電腦安全事件處理指南

(美國國家標準技術研究院 800-61 特別出版品修訂 2 版)

電腦系統技術報告

美國國家標準與技術研究院 (NIST) 的資訊技術實驗室 (ITL) 透過為國家測量和標準基礎設施提供技術領導來促進美國經濟和公共福祉。 ITL 負責開發測試標準、測試方法、提供參考資料、實施概念驗證和技術分析，以促進資訊技術的開發和生產性使用。 ITL 的職責包括制定管理、行政、技術和具備成本效益的實體標準及指南，以確保聯邦資訊系統的安全和隱私。特別出版物 800 系列提供了 ITL 在資訊系統安全方面的研究、指南和推廣工作，及其與產業、政府和學術組織的合作活動。

摘要

網路安全相關的攻擊不僅變得更加頻繁和多樣化，而且更具破壞性，新型態的安全事件頻傳，因此安全事件應變已成為資訊科技的重要工作。雖然藉由風險評估的預防活動可以減少資訊安全事件發生的次數，但並非都能成功預防所有事件，透過事件應變能力快速偵測異常事件、降低破壞造成的損失、減少被利用的弱點以及恢復企業服務就至關重要了。本出版物為此提供了事件處理指南，並特別針對分析事件相關數據並採取適當應變程序深入介紹。本指南不限定於特定硬體平台、作業系統、通訊協定或應用程式。

有效地執行事件應變是一項複雜的任務，必須預先建立一套可依循的計畫，當事件真正發生時才能依照計畫有條不紊地執行應變。成功的事件應變計畫關鍵要素包括：建立明確的程序以確認事件處理優先順序、實作有效的證據收集、規範分析和通報事件的標準方法、與內部單位(人力資源部門、法務部門)和外部團體(其他事件應變團隊、執法單位)建立關係及適當的溝通方式。

本出版物目的在於協助組織建立電腦安全事件應變能力並有效率地處理異常事件，修訂第 2 版更新了大部分出版物的內容以反映攻擊和事件的變化。組織若能了解威脅並在早期階段就識別攻擊手法是防止後續更大危害的關鍵，跨組織主動共享攻擊跡象的資訊是幫助及早識別攻擊的有效的方法。

組織必須創建、提供和運行正式的事件應變能力，聯邦機構須遵守美國聯邦法律規定向國土安全部(DHS)內的美國電腦緊急準備小組(US-CERT)辦公室通報資訊安全事件。

聯邦資訊安全管理法案(FISMA)要求聯邦機構必須建立事件應變能力，所有聯邦民事機構必須指定 US-CERT 的主要和次要聯絡點(Point of Contact，POC)，並根據該機構的事件應變政策通報所有安全事件，每一個聯邦機構都必須確實負責符合這些要求。

組織建立事件應變能力應包括以下行動：

- 制定事件應變政策和計劃。
- 制定執行事件處理和通報的程序。
- 制定與外部各單位溝通的準則。
- 選擇團隊組織架構和人員配置。
- 為事件應變團隊與內部組織(人事、法務部門)和外部組織(媒體、執法機構)建立關係和溝通管道。
- 確定事件應變團隊應該提供的服務。
- 為事件應變團隊成員進行教育訓練。

組織應透過有效保護網路、系統和應用程式來減少事件發生的頻率。

預防問題花費的成本通常比解決問題的成本更低也更有成效，事件預防是事件應變能力的重要互補。若安全控制不足，可能會發生大量無法控制的異常事件並壓垮事件應變的資源和能力，導致延遲災害復原或無法完整復原，造成更廣泛的損壞和更長的服務中斷及資料不可用時間。如果組織投入足夠的資源主動維護網路安全、進行系統和應用程式弱點修補來補足其事件應變能力，就可以有充足資源更有效地執行事件處理。安全控制也包括培訓員工遵守組織的安全標準，讓使用者了解有關正確使用網路、系統和應用程式的政策和程序。

組織應建立與其他組織就事件互動的準則。

在事件處理過程中，組織需要與外部各方(其他事件應變團隊、執法部門、媒體、供應商和受害者組織)進行溝通，由於這些溝通往往需要快速進行，因此組織應預先確定溝通準則，以便與正確的對象分享適當的資訊。

組織應做好應變事件的準備，專注於處理常見攻擊手法的事件。

事件發生的方式有無數種，為每一種事件類型制定專屬處理的逐步說明是不可行的。本出版品根據常見的攻擊向量定義幾種類型的事件，請注意，這些類型並非為事件提供明確的分類，其目的是用於定義更具體的處理程序，以針對不同類型的事件規劃不同的因應策略。

常見的攻擊向量(Attack Vector)包含：

- **可移動的外部裝置：**透過可移動儲存裝置(隨身碟、CD)或行動設備發動的攻擊。
- **損耗：**使用暴力方法損壞功能、降低效率、破壞系統、網路服務或企業服務的攻擊。
- **網址：**從網站或 Web 應用程式發動的攻擊。
- **電子郵件：**透過電子郵件或附件發動的攻擊。
- **不當使用：**有權限的使用者因違反組織規定而引發的資訊安全事件(但不包括上述類別)。
- **設備遺失或失竊：**使用者的設備(筆記型電腦或智慧型手機)遺失或被盜。
- **其他：**不屬於任何上述類別的攻擊。

組織應重視事件偵測和分析的重要性。

組織的每天的活動可能會產生數百萬個事件軌跡，這些跡象主要透過系統日誌或電腦安全軟體進行記錄，組織應建立日誌記錄的標準和程序，以確保日誌和安全軟體收集足夠的信息，定期利用自動化程式執行數據分析並選擇感興趣的事件進行人工審查。事件關聯軟體對於自動化分析過程具有很大的價值，然而，該軟體的有效性取決於數據收集的品質與完整性。

