記錄與事件管理完整指南

Anton Chuvakin 博士

我們人人都有記錄，而若法規強制要求，每個人最終都必須處理自己的記錄。在本指南中，Anton Chuvakin 博士分析 SIEM 和記錄管理之間的關係，不僅著眼在技術上的差異及這些技術的不同用途，還談到同時部署這些技術的系統架構。此外，Chuvakin 博士爲已部署記錄管理或 SIEM 的公司提供建議，方便他們規劃增強部署、最佳化部署及擴充部署的藍圖。他也爲已同時部署兩種技術的公司提供建議藍圖。

白皮書

由 NetIQ 贊助

目錄

簡介

自 90 年代末期，便已存在安全資訊與事件管理 (SIEM) 技術，但在資安產業中，這項技術卻始終存有爭議，因爲它最初的訴求是「資安的單一窗口」，且小型組織也以緩慢的步調採用這項技術。近年來，傳統 SIEM 結合了用途廣泛的記錄管理技術，並著重在各種用途的記錄收集活動，其中包括回應資安事件、法規遵循、系統管理和應用程式疑難排解等等。這份白皮書將分析 SIEM 和記錄管理間的關係，不僅著眼於技術上的差異及這些技術的不同用途，更討論將這些技術共同部署時的系統架構。假設，您需要滿足支付卡產業資料安全標準 (PCI DSS) 的記錄要求，您會部署哪種工具？哪項技術較適合用來最佳化您的事件回應與調查程序？哪種工具可讓您第一時間深入瞭解攻擊性質？此外，我們也爲已部署記錄管理或 SIEM 的公司提供建議，方便他們規劃增強部署、最佳化部署及擴充部署的藍圖。而對同時部署兩種技術的公司，我們也會提供建議藍圖。

1997 年，**SIEM 工具**首次在市場上現身。它原本的用途是減少網路入侵偵測系統 (NIDS) 的誤判情形，當時，這是 NIDS 系統的一大困擾。這類工具在部署及使用上較爲複雜，因此只有資安計畫最成熟的最大型組織才會使用。90 年代晚期的市場規模約在數百萬美元左右，而有分析師指出，未來幾年的市場規模預計可達數十億美元。例如 NetIQ Sentinel 等現今的 SIEM 工具，其使用者已無分公司規模大小，範圍囊括財星 (FORTUNE) 1000 大或全球前 2000 大組織到中小企業 (SMB)。

在開始分析之前，我們應該先定義何謂 *SIEM* 與 *記錄管理*，並且說明二者間的差異。*SIEM* 涵蓋的範圍包括相關記錄收集、彙總、標準化及保留；情境資料收集；分析(包括建立關連與識別優先順序)；呈現(包括報告與視覺化)；以及資安相關的工作流程和相關的資安內容。SIEM 的所有使用案例都著重在資訊安全、網路安全、資料安全和法規遵循上。

另一方面，*記錄管理*則包括全面的記錄收集、彙總、原始 (未經處理及修改的) 記錄保留；記錄文字分析；呈現(大多是以搜尋的形式存在，但也包括報告)；相關工作流程；以及內容。記錄管理的使用案例較爲廣泛，舉凡 IT 領域，甚至在 IT 領域之外，所有可能的記錄資料運用方式都包含在其中。

由上述定義看來，兩者之間的關鍵差異在於 SIEM 著重安全性 (「安全資訊與事件管理」一詞的開宗明義就是「安全」)，以及將各種 IT 資訊運用在資安用途。另一方面，記錄管理則著重於記錄和記錄資料的諸多用途，這些用途並不侷限在資安領域之中。

界定安全資訊與事件管理的功能

讓我們進一步探討界定 SIEM 的功能有哪些；多數使用者在選擇 SIEM 產品時，都會注意這些功能是否齊全。這些功能包括：

- **記錄與情境資料收集：**收集記錄和情境資料均歸屬於此類，例如身分資訊，或是混合使用無代理程式和以代理程式爲基礎的方法所得來的弱點評估結果。
- **標準化與分類：**此類功能的用途是將收集而來的原始記錄轉換成通用格式，以便用在 SIEM 產品中。事件也會歸類到適合的類別中，例如「組態變更」、「檔案存取」或「緩衝區溢位攻擊」。
- **關連：**包括規則式關連、統計或演算法關連，以及其他方法 (例如在不同事件之間建立關連，以及將事件與情境資料建立關連的方法) 在內，均屬於此類功能。建立關連可以是即時性的，但不是所有工具都支援即時關連功能，有些工具著重於利用資料庫中的歷程資料來建立關連。有時候，記錄分析方法也會被貼上關連的標籤。
- **通知與警示：**此類功能的用途包括觸發送達操作人員或管理者的通知或警示。常見的警示機制有電子郵件、簡訊服務 (SMS)，或甚至是簡易網路管理協定 (SNMP) 訊息。
- **排列優先順序：**凡是有助於分辨重要事件與次要資安事件的各類功能，均屬於此類。只要在資安事件與弱點資料或其他資產資訊間建立關連，便可排列優先順序。優先順序演算法通常也會使用原始記錄來源提供的嚴重性資訊。
- **即時檢視：**此類功能涉及操作人員使用的安全性監控儀表板及顯示畫面。前述畫面會以近乎即時的速度，向分析師顯示收集到的資訊及關連結果。歷程與歸檔資料也可以顯示在這類檢視畫面中。
- **報告：**SIEM 產品收集到的所有資料，都會以歷程資料檢視的方式呈現在報告與排程報告中。某些產品也具有透過電子郵件或利用專用的安全入口網站將報告提供給資安人員或 IT 管理者的機制。
- **安全角色工作流程：**事件管理功能均屬此類，例如開啓個案及執行調查工作，以及自動或半自動化執行資安作業的一般工作。某些產品也提供協同作業功能，可讓多位分析師共同處理同一份資安應變工作。

