標如下：

1.確認監視和具體的技術攻擊識別解決方案。

2.評估安全事件管理和危機管理流程的介接。

3.評估攻擊應變的即時性和充分性。

另一個著名的資通訊安全偵測控制指南是美國國家標準技術研究所(NIST)的提高關鍵基礎設施資通訊安全框架(Cybersecurity Framework-資通訊安全框架)[2]。於 NIST 的資通訊安全框架中，偵測功能是主要的關鍵元件之一，當中包括有相關類別的異常和事件並進行持續性的安全監控。

資通訊安全偵測控制應該被設計成能識別特定範圍內的威脅。洛克希德・馬丁公司所提出的網際攻擊狙殺鍊可用於檢測資通訊網路威脅，其中項目包含有監測(如：掃描)、武器化與派送(如：惡意程式)、漏洞攻擊(如：弱點)、指揮與控制(入侵管理者帳戶)和資料竊取(如：智慧財產權[IP]) 。[3]

雖然防止所有入侵幾乎是不可能的事情，但對於異常活動的即早發現，在所有資通訊安全制度來說，則是不可或缺的部分。企業也應加強在資通訊安全管理程序與工具的應變能力，以面對不斷變動的網路威脅環境。

資通訊安全檢測控制

如果，特定的資通訊安全檢測控制能被設計得當且有效運作，應可阻擋前段所討論的資通訊網路威脅議題。這些控制被執行於負責資通訊網路安全監控的資安監控中心(SOC)中進行管理與運作。

安全性資訊和事件管理(SIEM)系統是集中式的軟體管理平台，能夠整合事件日誌(Event Logs)，彙整從不同威脅資料來源(如：即時回應)與資產和使用者的前後文訊息。

對於「安全性資訊和事件管理」也有其他的替代品，包含匯總分析安全數據的入侵偵測系統(IDS)和入侵防禦系統(IPS)。也有乾脆將安全監視功能服務外包給第三方供應商的選項。不過，本文所討論的「安全性資訊和事件管理」做法，是能配合企業需求且具有高度適應性和靈活性的。

「安全性資訊和事件管理」匯集正規化(標準格式)與相關事件的數據資料，並排序威脅、剔除誤報資訊，最後提供可操作的威脅情報(Threat Intelligence)。一個企業的獨特環境(資產，使用者，風險)應納入「安全性資訊和事件管理」操作。「安全性資訊和事件管理」是安全分析、事故應變、鑑識和法規遵循(報告)的必備工具。安全性資訊和事件管理的關鍵能力[4] 中列舉了一般「安全性資訊和事件管理」的許多關鍵控制，包括了即時監視、威脅情報、資料與使用者監視，應用程序監視、分析、日誌管理和報告。

實際案例中，可能包括有可疑行為的監測(如：入侵特殊權限使用者帳戶，存取敏感資訊)、發現違反政策的行為(如：於伺服器中變更配置)，進階持續性滲透攻擊（APTs）的偵測（如：對於網際網路目的地之外發流量）和舞弊偵測（如：交易量或資金移轉的變化）。稽核師應對於所描述的「安全性資訊和事件管理」功能，進行設計與運行有效性的評估。

事件日誌管理是「安全性資訊和事件管理」功能中的重要組成元件之一，事件日誌必須要被匯總（如：置入）在企業中大多數或所有已部署的技術（如：原始系統），其中包括安全設備（如：防火牆、入侵偵測系統或入侵防禦系統、網頁代理伺服器）、網路設備（如：路由器、交換機）、系統（如大型主機，中型電腦，分散式伺服器）、應用程式、資料庫、儲存裝置、終端電腦和行動裝置等。事件日誌資料還可由各項技術功能中匯總，例如績效管理與變更管理。

在來源系統中將日誌資料主動發送到集中式的「安全性資訊和事件管理」系統中，可能需要大量的投入與努力。尤其在大型企業中，事件日誌的資料量通常是龐大的，同樣也需要有大容量的儲存的需求。

一套單獨的模組、伺服器或元件(如：惠普Arcsight Log Aggregator，Security QRadar Log Manager)通常被用來進行日誌管理的使用。稽核人員需要確認「安全性資訊和事件管理」應含括了所有企業資訊環境中的相關記錄。

威脅情報來源

市調機構顧能公司(Gartner)對於威脅情報的定義是，威脅情報是一種基於證據的知識，其包含場景、機制、指標、影響和可行的建議。這些現存或新出現對於資產的威脅或危險，可用來告知企業做出對此威脅或危險的應對決策[5]。

有一種廣泛的威脅情報供應商，可以提供的網際網路協議(IP)名譽訊息的策略或營運資訊饋送(如：可疑惡意程式使用的網際網路位址或網址[URL])、惡意軟件設定檔、感染指標、幕後操縱(C&C)型態和資料外洩途徑)。

這裡對於可將當前威脅情報來源服務匯入到「安全性資訊和事件管理」系統進行簡要的概述：

- 由「安全性資訊和事件管理」供應商提供威脅情報資訊饋送以作為一站式解決服務方案的一部分，例如：IBM QRadar SIEM結合IBM X-Force的威脅情報服務。
- 許多結構化與非結構化來源的商業資料和威脅情報套件，例如：CyberSquared ThreatConnect[6]饋送(與思科Sourcefire的合作夥伴)、和AlienVault Open Threat Exchange(OTX)號稱是世界上最大集合的威脅情報知識庫。
- 免費的威脅情報饋送(例如：Google安全瀏覽API，Zeus追蹤黑名單)，透過許多資訊安全論壇提供的crystallographic information file