組織應制定書面指南來確定事件的優先順序。

決定個別事件處理的優先順序是事件應變過程中的關鍵決策點，有效的資訊共享可以幫助組織識別較嚴重並需要立即關注的事件。事件處理的優先順序可以從不同面向進行評估，例如，事件當前和未來可能對業務流程造成的負面影響程度、事件對機密性、完整性和可用性的衝擊以及從事件中恢復所必須花費的時間和資源成本。

組織應利用吸取經驗教訓的過程從事件中獲取額外價值。

重大事件處理後，應召開經驗教訓會議，一方面審查事件處理流程的有效性，也確認現行安全控制是否足夠和執行面的改善措施。如果時間和資源允許，也可以針對較小的事件定期召開經驗教訓會議，將經驗教訓會議中累積的資訊應用於識別和糾正政策和程序中的系統性弱點及缺陷。為已解決的事件產生後續報告不僅對於保全證據很重要，也可提供未來處理事件和培訓團隊成員的參考。

1 簡介

1.1 權限

美國國家標準與技術研究院 (NIST) 制定本文件是為了履行 2002 年聯邦資訊安全管理法案 (FISMA) 公法 107-347 規定的法定職責。

NIST 負責制定標準和指南，為所有機構營運和資產提供資訊安全的最低要求標準，但此類標準和指南不適用於國家安全系統。本指南符合管理和預算辦公室 (OMB) 通告 A-130 第 8b(3) 節「保護機構資訊系統」的要求，如 A-130 附錄 IV：關鍵章節分析，相關的補充資料在 A-130 附錄 III 提供。

本指南已準備好供聯邦機構使用，非政府組織可以不受版權保護使用此文件，但使用時需要註明文件版權之歸屬。

本文件的任何內容不應被視為與商務部長根據法定權力對聯邦機構制定的強制和具有約束力的標準指南相矛盾，文件內容也不應被解釋為改變或取代商務部主管、OMB 或任何其他聯邦官員現有的權力。

1.2 目的和範圍

本出版物之目的在於透過提供有效和有效率地應變事件的實用指南，以幫助組織減輕電腦安全事件的風險。它包括建立有效的事件應變計劃指引，文件的主要重點是檢測、分析、確定優先順序和處理事件，組織可參考文件建議的指南自行客製化解決方案，以滿足特定的安全和任務要求。

1.3 適用對象

本文件是為電腦安全事件應變團隊 (CSIRT)、系統和網路管理員、資訊安全人員、技術支援人員、首席資訊安全長 (CISO)、資訊長 (CIO)、電腦安全專案經理和其他負責準備或應變資訊安全事件人員所建立的。

1.4 文件結構

本文件包含以下章節：

- 第 2 節討論事件應變的必要性，概述事件應變團隊組織架構，並介紹參與事件處理的其他小組。
- 第 3 節回顧基本的事件處理步驟，提供有效執行事件處理的建議，特別是事件偵測和分析部分。
- 第 4 節探討事件應變協調和資訊共享的必要性。

2 企業的安全事件應變能力

設計有效的電腦安全事件應變能力 (Computer Security Incident Response Capability，CSIRC) 涉及多項重大決策和行動。首先要考慮的因素是為「事件」一詞創建特定於組織的定義以便清楚了解該術語的範圍。其次組織需決定事件應變團隊提供的服務有哪些，選擇團隊的結構和運作模式以提供這些服務，並決定建立一個或多個事件應變團隊。

建立事件應變的計畫、策略和程序是能夠以有效率且一致地執行事件應變之團隊的重要組成部分，計劃、政策和程序應反映團隊與組織內各團隊與外部各單位的互動方式。本節提供建立事件應變能力組織的指南，也提供有關維護和增強現有能力的建議。

2.1 事件和安全事件

事件是系統或網路中任何可觀察到的變化，例如：用戶端連接到共享目錄、伺服器接收到網頁請求、用戶發送電子郵件至公司外、邊境防火牆阻止了來源端連接的請求，這些都是資訊系統的事件。不良事件是具有負面後果的事件，例如：系統毀損、氾濫封包攻擊、未經授權存取敏感性資料、惡意軟體加密硬碟等。本文件針對電腦安全相關的不良事件探討應變方法，但自然災害引起的不良事件，則不在討論之列。

電腦安全事件是指違規行為迫在眉睫的威脅違反了電腦安全政策、系統使用規範或安全標準。資訊安全事故的案例如下：

- 攻擊者命令殭屍網路向 Web 伺服器發送大量連線請求，導致伺服器當機。
- 用戶被誘騙打開夾帶惡意軟體的附件，導致用戶的電腦感染了病毒並與其他主機建立連接繼續擴散。
- 攻擊者獲取敏感數據並威脅組織如果不支付贖金，則詳細資訊將被公開。
- 使用者透過點對點文件向其他人提供公司敏感資料。

「迫在眉睫的違規威脅」是指組織有事實依據相信特定事件即將發生。例如，防毒軟體維護人員收到來自軟體供應商通報新的惡意軟體正在網路上迅速傳播。

2.2 安全事件應變的需求

發生安全事件時會損害個人和商業資料，擁有事件應變能力的好處是能夠遵循一致的事件處理方法，系統性地採取適當的行動處理事件，最大限度地減少事件造成的損失。另一個好處是能夠使用事件處理過程中獲得的資訊充分地準備面對未來的事件，為系統和資料提供更強有力的保護。事件應變能力也有助於處理事件期間相關的法律問題。