目前市面上的商用 SIEM 產品，大多提供上述功能。然而，多數產品也有其優缺點及其他獨家的專有功能。

界定記錄管理的功能

在此，我們首先要來思考界定記錄管理系統的功能。其中包括：

- **記錄資料收集：**這類功能是利用以代理程式爲基礎或無代理程式的方法，或是混合使用二者，來收集所有記錄。
- **高效率保留資料：**收集和儲存記錄資料，乍看不像是困難的大工程挑戰，但要高效率地收集以十億位元組或甚至是兆位元組爲單位的記錄資料，且除了保留資料之外，還要能飛快地搜尋及存取資料，可就不簡單了。記錄資料保留的相關法令規定眾多且期限不一，規定保留數年者亦不在少見，因此本功能對記錄管理系統而言實關重大。
- **搜尋：**這是存取所有記錄中資訊的方式，包括自定應用程式中的記錄。在您將記錄用於應用程式疑難排解時，會用記錄進行調查、記錄鑑識及偵錯，而在這些工作中，搜尋都是一項不可或缺的功能。因此，明確且回應互動良好的搜尋介面，就是記錄管理系統的關鍵。
- **記錄索引或剖析：**這些功能是記錄管理系統重要元件。製作索引可以使搜尋速度增加百倍。索引技術會建立稱爲索引的資料結構，能大幅加快記錄儲存檔的關鍵字與布林搜尋工作。有些時候，其他全文分析技巧也會需要使用索引。您可以將其視爲記錄界的 Google。並非所有記錄管理工具都支援索引功能，有些還會以無關索引的記錄收集率作爲宣傳，因此請留意廠商的訴求。
- **報告與排程報告：**記錄管理產品收集到的所有資料都將透過這類功能呈現給使用者，這點與 SIEM 報告類似。不管是資安、法規遵循或營運報告，報告的優劣都決定了記錄管理解決方案的成敗。報告應具備快速、可自定且易於用在多種用途的特性。搜尋與報告之間的差異顯而易見：搜尋功能會逐一檢視所有收集而來的可用記錄，且這些記錄都保留著未經處理的原始格式 (就如同 Google 搜尋網頁一般)，報告則是利用經剖析至資料庫的記錄來運作 (如同 Excel 試算表)。請仔細評估用記錄管理工具來建立自定報告的難易度。許多解決方案在這一方面力有未逮，使得操作人員必須先鑽研奧秘難解的記錄儲存資料結構，才能製作自定報告。

接下來，我們要詳細比較 SIEM 與記錄管理的特性和功能。

詳細比較：SIEM 與 記錄管理

我們藉由下表列出兩者在功能上的關鍵領域，並說明 SIEM 與記錄管理的差異。

功能	安全資訊與 事件管理 (SIEM)	記錄管理
記錄收集	收集資安相關記錄	收集所有記錄，包括作業記錄與 自定應用程式記錄
記錄保留	保留有限的剖析與 標準化記錄資料	長期保留原始及剖析記錄資料
報告	資安導向報告 即時報告	多用途報告，歷史報告
分析	關連、威脅評分事件優先順序	全文分析、標記
警示與通知	進階資安導向報告	適用於所有記錄的簡單警示
其他功能	事件管理，其他安全性資料分析	具備高延展性的收集與搜尋

讓我們複習一下 SIEM 與記錄管理技術的用途。

近年來，傳統 SIEM 結合了用途廣泛的記錄管理技術，並著重在各種用途的記錄收集活動，其中包括回應資安事件、法規遵循、系統管理和應用程式疑難排解等等。

SIEM 與記錄管理的使用案例

在我們討論 SIEM 與記錄管理的聯合架構之前，有必要簡短介紹客戶組織部署 SIEM 產品的一般用途。我們將由三種主要類型的使用案例開始概略說明：

1. 偵測與調查性質的資安用途：這類用途有時稱爲威脅管理，其重點在於偵測及抵禦攻擊、惡意軟體感染、資料盜竊及其他資安問題。

2. 針對法規 (全球) 及規則 (地方性) 的法規遵循用途：這類用途著重於滿足各種法令、規章、體制及當地企業規則的需求。

3. 業務、系統及網路疑難排解與一般業務用途：這類使用案例大多屬於記錄管理性質，並牽涉到調查系統問題和監控系統與應用程式的可用性。

更詳細來說，資安與法規遵循使用案例可分成幾種情況。讓我們深入探究。

第一種情況是傳統的安全性作業中心 (SOC)。這種情況會大量運用 SIEM 功能，例如即時檢視與關連。SIEM 客戶組織會有分析師隨時線上待命，並在資安警示出現時加以追蹤。這就是 SIEM 技術在 90 年代興起時的 SIEM 使用案例。如今，只有最大型的組織才會使用。

接下來的使用案例，有時稱爲迷你 SOC 情境。在這類案例中，資安人員會使用非即時性的延遲檢視方式來檢查資安問題 (「分析師早上才來上班」)。分析師可能每天只在線上待命幾個小時，必要時才會檢閱警示和報告，其時效性連接近即時的程度都不到，除非事件剛好發生在他們登入產品的時段中。

第三種情況是自動化 SOC 情境：組織設定其 SIEM 根據規則來發出警示，除非出現警示，否則一概不予理會。分析師不會登入系統，除非有需要調查警示，或是到了每週或每月檢閱報告的時間，或是需要執行其他非常態性的工作。這是許多小型組織想要的使用案例，但如果不經過相當程度的客製化，很少有 SIEM 產品能提供此類功能。值得一提的是，人們在購買很多 SIEM 產品時，往往期待的是自動化的 SOC，但這樣的期待往往也都落空了。

除了資安用途以外，記錄管理技術在其他情境中也扮演著要角。應用程式疑難排解與系統管理是記錄管理系統的另外兩種重要使用案例。當應用程式部署完畢，記錄功能設定完成後，記錄管理系統便可用來快速檢閱錯誤和例外記錄。此系統亦可用來檢閱一般應用程式活動的摘要，以便判斷應用程式的健全情況，並針對可能的異常之處進行疑難排解。

本類別中的最後一種情況，是法規遵循狀態報告。在這種情況中，分析師或資安管理者在檢閱報告時，會注重法規遵循方面的問題。每週或每個月會檢閱報告一次，或是按照特定法規的規定來進行。這種使用案例不一定會有資安或業務上的考量。它往往只存在於過渡階段中，且日後，組織通常會演變成上述使用案例之一。記錄管理工具通常是部署在此種使用情境中，但將 SIEM 產品運用在法規遵循用途的情形也不在少數。長期記錄保留需求常對部署工作形成挑戰。

由於記錄是達成法規遵循目標的重點所在，我們將在此深入探討幾個法規。

PCI-DSS

支付卡產業資料安全標準 (PCI-DSS) 的適用對象是處理信用卡交易的組織。此標準規定了記錄的特定相關細節、記錄保留及日常記錄檢閱程序。

即便所有的 PCI 要求都與記錄有關，PCI DSS 仍舊包含了專門針對記錄與記錄管理的第 10 項規定。根據這項規定，所有系統元件的記錄都必須至少每天受檢閱一次。更甚者，PCI DSS 明定組織必須對記錄檔執行檔案完整性監控與變更偵測軟體，以確保記錄的完整性。另外，也規定範圍內的系統記錄必須儲存至少一年。