(CIF)檔案，當中包含有疑似惡意行為的IP位址與網址黑名單[7]。

- 由威脅反饋、規則、黑名單與分析器所產生的原創威脅情報，(例如：RSA FirstWatch[8]，在策略與戰術層面提供先進與新興的威脅情報)

這些威脅資訊，有些來自於不同程度公信力的原始、未經分析或未確認的資料，也可能是由經處理、排序、純化、精準、即時的可靠來源資訊而來。因此，就看看使用者偏好何種威脅情報了。

當安全分析師運用情境知識和對威脅情報進行分析(如：串連線索)時，則威脅情報變得更加的有用。在此情境知識是指事件中的更深層含義，包含過去、現在與未來。此外，這方面的關係著當中的戰術、技術、程序（TTPs）和操作環境（如：基礎設施）[9]。

情報是具體且豐富的背景資訊與可操作的資料，也成為設定嚴重程度和優先等級的重要參考來源。雖然本文不廣泛的討論到威脅資料、情報和供應商等部分，但從稽核的角度來說，威脅情報仍舊是資通訊安全偵測控制的重要組成部分。

嚴重性和優先等級的評定

監視安全相關活動的固有問題是，如何將潛在的大量事件與警報資料建立並傳送到「安全性資訊和事件管理」系統。根據FireEye的估算，於典型的資通訊安全網路佈署中，每秒將可產生5個警報[10]。目前僅有少數企業會投入資源進行調查。

對於資通訊安全監視工具(如：安全性資訊和事件管理)的關鍵指標，不在於警報的數量的多少，而是要發現真正的威脅，篩選出有意義的警報，並強化警報的情境資訊，以做出有利的行動[11]。

這裡所提出對於匯入的事件與警報的過濾、驗證與關聯是整體偵測能力的關鍵指標。必須要專注於最顯著威脅的資源(如：安全分析師的時間)，企業應以如下陳述來處理安全事件：

- **降低警報數量**，透過降低設備的警報頻率(如：將警報的頻率由每秒更改為每分鐘)，匯總相同來源的目的地網路IP位址；並移除無意義的指標與誤報。
- **訂定優先的警報**，基於業務風險的配置。透過資產價值、對業務功能 (如：核心流程)和活動的類型(如：指標、違反政策) 的影響。

結論

大數據提供組織許多極大化其潛在資料的機會，一個「儲存所有資料再決定其用途（可能是獲利）的時代開始了，當組織要利用這樣的發展來處理資料時，必須謹慎地確保其同時遵循在不同資料隱私與保護架構下的成文規範（法定和管制要求）和隱性規範。

在大數據時代中，資料隱私和保護規範仍必須更新，事實上，許多既有的規範連在資料倉儲環境中，都尚未被重新審視（例如：隱私法僅涵蓋竊聽行為），組織針對不斷改變的法規環境，應格外謹慎且持續保持警覺，這也代表應審視資料所在環境。探討OECD和APEC兩套架構原則是很有益處的，以兩者的核心原則為基礎，針對大數據環境來加以更新，將可在現在和未來為應用大數據的組織，帶來更多效益，同時也避免法規遵循的風險。

ENDNOTES

1 ISACA, *Transforming Cybersecurity*, USA, 2013, *www.isaca.org*
2 National Institute for Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2014, *www.nist.gov/cyberframework*
3 Lockheed Martin, Cyber Kill Chain, *www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html*
4 Nicolett, Mark; Kelly M. Kavanagh; *Critical Capabilities for Security Information and Event Management*, Gartner, 2012, *www.gartner.com/doc/2022315/critical-capabilitiessecurity-information-event*
5 Chuvakin, Anton; "Made for Each Other: How to Use Threat Intelligence With SIEM," Gartner, *http://searchsecurity.techtarget.com/tip/Made-for-eachother-How-to-use-threat-intelligence-with-SIEM*
6 CyberSquared, "ThreatConnect," Cisco Sourcefire, *www.sourcefire.com/partners/technology-partners/sourcefire-technology-partners/threatconnect*
7 Chuvakin, Anton; "On Comparing Threat Intelligence Feeds," 7 January 2014, *http://blogs.gartner.com/anton-chuvakin/2014/01/07/on-comparing-threatintelligence- feeds/*
8 EMC Corp., FirstWatch, *www.emc.com/emc-plus/rsathought- leadership/firstwatch/index.htm*
9 Hartley, Matt; "Cyber Threats: Information vs. Intelligence," 22 October 2014, *www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vsintelligence/a/d-id/1316851?page_number=2*
10 FireEye, "Speed Dating For Security Teams—Finding the Alerts That Lead to Compromise," webinar, August 2014
11 FireEye, *The SIEM Who Cried Wolf: Focusing Your Cybersecurity Efforts on the Alerts That Matter*, white paper, 2014

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 5, 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 5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。

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。