除了這些與商業活動有關的考量之外，美國政府規定聯邦部門和相關機構必須遵守與防禦資訊安全威脅有關的法律、法規和政策，包含：

- OMB 通告第 A-130 號附錄 III。該法案於 2000 年發布，規定聯邦機構確保「有能力在系統發生安全事件時向用戶提供協助，並分享有關常見漏洞和威脅的資訊」。這種能力保證機構間共享資訊，機構互相協助遵循司法部的指導採取適當的法律行動。
- 自 2002 年起 FISMA 法案要求各機構制定“檢測、通報和應變安全事件程序”，並建立一個集中的聯邦資訊安全事件中心，其目的為：
  1. 為資訊系統維運單位提供及時的技術援助。
  2. 彙整和分析有關威脅資訊安全事件的資訊。
  3. 向所有資訊系統維運單位通報當前和潛在的資訊安全威脅和漏洞。
- 聯邦資訊處理標準 (FIPS) 200。2006 年 3 月發布此標準，為美國聯邦資訊系統和事件應變的最低安全要求。其具體的要求定義在 NIST SP 800-53:聯邦資訊系統和組織的安全控制措施。

■ OMB 備忘錄 M-07-16。2007 年 5 月公布，提供防範和應對個人識別資訊洩露的指南。

2.3 事件應變的政策、計畫和程序建立

本節討論與事件應變相關的政策、計劃和程序的要素，其中最重要的部分是應變團隊如何與外部各方進行互動。

2.3.1 政策要素

事件應變政策要素對於不同組織是依據自身需求高度客製化的，然而仍有著許多相同的關鍵要素：

- 政策獲得管理階層的承諾與支持。
- 明定應變策略的目標。
- 明定政策適用的範圍、適用的情況、適用的對象。
- 明定電腦安全事件相關術語。
- 明定應變團隊的組織架構以及角色職掌和權限層級。
- 明定事件處理優先順序或其嚴重性的評核方法。
- 明定衡量績效應變績效的指標。
- 明定事件通報和聯繫的標準範本。

2.3.2 計畫要素

滿足組織獨特要求的安全事件應變計劃應以正式的、重點式的和一致的協調方法建立應變能力路線圖，這些獨特的要求與組織的使命、規模、結構和功能有關，因此事件應變計畫應包括以下要素：

- 組織的使命 (Mission)，也就是組織存在的目的，想要解決的問題。
- 組織的目標 (Vision) ，也就是知道自己是誰、想要達到的目標與方向。
- 計畫需獲得高階管理層的核准。
- 資訊安全事件應變的方法。
- 事件應變團隊如何與組織內部團隊及組織外部其他團隊溝通。
- 衡量事件應變能力及其成效的指標。
- 達成事件應變能力成熟度的路線圖。
- 該計劃如何融入整個組織。

一旦制定了計劃並獲得管理層批准，組織就應該著手實施計劃並每年至少進行一次審查，確保組織依循事件應變路線圖邁進，讓實務上執行事件應變的能力更加成熟。

2.3.3 過程要素

基於事件應變政策和計劃定訂標準作業程序 (SOP) 讓事件應變團隊有一致的流程、技術、檢查表和通報格式的標準操作文件。SOP 應當全面且盡量詳細，讓遵循標準化的應變團隊避免因誤解而發生錯誤，特別是那些當處理重大事件時因時間急迫壓力所引起的人為錯誤。SOP 文件必須仔細測試驗證其準確性和實用性後分發給團隊所有成員，使用 SOP 文件用作訓練指導工具，並定期透過上課複習或演練資安事件培訓應變團隊。

2.3.4 與外部各方分享訊息

組織有時需要在適當的時機主動與外部各方溝通資訊安全事件處理狀況(例如，聯繫執法部門、接受媒體詢問、尋求外部專業知識)。組織也可以主動與同行分享相關資訊安全事件訊息，以改善產業的資訊安全防禦。事件應變團隊在分享資訊安全事件前應與組織的公關室、法務部門和管理階層討論，以制定有關資訊共享的政策和程序，否則敏感資訊可能會意外地提供給未經授權的各方，導致意料之外的財務和商譽損失。

圖 2-1 提供了與多種類型外部各方進行溝通的指南，雙頭箭頭表示任何一方都可以發起溝通。

圖 2-1 與外部各方的溝通

2.3.4.1 媒體單位

事件處理團隊應建立符合組織與媒體互動和資訊揭露政策的溝通程序。為了與媒體討論事件，組織通常會指定單一聯絡人 (Point of Contact、POC)和至少一個備用聯絡人。建議可採取以下行動來幫助這些指定的聯絡人和其他與媒體溝通的負責人員做好準備：

- 舉辦有關與媒體就事件進行互動的培訓課程，內容包括不洩露敏感訊息(例如，組織如何應付攻擊者的技術細節)之重要性。
- 在與媒體討論之前，制定媒體聯絡人如何簡要介紹事件和問題敏感度的程序。
- 保留對事件當前狀態的聲明，以便與媒體的溝通保持一致和提供最新資訊。
- 提醒所有員工處理媒體詢問的一般程序。
- 在事件處理演練期間舉行模擬採訪和新聞發布會，以下是媒體經常會提問的問題：
  1. 誰攻擊你了？為什麼會被攻擊？
  2. 什麼時候發生的？它是怎麼發生的？發生這種情況是因為您的安全措施不佳嗎？
  3. 這事件影響有多廣泛？您正在採取哪些步驟來確定發生的情況並防止將來再次發生？
  4. 此次事件有何影響？是否暴露了任何個人識別資訊 (PII)？此事件的損害是多少？