FISMA

2002 年聯邦資訊安全管理法 (Federal Information Security Management Act of 2002，FISMA) 強調聯邦機構必須制定、記錄及執行範圍遍及整個組織的計畫，保障支援組織業務及資產的資訊系統。NIST SP 800-53，聯邦資訊系統建議資安控管措施 (Recommended Security Controls for Federal Information Systems) 記載了記錄管理的各項控管措施，包括稽核記錄的產生、檢閱、保護及保留，以及稽核失敗時所應採取的步驟。

NIST 800-92，電腦安全性記錄管理指南 (Guide to Computer Security Log Management) 是簡化版的 FISMA 法規，其內容專爲記錄管理所制定。該指南記載聯邦機構的記錄管理需求，以及可成功見效地設立並維護記錄管理基礎架構的方法，其中包括記錄產生、分析、儲存和監控。NIST 800-92 探討了分析不同來源、不同類型記錄的重要性，並且清楚定義了特定角色，以及記錄管理所涉及的團隊與人員職責。

HIPAA (醫療保險流通與責任法案)

1996 年醫療保險流通與責任法案 (Health Insurance Portability and Accountability Act of 1996，HIPAA) 勾勒出醫療資訊的相關資安標準。NIST SP 800-66，醫療保險流通與責任法案資安規定執行資源指南 (An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule) 中詳述了用於保護電子病歷的記錄管理規定。NIST 800-66 第 4.1 節規定了資訊系統活動的定期檢閱需求，例如稽核記錄、存取報告及資安事件追蹤報告。第 4.22 節則明確規定各項動作與活動的文件必須保留至少六年。記錄有時也被視爲文件的一部分。最近的 2009 年經濟與臨床健康資訊科技法 (Health Information Technology for Economic and Clinical Health Act of 2009，HITECH) 承諾將在未來提高 HIPAA 的執行率。

如今的 SIEM 工具，例如 NetIQ® Sentinel™，其使用者不分公司規模大小，包括財星 1000 大或全球前 2000 大組織，乃至中小企業。

技術趨勢

SIEM 技術已有超過十年以上的歷史。這項技術歷經多個階段的變遷，但礙於白皮書篇幅，無法在此詳盡介紹。在此，我們將重點擺在 SIEM 技術的幾項趨勢上。SIEM 起初雖然是供大型跨國公司與機密政府機構使用的技術，但如今也逐漸打入小型組織的市場。過去，分析師曾預測，各家 SIEM 大廠會在 2011 年前開始爭奪中階市場。小型客戶的資安管理工具便能獲得改善。

另一項趨勢則是大眾普遍接受 SIEM 與記錄管理這兩種角色分工。多數 SIEM 廠商如今也提供記錄管理解決方案。如此將有助於擴展 SIEM 工具的用途，包括 IT 作業、詐騙分析、應用程式疑難排解，乃至於著眼高階治理與風險測量目標的 IT 治理、風險與法規遵循 (GRC) 等用途。

我們也目睹了 IT 作業與管理開始結合資安管理的趨勢。分析師雖然數年前便已提出預測，但這樣的趨勢迄今才真正成形。儘管如此，仍有許多專家預測資安管理結合 IT 作業與管理的趨勢將持續延燒，資安工具與 IT 營運工具 (例如網路與系統管理) 間的關係將更爲密切。

SIEM 與記錄管理情境範例

本案例研究探討的是大型連鎖零售業者爲達成 PCI-DSS 規定而部署的 SIEM 與記錄管理解決方案。由於 PCI 評估人員建議零售業者必須部署商業記錄管理解決方案以通過評估，因此該零售業者決定著手部署。某家記錄管理廠商提議零售業者同時採用記錄管理與 SIEM 解決方案。因此，該零售業者從原本的完全不運用記錄，直接進展到執行進階記錄管理系統與即時關連功能。

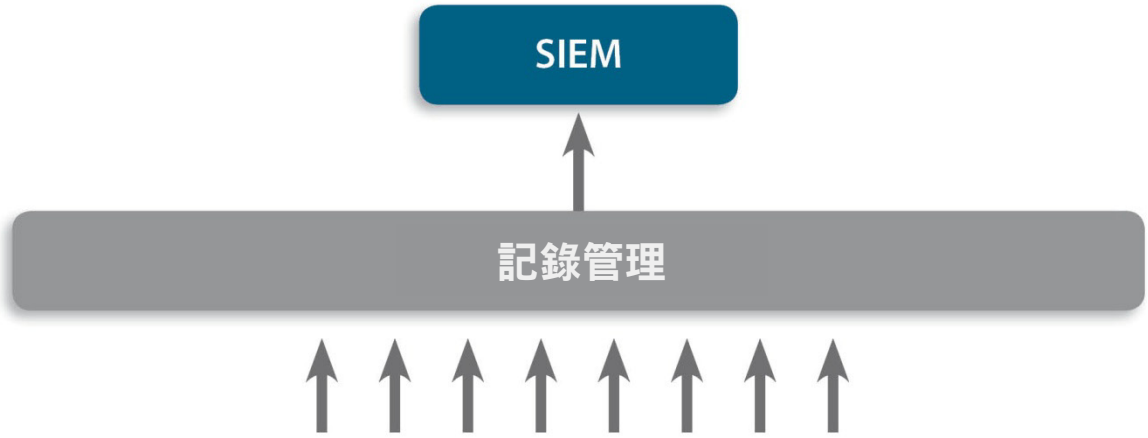
專案花費了幾個月的時間，並採取階段式策略進行。根據初步風險評估的結果，零售業者的 IT 人員決定以由外而內的方式來執行。業者首先由邊界網路 (DMZ) 防火牆開始，然後將額外的記錄輸入記錄管理系統中，並在此同時定義關連規則，執行廠商的 PCI DSS 法規遵循套件所提供的報告。零售業者學會如何回應警示後，整套程序已臻成熟，他們開始更進一步運用 SIEM 功能。

整體而言，本專案是成功落實 PCI 記錄規定的最佳代表案例。該組織高分通過了 PCI 評估，而業者對記錄與資安監控的整體策略也獲得讚賞。另外，在此案例中，業者的資安團隊還使其 PCI SIEM 成果能滿足額外的法規，因爲 PCI DSS 雖然有較爲深入的細節要處理，但基本上與 IT 治理仍屬於同一個領域。在此同時，記錄管理工具也提升了營運能力與整體的 IT 效率，SIEM 則成爲該組織未來採用即時偵測與回應功能時的核心。