2.3.4.2 執法單位

許多安全相關事件沒有被定罪的原因之一是組織沒有正確聯繫執法單位。在美國境內有多個層級的執法機構可以調查資訊安全事件，例如，聯邦調查局、美國特勤局、地區檢察官辦公室、州執法機構和地方執法機構，當發動跨國攻擊事件時，其他國家的執法機構也可能參與其中。事件應變團隊應熟悉每一個執

法單位，訂定發生安全事件時應該在什麼條件下向他們通報、如何進行通報、應該收集那些證據以及收集的標準作業程序。

許多組織會指定一名特定的事件應變團隊成員作為與執法部門的主要 POC，透過符合法律要求和組織程序的方式聯繫執法部門，此人應熟悉所有相關執法機構的通報程序，並做好聯繫哪一個執法機構的準備(請注意，組織通常不應該聯繫多個執法機構，因為這樣做可能會導致管轄權衝突)。事件應變團隊必需了解潛在的管轄問題是什麼，舉例來說，位於美國的雲端服務商在日本當地機房代管台灣某公司的郵件伺服器，受到來自中國大陸駭客的攻擊，此時該向哪一個國家的執法單位報案?

2.3.4.3 事件通報組織

FISMA 要求美國聯邦機構向美國電腦緊急準備小組 (US-CERT) 通報資訊安全事件，US-CERT 是政府管轄範圍內的事件應變組織，負責協助聯邦民事機構進行事件處理工作。US-CERT 並不會取代現有的應變團隊，相反地它能夠透過充當處理事件的協調中心來加強聯邦民事機構的努力。US-CERT 分析組織報案時提供的資料，協助確認攻擊趨勢和指標，並檢查來自多個組織的數據，相較於查看單一組織的數據更容易判別事件的嚴重度。

美國政府規定，所有聯邦機構都必須向 US-CERT 指定一個主要和次要 POC，並根據該機構的事件應變政策通報所有事件。向 US-CERT 通報事件的要求、類別和時間表位於 US-CERT 網站上，所有聯邦機構必須指派特定人員通報事件、確保其事件應變程序符合 US-CERT 的通報要求，並正確遵循這些程序。

如果組織沒有自己的資訊安全事件應變團隊可以向聯邦機構聯繫，組織也可以向行業的資訊共享和分析中心(ISAC)回報，這些特定私人行業的服務之一是在其成員之間共享重要的電腦安全相關資訊，在美國針對通訊、電力部門、金融服務、資訊科技以及研究和教育等行業已有多個 ISAC 成立。

2.3.4.4 其他外部各方

組織可以與下面列出的團體討論事件應變處理，在與這些外部各方接觸時，組織可透過 US-CERT 或其 ISAC 作為「值得信賴的介紹人」來居中協調。值得信賴的介紹人可以提供其他組織過去曾發生類似的問題的經驗，加速正確識別問題點及應變處置。

- **組織網路的 ISP。**組織需要其 ISP 的幫助來阻止網路攻擊或追蹤攻擊來源。
- **發起攻擊位址的擁有者。**如果攻擊源自外部組織的 IP 位址，事件處理人員需要與該組織指定的安全聯絡人聯絡，向他們發出異常活動的警報或要求他們收集證據。強烈建議與 US-CERT 或 ISAC 協調此類溝通，避免直接接觸來源組織。
- **軟體供應商。**事件處理人員可能需要與軟體供應商討論可疑活動。如果懷疑因未知軟體漏洞而受到損害，軟體供應商可以提供有關已知威脅或新的攻擊方法資訊，以幫助組織掌握當前的威脅。
- **其他事件應變團隊。**組織可能會遇到與其他團隊曾經歷過的類似事件，主動分享資訊可以更有效率處理事件。
- **受影響的外部各單位。**內部的資訊安全事件可能會直接影響外部各單位，在某些司法管轄區，組織必須主動通知受事件影響的所有各單位。無論情況如何，組織最好在媒體或其他外部組織知道之前主動將事件通知受影響的外部單位，處理人員也應謹慎僅提供適當的信息，並要求受影響的各方不可公開披露的有關內部調查的詳細狀況及相關資訊。

美國政府的 OMB M-07-16 防範和應對個人識別資訊洩露備忘錄，針對涉及個人資料保護的安全事件要求聯邦機構制定並實施個人識別資訊(PII)違規通知政策。事件處理人員應了解當懷疑發生 PII 洩漏時，他們的事件應變處理行動應有何不同。

2.4 事件應變團隊模型

任何可能發生安全事件的組織都應該有事件應變的團隊，根據事件的嚴重程度及可用的人力資源至少

需指派一名人員負責處理該事件。事件處理團隊負責分析事件相關資料以確定事件的影響、採取適當的行動限制損害並恢復正常服務。事件應變團隊是否成功取決於整個團隊成員的參與和合作。本節主要介紹事件應變團隊模型、團隊人員配置並提供有關選擇適當模型的建議。

2.4.1 應變團隊模型

事件應變團隊有三種團隊模型：

1. **集中式事件應變團隊。**由中央單一事件應變團隊負責處理整個組織的安全事件，此模型適合於小型組織。
2. **分散式事件應變團隊。**組織擁有多個事件應變團隊，個別團隊負責的特定邏輯或物理部分的事件應變。此模型適合大型組織或計算資源分散各地的組織(例如，每一個分公司建立一個資訊安全應變團隊)。雖然團隊各自負責，但仍應該由單一協調指揮中心調度，以確保事件應變過程在整個組織中保持一致，更重要的是資訊在團隊之間透明共享，避免多個團隊看到相同的事件訊息並在相同時間同時處理相同的資訊。
3. **協調式事件應變團隊。**事件應變團隊向其他團隊提供建議，但對其他團隊沒有指揮權力，例如，部門的技術團隊向組織的安全應變團隊提出技術建議，但不主動介入事件應變。此模型可以被視為 CSIRT 的 CSIRT。本件主要探討集中式和分散式 CSIRT，不會詳細介紹協調式團隊模型。

事件應變團隊有三種人員配置模型：

1. **內部員工。**完全由內部員工執行所有事件應變工作，承包商僅提供有限的技術和管理支援。
2. **部分外包。**將部分事件應變工作外包，最普遍的做法是組織將入侵偵測、防火牆和其他安全設備的監控 7x24 外包給安全服務提供者(MSSP)。MSSP 責識別並分析可疑活動，將偵測到的異常事件回報給組織的事件應變團隊。組織事件應變團隊僅執行基本的事件應變工作，承包商處理較嚴重或廣泛影響的事件。
3. **完全外包。**完全外包給承包商執行事件應變工作，當組織需要全職的現場事件應變團隊但沒有足夠的合格員工時，可以選擇使用此模型。完全外包的情況下組織仍需指派員工監督外包商工作。

2.4.2 選擇團隊模型考慮的因素

在為事件應變團隊選擇適當的結構和人員配置模型時，組織應考慮以下因素：

- **7x24 全天可用。**即時可用性對事件應變是重要的條件，事件持續的時間越長，造成損失的就越大。因此大多數組織要求事件應變人員 7x24 待命 On Call 或人員在現場值班。
- **全職或兼職團隊成員。**資金、人員、配備和事件應變能力有限的組織可能只有兼職的團隊成員充當虛擬事件應變團隊，在這種情況下，事件應變團隊可以視為志願消防隊，當發生緊急情況時便迅速聯繫團隊成員立即組織應變團隊。兼職團隊可善用現有 IT Helpdesk 資源， Helpdesk 成員接受培訓，擔任事件通報的一線接觸點，負責執行初步調查和資料收集，當出現嚴重事件時立即向事件應變團隊發出警報。
- **員工士氣。**處理事件應變的工作壓力很大，待命中的團隊成員也是如此。這種工作內容使得組織很難找到願意、有空、經驗豐富且具備適當技能的人員參與，特別是在 24 小時支援方面。將角色分離，並減少團隊成員需負責執行的行政工作量可以顯著地提高士氣。
- **維運成本。**事件應變團隊涉及 IT 的許多技術，其成員需要比大多數 IT 員工具備更廣泛的知識，他們還必須熟練使用事件應變工具，團隊工作區域的實體安全和通訊機制也都要納入成本考量。成本是一個重要考量因素，需在投入事件應變、人員培訓和 7x24 值班費用間取得預算平衡。
- **員工專業知識。**處理資訊安全事件需要多種技術領域的專業知識和經驗，所需知識的廣度和深度會根據組織風險的承受程度而有所不同。外包商比組織的員工擁有更深入的入侵偵測、取證、漏洞和其他安全方面的知識，然而組織內的技術人員通常比外包商更了解組織的環境，當組織員工專業程度越高就越有助於判別事件並降低誤警報。

大多數組織會採購外包服務，在考慮外包時應評估以下問題：

- **確保一致的工作品質。**組織不僅應考慮外包商目前工作的廣度與深度的品質，還應評估外包商未來的工作品質能夠保持一致，例如，要求外包商減少人員流動和倦怠，為新員工提供可靠的培訓計劃等。對於如何客觀地評估外包商的工作品質，組織應該有一套評量標準。
- **明確的職責分工。**組織通常不會授予外包商針對環境做出營運決策的權力(例如，中斷 Web 伺服器的連線)。規範這些決策點的適當操作非常重要，有些外包的模式讓外包商可以向組織的內部團隊提供事件資料及進一步處理的建議，當組織內部團隊依據建議做出最終營運決策後，外包商根據決策執行工作。
- **必需限制透露的敏感資訊。**保密協議(NDA)是保護敏感資料的一種機制，要求外包商簽訂 NDA 或限制其對敏感資訊的存取可以改善這種情況，例如讓承包商可以看到事件中的使用者 ID，但不知道什麼人與該使用者 ID 關聯，若要更進一步得知此 ID 資訊，則由內部員工接管調查。
- **是否了解組織特定的知識。**準確分析事件和判斷優先順序取決於對組織環境的了解程度。組織應定期向外包商提供更新的文件、說明組織關注的事件、提供重要的資源資訊，以及在各種情況下應採取何種應變等級。組織也應透漏其 IT 基礎設施、網路配置和系統所做的所有變更，否則承包商只能對每一個事件做出猜測，不可避免地會導致事件處理不當造成雙方誤解。如果團隊之間的溝通薄弱或組織根本不收集必要的訊息，不管有沒有將事件應變外包，缺乏組織特定的知識都是一個大問題。
- **是否缺乏資料相關性。**多個資料來源之間的關聯性非常重要，如果入侵偵測系統記錄了對網路伺服器的攻擊跡象，但外包商無法存取伺服器的日誌，就無法確定攻擊是否成功。為了提高效率，通常會讓外包商透過安全通道取得關鍵系統和安全設備日誌的資料，然而這會增加安全管理成本，開放額外的存取入口點，也會增加資料洩漏的風險。
- **能夠處理多個地點的事件。**有效的事件應變工作通常需要在組織的設施中實際操作，如果有多個可能的事件應變地點，須考慮外包商所在的位置以及組織在現場建立事件應變團隊的速度和花費的費用。規劃時需實地考察是否某些設施或區域不應允許外包商工作，只能由內部團隊執行應變程序。
- **內部掌握事件應變技能。**將事件應變完全外包的組織也應努力在內部保持基本的事件應變能力，以預防無法聯繫到外包商的情況。無論如何，組織都要準備好自己執行事件應變的流程和能力。