記錄管理與 SIEM 架構

由於技術上的差異，許多組織都同時部署 SIEM 與記錄管理，或考慮以這兩項技術之一來強化目前部署的另一項技術。SIEM 與記錄管理常見的共同架構有哪些？

我們將把最常見的情境稱爲「SIEM 護盾」。許多部署舊式 SIEM 解決方案的組織往往將太多資料輸入到 SIEM 中，而造成超載的情形，並且有可能失去重要的資料和功能。他們解決此問題的方法，是同時採用記錄管理工具，並將其部署在 SIEM 解決方案的前端。

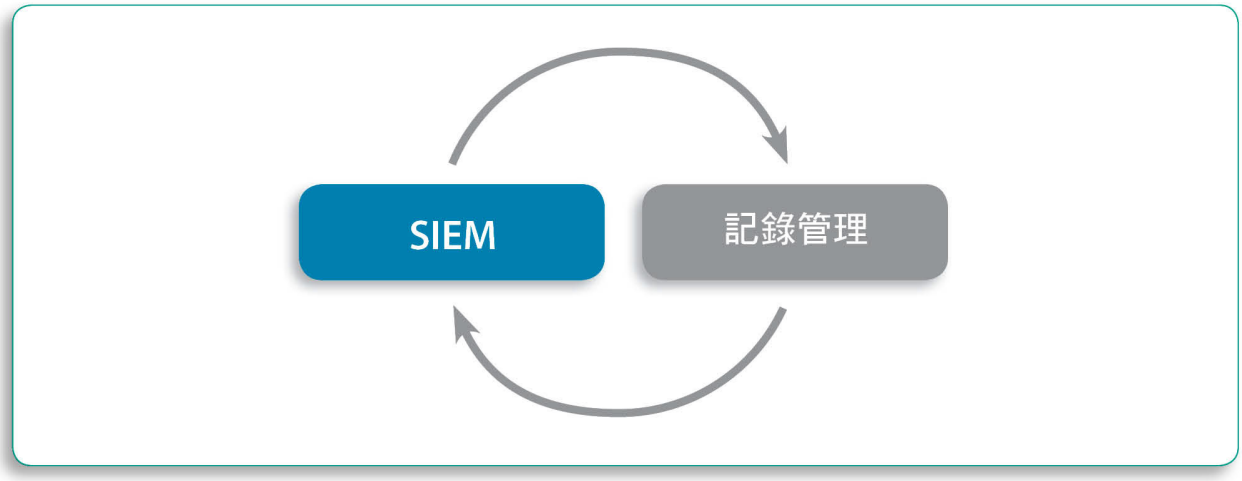


在這種案例中，是以本質上更具擴充能力的記錄管理工具來部署在 SIEM 的前端作爲護盾，並且以過濾資料的方式來避免較不具擴充能力的 SIEM 工具湧入過多記錄流量。位於記錄護盾後方的 SIEM 往往只能收到十分之一的事件量。在此同時，收到的所有事件都會由記錄管理工具加以歸檔。舉例來說，如果總記錄量等同於每秒 40,000 則記錄訊息，則 SIEM 工具每秒只會收到 4,000 則訊息。

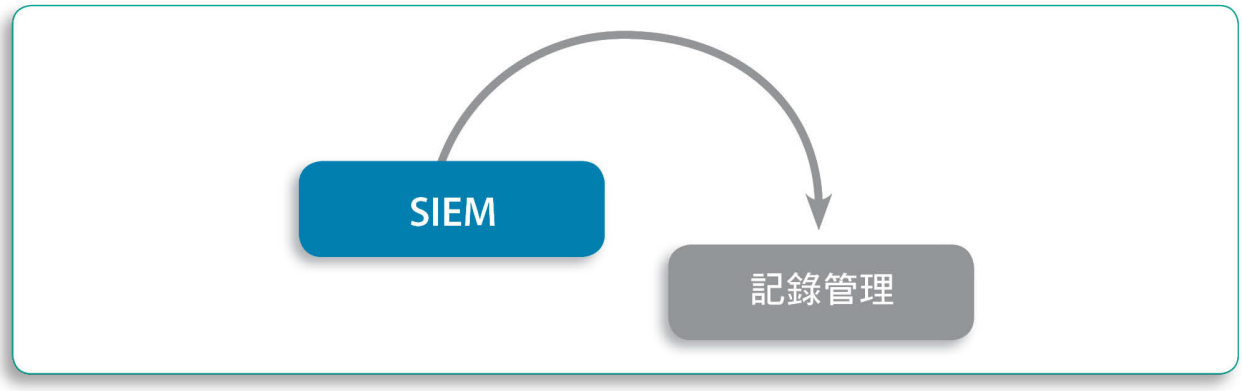
如果記錄管理是爲了建置企業記錄平台而先部署的一方，則將產生另一種情境。SIEM 隨後便會加入平台中，成爲其中的應用程式之一。第二種情境可稱爲「成長型 SIEM」，目前多達 50% 的 SIEM 部署屬於此類。在此類案例中，組織首先是由記錄管理工具開始用起，然後逐漸發現對關連、視覺化、監控、工作流程等功能的需求，並發展出相關能力。這類情境對大多數的組織而言是最合乎邏輯的，我們將在本白皮書中深入探討這點。

您必須先改善回應成效，然後才能考慮改善回應速度。 做好回應的準備，遠比監控要來得簡單。

在下一個案例中，SIEM 與記錄管理的部署是同時並行的。我們將此稱爲「新興情境」，因爲如今越來越多人是同時取得兩者，而且通常是來自同一家廠商。如果組織因故瞭解到自身對關連功能的需求，自然就會需要收集和儲存所有記錄，並擁有執行高效率搜尋與原始資料分析的能力。



在下一個情境中，請看 SIEM 部署如何利用記錄管理功能作爲歸檔工具，以供經處理的記錄和其他記錄使用。如果有人採購了龐大的 SIEM 解決方案作爲資安監控用途，但過了一段時間之後又發現功能有所不足，便會產生此情境。爲解決上述狀況，一般會部署記錄管理工具來接收所有記錄，並且執行 SIEM 無法勝任的原始記錄分析工作，例如 SIEM 不知道如何剖析、標準化或分類的記錄。這會導致使用案例從資安監控擴展成事件回應與 PCI DSS 法規遵循。



除前述情境以外，還有許多只採用記錄管理 (數量仍在成長) 的案例，以及一部分只採用 SIEM (數量可能正在萎縮中) 的部署情境。

SIEM 與記錄管理的先後順序爲何？

所幸，關於哪項技術需要優先部署的問題，答案其實很簡單。只要您有記錄，就需要管理記錄。不管是只有一部伺服器的組織，或是有 100,000 部伺服器的組織，答案都一樣。很明顯地，這些組織部署來管理記錄的技術都不盡相同，但只要有記錄存在，就代表他們需要進行記錄管理。舉例來說，如果您只需要檢閱某一台機器上的記錄，內建的作業系統工具通常就夠了。但如果您每日的記錄量達到驚人的 100 GB (這並非不可能的)，那就需要高階且昂貴的工具。