2.4.3 事件應變人員

應由至少一名專責人員和至少一名備援替補人員負責處理事件應變。在完全外包模式中，此人可負責監督和評估外包商的工作，如同其他專案模型通常都有一名團隊經理和至少一名副手，副手在團隊經理缺席時承擔權力。專責人員除了化解危機並確保團隊擁有必要的人員、資源和技能，也要擔任與高階主管和其他團隊及組織的聯絡人。

除了團隊經理和副手之外，有些團隊還設有技術負責人，即具有較強技術能力和事件應變經驗的人員，主要負責團隊技術工作的品質並承擔監督和最終責任。技術負責人的職位不應與事件負責人的職位混淆，較大的團隊通常會指派一名事件負責人作為處理特定事件的主要 POC，對事件的處理負責。根據事件應變團隊的規模和事件的嚴重程度，事件負責人實際上可能不會執行任何實際的事件處理，而是協調處理程序的活動，從處理程序收集消息並向其他組織提供事件更新，確保團隊的運作順暢。

事件應變團隊的成員應具有系統管理、網路管理、程式設計、技術支援和入侵偵測等技術硬實力，也應該具備良好的解決問題和批判性思考的軟實力，團隊每位成員不一定都是技術專家，但在每一個主要技術領域至少有一名高度熟練的人員是必要的。

透過提供學習和成長的機會來抵消員工的倦怠非常重要，建立和維持技能的建議如下：

- 編列足夠預算來維持、增強和擴展技術領域和較不具技術性的領域知識(例如，事件應變的法律方

面知識)。指派員工參與各項會議或研討會，學習更深入技術的參考資料。在資金允許的情況下引入在相關領域具有深厚技術知識的外部專家擔任顧問。

- 為團隊成員提供執行其他任務的機會，例如擔任教育訓練講師、規劃安全意識研討會、負責特定領域知識的研究等。
- 讓事件應變團隊人員輪替交換工作內容，以獲得新的技能。
- 保持足夠的人員配備，讓團隊成員可以有足夠休息時間。
- 建立指導計劃，讓資深技術人員幫助經驗不足的員工學習事件處理技巧。
- 制定事件處理場景並讓團隊成員討論並演練如何處理這些場景。

除技術專長外，團隊合作默契也很重要，合作和協調是成功應變事件的必要條件。每一位團隊成員也應該有良好的溝通和寫作技巧能力，不是要求團隊中的每個人都具備很強的寫作和口語能力，但團隊中至少應該有一些人具備這些能力，這樣團隊才能在其他人面前展現成果。

2.4.4 組織內的依賴關係

確定組織內需要參與事件處理的其他團體以便在需要時徵求他們的合作。事件應變團隊需依賴於其他人的專業知識、判斷力和能力，包括：

- **管理。**管理階層制定事件應變政策、預算和人員配置，並負責協調各利害關係人之間的事件應變程序，最大程度地減少損失，並向國會、OMB、審計總署 (GAO) 和其他各方通報。
- **資訊保護。**在事件處理的某些階段(預防、遏制、根除和復原)需要資訊安全人員協助，例如變更防火牆規則。
- **IT 支援。**系統和網路管理員等 IT 技術專家不僅擁有提供協助所需的技能，而且他們通常對日常管理的技術有最深入的了解，能夠正確評估對受影響系統的操作是否適合。
- **法務部門。**法律專家審查事件應變計畫、政策和程序，以確保其符合法規和聯邦指南。如果事件可能引發法律訴訟，則收集證據、起訴嫌犯或提起訴訟都需要法律顧問或法務部門的指導。
- **公共事務和媒體關係。**根據事件的性質和影響，可能需要通知媒體和社會大眾。
- **人力資源。**如果懷疑員工涉入事件，相關懲處程序須由人力資源部門介入處理。
- **持續營運計劃 (BCP)。**事件應變政策和持續營運計畫的流程必須一致。當安全事件破壞了組織的業務彈性，持續營運計畫人員應了解事件及其影響，以便進行業務影響評估、風險評估和營運計劃的連續性。由於持續營運規劃人員在嚴重情況下降低營運中斷風險擁有豐富的專業知識，因此他們通常對某些安全處理的建議作法具有參考價值。
- **實體安全和設施管理。**有些電腦安全事件是透過物理攻擊破壞設備實體安全而發生的。事件應變團隊在事件處理期間也需要存取應變所需設施，例如，從上鎖的辦公室取得受病毒感染的工作站。

2.4.5 事件應變團隊服務

事件應變團隊的工作重點是執行事件應變，但僅負責執行事件應變的團隊相當罕見，通常團隊也會負責其他相關業務：

- **入侵偵測。**日常負責偵測入侵的工作。
- **提供意見。**為組織發布新漏洞和提供威脅處理的建議。組織內只需一個小組負責安全建議，避免重工和資訊衝突。
- **教育和加強員工安全意識。**透過多種方式，如研討會、網站訊息、時事電子報、海報、螢幕保護程式或筆記型電腦貼紙等方式教育和強化使用者及技術人員對偵測、通報和應變事件的了解。當使用者的安全意識越高，組織在資訊安全應變所需的資源就越少。
- **資訊共享。**參與資訊共享小組或網路社群，例如 ISAC 或區域合作夥伴，彙整事件相關的資訊並在企業內部共享相關資訊。

2.5 建議

本節提出的有關組織電腦安全事件處理能力的主要建議總結如下。

- **建立事件應變能力。**當電腦安全防禦網遭到破壞時，組織需有快速有效的應變程序。
- **建立事件應變策略。**事件應變策略是事件應變計劃的基礎，用來定義異常事件的條件、應變團隊的組織結構、團隊成員角色和職責，並規範事件通報格式。
- **根據應變政策制定事件應變計劃。**事件應變計劃提供了組織根據政策實施應變的路線圖，應變計劃應有短期和長期目標及能夠衡量計劃成效的指標。事件應變計畫也應說明事件處理人員接受訓練的頻率以及對事件處理人員的技能要求。
- **制定事件應變程序。**事件應變程序提供應變事件的詳細步驟，涵蓋事件應變過程所有階段。
- **制定有關事件相關資訊共享的政策和程序。**組織應與外部各方，如媒體、執法機構和事件通報組織溝通適當的事件詳細資訊。事件應變團隊也應與組織的公共事務辦公室、法務部門和管理層討論，以制定有關資訊共享的政策和程序。
- **向適當的組織提供有關事件的相關資訊。**聯邦民事機構必須向 US-CERT 通報事件，其他企業組織則可以聯繫 US-CERT 或其 ISAC。
- **選擇事件應變團隊模型時考慮的相關因素。**根據組織的需求和能夠運用的資源仔細權衡每種可能的團隊結構模型和人員配置模型的優缺點。
- **為事件應變團隊選擇具有適當技能的人員。**團隊的可信度和熟練度取決於其成員的技術能力和批判性思考能力。關鍵技術包括系統管理、網路管理、程式設計、技術支援和入侵偵測。有效的事件處理還需要團隊合作和溝通能力，必須為所有團隊成員提供相關的教育訓練。
- **確定組織內可能需要參與事件處理的其他小組。**事件應變團隊都需依賴於其他團隊的專業知識、判斷和管理、資訊保證、IT 支援、法律、公共事務及設施管理等能力。
- **確定團隊應提供哪些服務。**儘管團隊的主要重點是事件應變，但大多數團隊平日也需負責其他諸如入侵偵測、提供組織安全建議、對使用者進行資訊安全教育訓練等業務。

3 處理事件應變

事件應變過程分為幾個階段：初始階段建立和訓練事件應變團隊，並取得必要的工具和資源。準備階段根據風險評估結果選擇和實施控制措施以限制事件發生的數量。實施控制後，將不可避免地持續存在殘餘風險，因此必須持續偵測安全漏洞，並在事件發生時向組織發出警報。根據事件的嚴重性，組織透過遏制事件損害擴大或重建系統恢復原狀來解決事件的造成的影響。完成事件應變處理後，流程循環回到偵測和分析，檢查是否有其他主機也發生相同事件。當事件充分處理後，組織發布報告詳細說明事件的原因和損失以及組織採取的預防再犯措施。

本節描述事件應變過程的主要階段: 準備階段、偵測分析階段、遏制根除復原階段、事件後活動階段，如圖 3-1 事件應變生命週期所示。

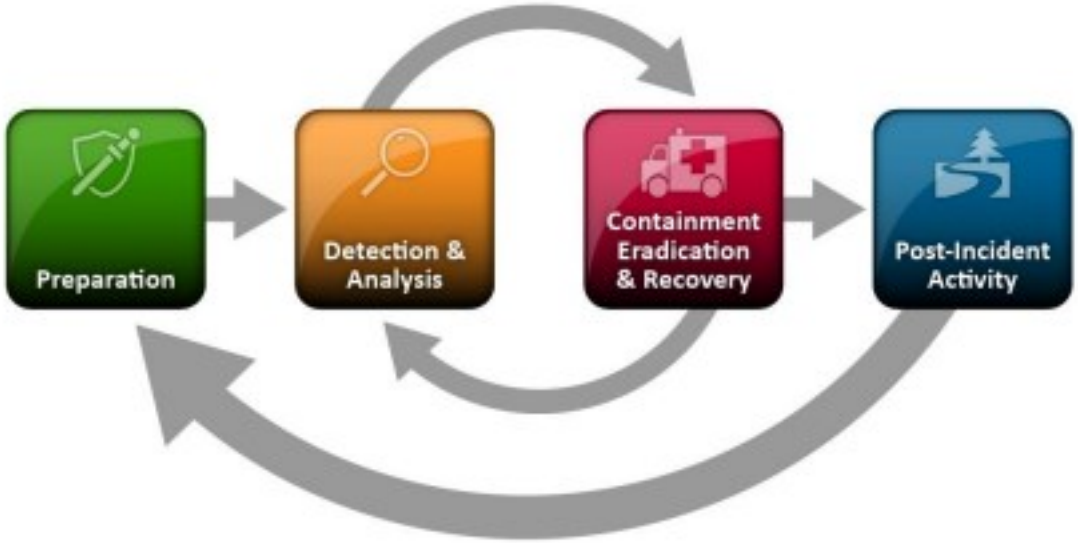

圖 3-1，事件應變生命週期

3.1 準備工作

事件應變的準備工作在於建立事件應變能力以利組織做好應變事件的準備，確保系統、網路和應用程式有足夠安全性來預防事件。儘管事件應變團隊通常不負責事件預防，但預防對於事件應變計畫的成功至關重要，本節提供有關準備處理事件和預防事件發生的建議。