Gartner 最近有一篇名爲〈如何實作 SIEM 技術〉(Gartner，2009) 的評論文章便明確指出：「在您嘗試大範圍實作即時事件管理功能之前，請先部署記錄管理功能。」這篇文章更明言，即使部署 SIEM 技術是出於法規遵循需求，也該堅持同樣的部署順序：「SIEM 部署主要是出於 PCI 方面的需求，而部署的第一階段就是爲 PCI 評估對象範圍內的系統導入記錄管理功能。」我們在此探討的整體主題，是您必須先改善回應成效，然後才能改善回應速度。

> 只要您有記錄，就需要管理記錄。無論是只有一部伺服器的組織，或是有 100,000 部伺服器的組織，答案都一樣。

那麼，已部署舊式 SIEM 工具的組織，又該如何是好？對這些組織而言，儘快著眼於記錄管理工具，會是比較明智的作法。若能完整運用記錄，將可大幅改善這些組織的調查能力，並協助他們達成法規遵循需求。

是否所有公司都必須從記錄管理升級到 SIEM？

當組織部署了記錄管理工具，並開始將其有效運用在資安、法規遵循與營運用途之後，接下來該如何？組織部署 SIEM 工具來升級到接近即時的事件管理功能，是自然且合乎邏輯的順序。

本白皮書首開先例，以系統化的方式說明這類部署的升級條件。升級過快的組織將會浪費時間與精力，而且完全無法提高資安作業效率。然而，等待過長的時間，也代表組織將無法發展出必要的自保能力。

升級條件簡述如下：

- **回應能力：**組織必須準備好，在警示發生的第一時間立即做出回應。
- **監控能力：**組織必須擁有資安監控能力，或是透過建立安全性作業中心作爲建置資安監控能力的開始，或至少要有專責團隊持續進行定期監控。
- **微調與自定能力：**組織必須負責在 SIEM 工具部署完成後，進行微調與自定。現成可用的 SIEM 部署，成功的機率不大，也難以發揮完整的潛力。

接下來讓我們詳細探討上述條件。

首先，組織必須準備好在警示發生的第一時間，立即做出回應。雖然我們常聽到各家廠商打出「當今的企業業務瞬息萬變，資安也應該趕上腳步」等訴求，但目前幾乎沒有一家組織能做到這點。在部署 SIEM 之前，請先自問貴組織的資安即時性能做到怎樣的程度。您可能會認爲，資安時效多半確實能達到或非常接近即時的程度。網路入侵偵測系統會在攻擊發生的幾毫秒內就接收到信號，防火牆能隨時封鎖連線，而防毒技術則可在病毒一出現的時候就抓到病毒。

因此，很少人會願意購買每隔兩次攻擊才會通知一次的網路入侵偵測系統 (NIDS)。然而，這些人卻願意讓資安分析師只在每天早晨檢查 IDS 警示。如果他們發現了重大危害，NIDS 系統一毫秒的回應時間根本沒有什麼差別，倒是人員長達數小時的回應時間會造成很大的影響。有鑑於此，事後的警示調查若是能發現重大系統危害事件，倒也仍在可接受的範圍內。

如果遭病毒感染的檔案抵達時，能由軟體即時清除病毒，問題自然迎刃而解。但如果防毒軟體偵測到惡意程式碼，卻又無法自動清除或隔離，只能發出警示時 (某些後門程式與木馬的案例會發生此情形)，回應的責任就又落到了分析師的頭上，這可能是幾小時後的事了。面對今日的複雜威脅，這段時間往往足以發生重大的資料外洩事件，事後得花上好幾個月才能收拾殘局。進階的警示與狀態關連規則能提供一秒內的回應時間，但您必須先做好回應的準備。

如果組織沒有 SOC 或任何監控能力，無論是安全性監控或作業監控，在嚴格的服務等級合約 (SLA) 約束下，許多 SIEM 功能都無法徹底發揮。從純粹被動性質的使用記錄，到成熟的資安監控，常見的第一步是採用延時定期監控的方式，也就是每天早晨檢閱記錄報告。這點用記錄管理工具或 SIEM 工具都能達成。

最後一項升級條件，與微調和自定能力有關。組織必須負責在 SIEM 工具部署完成後進行微調與自定，才能將強大的自定功能應用在組織面臨的問題上。第二個選項是雇用顧問公司來進行微調。每家公司都是讀一無二的，爲發揮最高效力，SIEM 解決方案必須能照顧到既有的各種獨特企業程序。這可能代表了您必須建立警示、撰寫關連規則或自定報告，才能洞悉組織的資安或法規遵循狀態。現成的部署，加上過分期待 SIEM 解決方案能擔任迷你分析師的心態，因此成功的機率不大。

組織若不打算立即從法規遵循導向記錄管理移轉至下一階段，仍應選擇可讓組織於稍後升級至 SIEM 的記錄工具。即使一開始未打算升級至法規遵循以外的用途，許多 SIEM 與記錄管理部署仍可歸類到我們稱爲法規遵循附加價值的模式之中，這代表，工具是針對特定法規架構而採購的，但同時也可用在許多其他方面的資安與 IT 挑戰。

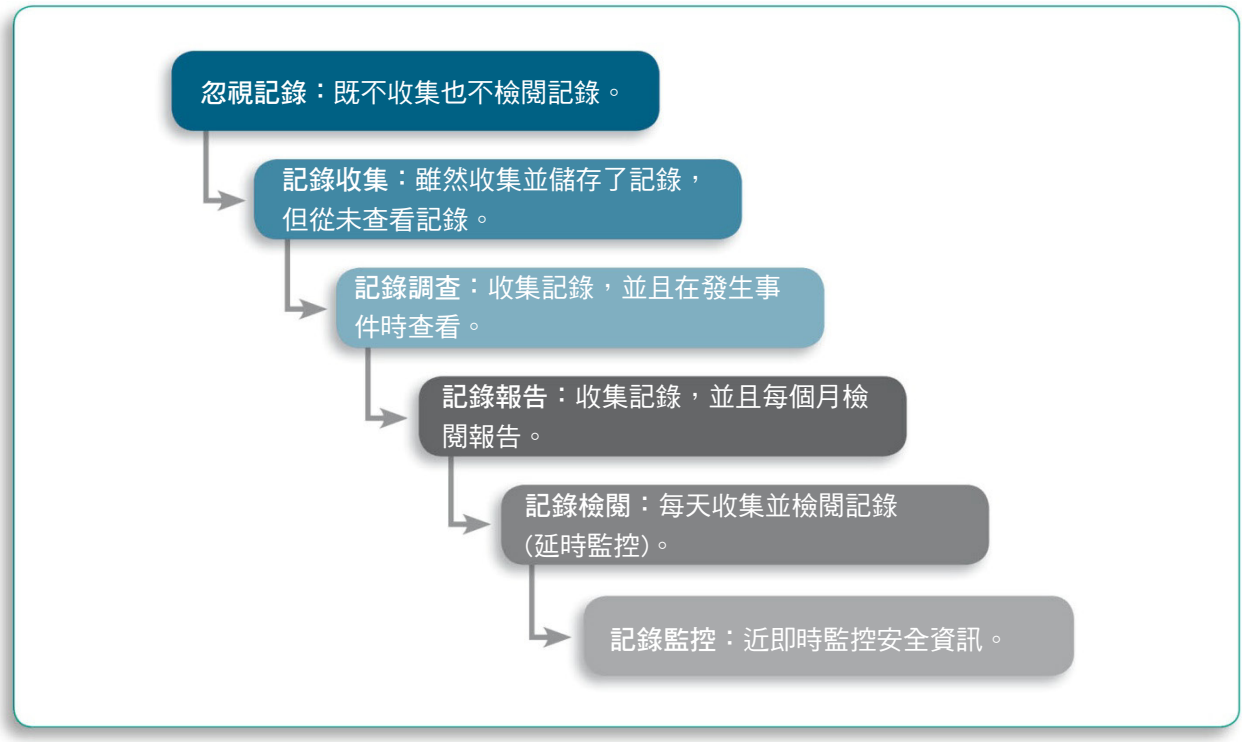
請注意，某些記錄管理工具無法提供升級至 SIEM 的管道。特別是那些只能讓您收集原始記錄並執行搜尋的簡單工具，這類工具或許相當實用，但無法讓您輕鬆達到完全標準化、分類及針對資安用途而加強記錄資料的其他目標。一般說來，如果您的工具可以收集並保留原始記錄，但無法搭配用這類資料來進行資安監控與分析的 SIEM 解決方案，便無法升級至監控功能。當貴組織做好即時監控的準備時，您會需要購買其他工具。

若能有效使用 SIEM 解決方案，便可透過進階資安導向分析 (貴組織必須已做好 SIEM 的準備)，擁有直接減少威脅的優勢，因此法規遵循附加價值模式是一種合理的模式。整體而言，它讓組織更接近神話般的資安管理單一窗口境界。

在記錄管理與 SIEM 之後：成熟曲線

爲協助達成法規遵循，並且爲組織提供資安優勢，記錄管理與 SIEM 如今已部署完畢並投入營運，接下來呢？成熟曲線從完全忽視記錄通往記錄收集與保留，再通往偶爾進行調查，然後是定期檢閱記錄，接下來一路前進到近即時資安監控的目標。

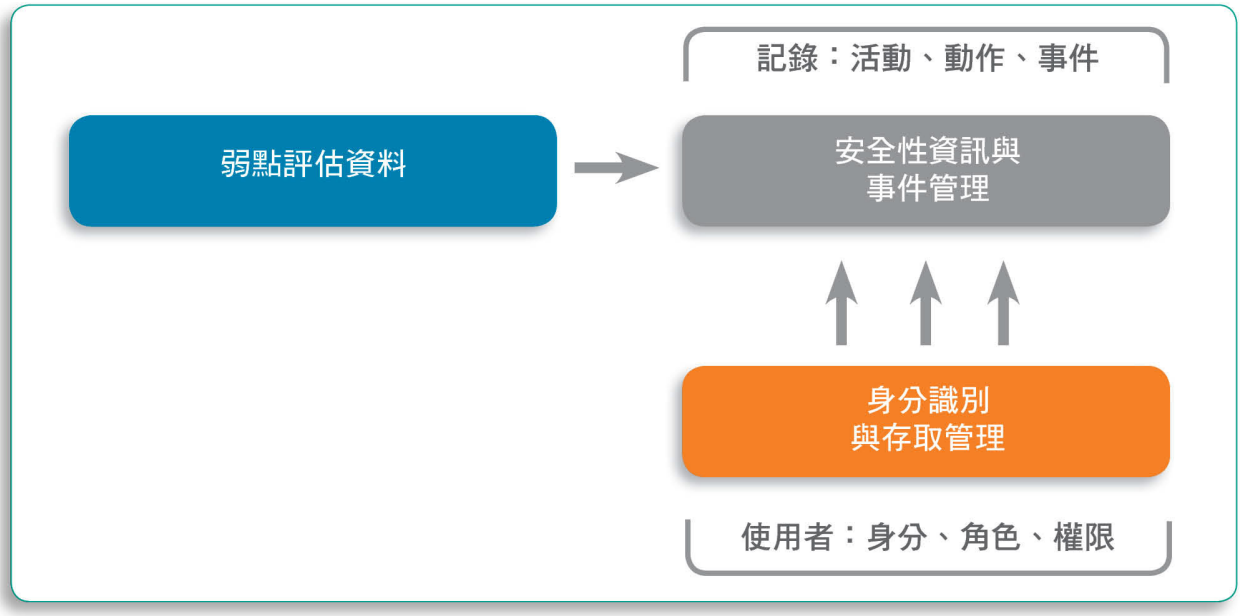
這條曲線的走勢是由無知到慢速反應，再到快速反應，最終達到主動出擊的心態，並且能夠瞭解 IT 環境的整體情況。想從無知的階段一步登天進入主動階段，這可謂天方夜譚！



到達該點後，接下來的進化之路該怎麼走呢？新手組織應該將 SIEM 整合到更多系統之中，持續改善 SIEM 部署的廣度及深度，如此方可善加利用 SIEM 的分析功能。這就接近了 SIEM 資安監控的核心任務，並且也能解決詐騙、內部威脅、應用程式監控與整體使用者活動監控等新問題。SIEM 會開始取得更多資訊，並且從網路升級到應用程式，從有限數量的資料來源升級到企業整體的部署。在此同時，資安組織也會隨之成長，並發展出更理想的運作程序，讓組織更加靈活。在擴大部署時，請務必記得，唯有按部就班，才是成功之道。

有哪些系統可以強化 SIEM 的任務執行能力，並且讓 SIEM 能夠解決其他問題？最有趣的例子之一，牽涉到使用來自 NetIQ Identity Manager 這類的身分識別管理系統的資訊。此系統提供的資訊包括真實姓名、工作角色、業務單位歸屬、各種系統與應用程式的存取權限等使用者身分識別資訊。知道使用者身分及其權限，是對內部活動進行資安監控的關鍵所在。例如，您便可以替每位使用者建立統一的身分，然後使用該身分來監控使用者在多個系統上的動作，或甚至是不同的使用者名稱與帳戶。

除此以外，與身分識別管理程式整合，SIEM 產品也可以區分哪些是經授權的正式登入，哪些又是走後門且未授權的登入嘗試。這類整合也讓 SIEM 得以掌握哪些角色不允許執行特定動作，進而實現自動化責任區分 (SoD) 監控功能。



此外，資產管理系統將包含組織內所有 IT 資源的類似詳細資訊。如同對使用者一般，我們可以擷取資產業務角色、業務關鍵性、法規遵循相關性、系統管理者名稱與位置，以及資產功能與負責人等其他資訊。這類資訊可大幅改善 SIEM 的風險計算與事件優先順序排列功能。請注意，雖然很多廠商宣稱已整合身分識別功能，但大多只是執行了簡單的輕量目錄存取協定 (LDAP) 查詢而已。這類系統無法完整利用身分識別系統可以提供的豐富資料，因此也無法協助 SIEM 判斷活動是否具惡意或法規相關性。

若能將 SIEM 產品與設定管理資料庫 (CMDB) 整合，就能提高整合程度—並且加強偵測能力。這類整合讓 SIEM 產品能在偵測到的系統與應用程式變更與經許可和授權的變更之間，建立關連。

錯誤

在規劃與實作記錄收集與分析基礎架構時，無論是 SIEM 或記錄管理，組織往往會發現本身未能徹底實現這系統的潛能。事實上，他們有時還會發現喪失了效率。由於以下的常見實作錯誤，因此常會有前述情形發生。

我們將從最明顯，但不幸的是也最常見的完全未進行記錄錯誤開始說起。即使在沙賓法案 (Sarbanes-Oxley，SOX) 與 PCI DSS 當道的這個年代。這類錯誤將摧毀記錄管理或 SIEM 所能提供的一切優勢。

相同錯誤的另一種版本，則是既無記錄，也不知道自己忘了記錄，直到一切已無法挽回。

爲何無法挽回？沒有記錄，您就可能損失收入—PCI-DSS 記錄規定指出，違反者將可導致 Visa 或 MasterCard 取消信用卡處理權，您可能面臨倒閉的命運—商譽—假設有人從您的資料庫中偷走了幾張信用卡卡號，結果媒體因爲您無法提出反證，便報導所有 4 千萬張信用卡通通被盜—您甚至還可能失去自由—媒體所報導那些駭人聽聞的 SOX 案例，就是前車之鑑。

> 一旦 SIEM 與記錄管理均開始運作，貴組織的成熟度就能獲得提昇，網路和應用程式便能全面透明化，能監控使用者活動，並與不同的系統進行其他種類的整合。

即便是做好充分準備的組織，也會犯下這種錯誤。我們來看看這個近期的例子。您的 Web 伺服器是否啓用了記錄功能？的確，在 Apache 和 Microsoft IIS 這兩種熱門的 Web 伺服器中，記錄功能都是預設選項。您的伺服器作業系統是否有記錄訊息？當然，沒有人會取消 */var/log/messages*。但您的*資料庫*呢？Oracle 的預設選項是不執行任何資料存取稽核記錄。換成 Microsoft SQL 就可以了嗎？很抱歉，答案是不行。您需要深入系統，才能開始進行一般程度的稽核線索產生。

因此，爲了避免此錯誤，您通常會需要更動預設值，並確保軟體與硬體都啓用了某種程度的記錄功能。以 Oracle 爲例，您可能必須要確定將「audit trail」變數設定爲「db」。至於其他系統，還可能更複雜。

未檢閱記錄是第二項錯誤。確保記錄存在，並加以收集和儲存固然重要，但這些畢竟只是手段。知道您環境中發生了哪些事，並且能夠進行回應，或甚至有可能預測未來將發生的事，這才是目標。前文曾提到，這只是一個階段，而非終點。如果貴公司剛剛才從忽略記錄的階段前進到收集記錄的階段，那麼請務必明白，您終究還是得檢閱記錄檔。如果您只收集記錄而不檢閱記話，您就只是在記錄自己的疏忽而已，特別是當貴單位的 IT 安全性政策還規定要檢閱記錄的時候。

因此，一旦技術到位，記錄收集成功，您就必須要有後續監控的流程來付諸行動，並且視需要將事件向上呈報。此外，檢閱或監控記錄的人員應該有足夠的資訊來判斷記錄的真正含意，以及是否需要採取任何行動。

請注意，某些組織雖然往正確的方向邁進，但卻只是半吊子而已：他們只在發生重大事件時才會檢閱記錄，例如駭客入侵、資訊洩漏或原因不明的伺服器當機，平時則逃避持續監控與記錄檢閱的工作，而他們的藉口，往往是老話一句：人手不足。他們雖然擁有記錄分析的反應優勢，這的確很重要，但卻未能實踐主動優勢：知道壞事何時會發生或更加惡化。舉例來說，如果您檢閱記錄，您可能會發現防火牆啓動了容錯移轉功能，而雖然連線正常，但這項事件依然值得關注。如果您不這樣做，而網路連線中斷了，您就只好依賴忠實的記錄來調查爲何兩道容錯移轉裝置都正巧故障了。

在此也有必要強調，出於特定法規的壓力，某些類型的組織*必須*查看記錄檔和稽核證據。如前文所述，HIPAA 法規敦促醫療組織必須制定稽核記錄與分析計畫。PCI-DSS 資安標準也有特別針對記錄收集與記錄監控及定期檢閱的條款，強調組織不能只進行記錄收集而不採取配套行動。

第三項常見錯誤是記錄儲存時間太短。SIEM 系統的作業記錄儲存庫可能會保留標準化事件 30 天的時間，但要長期保留，就需要記錄管理系統。這會讓資安或 IT 作業團隊認爲他們已有可供監控、調查或疑難排解的所有必要記錄。當他們缺乏遠見的保留政策導致所有記錄消失之後，往往才會後悔莫及。犯罪或濫用事件發生後，往往在一段時間後，有時甚至經過數個月之久，才會有人察覺，內部攻擊尤其如此。您也許在儲存硬體的方面省了小錢，但法規罰款卻會讓您付出十倍的代價。

如果降低成本很重要，那麼解決之道有時便在於將保留分爲兩部分：成本較高的短期線上儲存，以及便宜的長期離線儲存。良好的記錄管理工具可以讓您同時透明化搜尋這兩者的儲存庫，而不必移動資料。更理想的三階式策略也很常見，這可以解決上述方法的某些侷限。在此案例中，是以近線儲存來輔助短期線上儲存，記錄仍可供存取和搜尋。最舊和重要性最低的記錄則可卸載至第三階，例如磁帶或 DVD 等較便宜的儲存方式。然而，您將無法選擇性地存取需要的記錄。更明確來說，財經機構必須將記錄在線上儲存 90 天的時間，然後儲存在記錄管理系統的近線可搜尋式儲存區兩年的時間，接著再儲存在磁帶上最多七年的時間，而在某些案例中，儲存時間會需要更久。

第四種錯誤與記錄優先順序有關。人們雖然需要優先順序的概念，才能有條不紊地整理記錄分析的工作，但現今常見的錯誤，是將「記錄」視爲比「收集」更優先。事實上，就連某些最佳實務文件也建議只收集「最重要的資料」。但何謂重要？上述指引文件的缺點，就在於未以任何有用的形式來指明這點。此問題雖然有法可解，但卻可能導致資安狀態出現大漏洞，或甚至危及您的法規遵循工作。

例如，許多人會指稱網路入侵偵測與預防記錄在本質上就比虛擬私人網路 (VPN) 的集中記錄來得重要。如果外部威脅是主要威脅來源，而所有員工與合作夥伴又都是可信任的，那麼上述主張的確不爲過。VPN 記錄以及伺服器與工作站記錄，是您最可能需要用來對資訊洩漏事件或甚至惡意軟體感染進行內部調查的目標。因此，宣稱某種記錄重要性優於其他記錄類型的類似主張，都是有爭議的，而最終的結論必定令人痛苦不已，那就是，您勢必得收集所有或絕大部分的記錄。但您做得到嗎？在您回答這個問題前，請先想想，您是否可以不查看就判斷出哪項記錄比較重要，那麼，這個問題就不會再如此棘手。事實上，要達到這個目標，大有符合成本效益的解決方案在。

要避免此錯誤，您必須依照我們稍早提到的方法進行：在部署 SIEM 之前，先部署記錄管理。這樣就能保證所有需要的記錄均可用於分析，即便 SIEM 關連引擎只能看到其中的一小部分。

最後的錯誤是忽略來自應用程式的記錄，只專注在邊界與內部網路裝置，或者可能包括伺服器，但卻未能查看更高階的應用程式記錄。

企業應用程式的領域從 SAP 與 PeopleSoft 一路延伸到小型的自行開發應用程式，後者同樣爲許多企業處理關鍵任務程序。大型主機與中階系統上執行的老舊應用程式同樣也佔有一席之地，且往往用於執行核心業務程序。記錄的可用性與品質隨應用程式不同而有極大差異，有的應用程式完全付之闕如 (許多自行開發的應用程式皆是如此)，有的則是極爲細瑣繁雜 (這是許多大型主機應用程式的狀況)。缺乏共同的記錄標準，甚至軟體開發人員也沒有記錄指引，這些情況爲應用程式記錄帶來許多挑戰。所幸，未來的 MITRE 通用事件表達格式 (CEE) 可以解決此問題。

不管挑戰爲何，您都需要確實收集應用程式記錄，並使其可供分析使用及長期保留。您可以設定記錄管理軟體來收集這些記錄，並同時針對事件檢閱和定期的主動記錄檢閱來建立記錄檢閱規則。您該尋找能輕鬆設定其系統的廠商，以便收集自定應用程式中的記錄，因爲這類記錄往往是最重要的。您可以在稍後設定 SIEM，針對資安及網路用途來分析這類記錄，同時也一併分析其他記錄。

結論

請記得，我們人人都有記錄，也因此，人人最終都需要管理記錄，這是本文的主要結論之一。以最廣義的形式來說，記錄管理就是記錄的處理工作。 如果您有記錄，就得處理它們，就算只是爲了符合許多近來的法規規定也好。

另請切記，從傳統的事件回應乃至於極複雜的狀況，在諸多情境中，記錄都會派上用場。記錄的使用時間點，大多比事件發生並記載到記錄中的時間點要晚上許多。做好回應的準備，遠比監控要來得簡單。

貴組織可能需要加強複習記錄功能，然後才能準備好升級到 SIEM。在升級前，一定要具備回應警示及自定和微調產品的能力。

一旦 SIEM 與記錄管理開始運作之後，貴組織的成熟度就能獲得提昇，網路和應用程式便能全面透明化，能監控使用者活動，並與不同的系統進行其他種類的整合。

關於作者

Anton Chuvakin 博士 (http://www.chuvakin.org) 是記錄管理與 PCI-DSS 法規遵循領域的公認資安專家。他是《Security Warrior》(資安戰士) 與《PCI Compliance》(PCI 法規遵循) 二書的作者，並且亦曾參與《Know Your Enemy II》(知己知彼 II) 和《Information Security Management Handbook》(資安管理手冊) 和其他書籍的著作。Anton 出版了數十篇記錄管理、關連、資料分析、PCI-DSS、資安管理等主題的文章 (完整清單請參閱 www.info-secure.org). 他的部落格 http://www.securitywarrior.org 是業界最高人氣的部落格之一。此外，Anton 也在全球多場資安研討會上教授課程及發表簡報。近期他曾在美國、英國、新加坡、西班牙、俄國及其他國家舉辦演講。Anton 專精於新興資安標準，並擔任數家資安公司的顧問團成員。

目前，Anton 正在撰寫資安顧問實務，www.securitywarriorconsulting.com，內容圍繞資安廠商與財星 500 大組織的記錄和 PCI-DSS 法規遵循。Wolfgang Seiler Anton Chuvakin 曾擔任 PCI Compliance Solutions at Qualys 的總裁。早先，Anton 曾任職 Log Logic 的 Chief Logging Evangelist (首席記錄使徒)，工作內容是對外推廣記錄對資安、法規遵循和業務營運的重要性。進入 Log Logic 前，Anton 曾擔任一家資安廠商的策略產品管理一職。Anton 於 Stony Brook University (紐約石溪大學) 獲得博士學位。

關於 NetIQ

NetIQ 是一家企業軟體公司，客戶的成功是我們永續致力的焦點。客戶與合作夥伴選擇 NetIQ，無非是因爲本公司能協助他們以合乎成本效益的方式，克服資訊保護方面的挑戰及 IT 營運的複雜性。本公司針對安全性與法規遵循、身分識別與存取，以及效能與可用性等領域，推出一系列可擴充的自動化管理解決方案；我們以實用、重點式的方針因應各種 IT 挑戰，除了幫助客戶實現更遠大的策略價值、達成可見的企業改良成效外，相較於其他替代方法，還能幫助客戶省下更多的成本。

如需更多資訊，請造訪 www.netiq.com。

562-TW1003-001