3.1.1 準備處理事件

下列清單提供了事件處理過程中有用的工具及可用資源，目的在提供組織討論事件處理程序需要的工具和資源參考，組織應該準備多種機制，以防單一機制失效後無法應變。

- 事件處理者通訊和設施
  - **聯絡資訊：**團隊成員和備用聯絡人的電話號碼、電子郵件地址、公共加密金鑰以及聯絡人身分驗證的方法。
  - **On Call 待命資訊：**組織內的其他團隊待命 On Call 的資訊，以及當聯絡不到值班人員時通知其主管的方法。
  - **事件通報機制：**透過何種方式通報，例如電話號碼、電子郵件、電子表格或其他可讓使用者通報事件的安全即時訊息系統，而且至少要有一種允許匿名通報事件的機制。
  - **問題追蹤系統：**用於紀錄、追蹤事件資訊及處理狀態。

- **智慧型手機：**方便團隊成員於非工作時間與現場人員進行支援和溝通。
- **加密軟體：**用於團隊成員之間或組織內部與外部各方的溝通。美國聯邦機構規定必須使用支援 FIPS 驗證加密演算法的通訊軟體。
- **戰情中心：**用於集中溝通和協調。建立永久性的戰情中心沒有必要也不切實際，團隊應制定建立臨時戰情中心的條件和程序，以便在需要時才建立戰情中心。
- **安全儲存設施：**用於保護證據和其他敏感資料。

■ 事件分析硬體和軟體

- **數位蒐證電腦和備份設備：**建立事件裝置其磁碟的備份映像檔、保留事件日誌紀錄及其他相關檔案資料。
- **筆記型電腦：**用於分析和擷取資料封包與撰寫報告等活動。
- **備用工作站、伺服器和網路設備或虛擬化的主機設備：**用於從備份檔回復和研究惡意軟體。
- **空白的移動儲存裝置。**
- **隨身印表機：**從未連線網路系統的機器列印日誌檔案和其他證據的副本。
- **資料封包偵測和協定分析工具：**擷取並分析網路封包和流量。
- **數位搜證軟體：**用來分析磁碟映像檔的資料。
- **移動式裝置：**在移動裝置安裝乾淨且安全的應用程式，用於從系統收集相關資料。
- **證據收集工具：**包括筆記本、數位相機、錄音機、表格、證據儲存袋、標籤貼紙以及數位證據磁碟以保存可能採取法律行動的證據

■ 事件分析資源：

- **連接埠列表：**包括常用應用程式連接埠和已知惡意程式和木馬程式的連接埠。
- **說明文件：**包含作業系統、應用程式、通訊協定以及入侵偵測和防毒產品的說明。
- **網路拓樸圖和關鍵資產列表。**
- **系統安全狀況時的 Baseline：**網路、系統和應用程式正常活動的 Baseline。
- **哈希加密關鍵文件：**以加快事件分析、驗證和消除異常的速度。

■ 事件緩解軟體：

- **使用包含乾淨作業系統和應用程式的備援映像檔，用於系統復原。**

許多事件應變團隊會準備便捷工具包(Jump Kit)，其中包含上面項目列表中列出的裝備，其目的是為了更快的應變事件，平常避免將便捷工具包的工具挪作他用。

在設備使用便捷工具包對設備執行封包探測、惡意軟體分析前，應對設備進行清除並重新安裝所有軟體，確保乾淨的設備不會影響分析。由於此設備是特殊用途，它可能還需安裝標準企業工具和配置之外的軟體。除了此調查用的設備外，每一位事件處理人員還配給一台標準筆記型電腦、智慧型手機或其他設備，用於編寫報告、閱讀電子郵件以及執行與事件分析無關的其他職責。

模擬事件的演習對於讓員工做好事件處理的準備也非常有用，有關練習的更多信息，請參閱 NIST SP 800-8423 附錄 A 提供範例演練場景。

3.1.2 預防事故

將安全事件保持在合理的低水位對於保護組織的業務流程非常重要，如果安全控制不足，會不斷發生更多的事件，使事件應變團隊不堪負荷，導致應變緩慢或復原不完整，造成更大的負面業務影響。以下簡要概述實務上保護網路、系統和應用程式安全的一些建議：

■ **風險評估：**定期為系統和應用程式進行風險評估以確定威脅和漏洞會帶來哪些風險，其內容包括了解通用的威脅和特定於組織的威脅。進行風險優先排序，採取減輕、轉移或接受風險直到達到合理的整體風險等級。定期進行風險評估的另一個好處是確定關鍵重要的資源，使工作人員能夠專注於對這些

重要資源的監控和應變活動。

- **主機安全：**所有主機都應使用標準配置進行適當的組態強化。除了保持每台主機正確更新修補程式之外，主機的配置還應遵循最小授權原則，僅授予使用者執行其授權任務所需的權限。主機應啟用審核並記錄重要的安全相關事件，並持續監控主機及其配置的安全性。使用安全內容自動化協定 (Security Content Automation Protocol，SCAP) 產生作業系統和應用程式配置清單協助以一致性有效的方法保護主機。
- **網路安全：**網路邊界應設定為預設拒絕所有未授權的活動，包括虛擬私人網路 (VPN) 和與其他組織的專用等連線。
- **預防惡意軟體：**在整個組織內佈署偵測和阻止惡意軟體的軟體，佈署在主機層級(伺服器和工作站作業系統)、應用程式伺服器層級(電子郵件伺服器、Web 代理程式)和應用程式用戶端層級(電子郵件用戶端、即時通訊用戶端)。
- **培訓使用者安全意識：**讓使用者了解有關正確使用網路、系統和應用程式的政策和程序。歷史事件學到的實用經驗教訓也應該與使用者分享，以便他們能夠了解他們的行為如何影響組織。提高使用者對事件的認識應該會減少事件的發生頻率， IT 員工也必須接受培訓，以便他們能夠根據組織的安全標準維護其網路、系統和應用程式。

3.2 偵測與分析

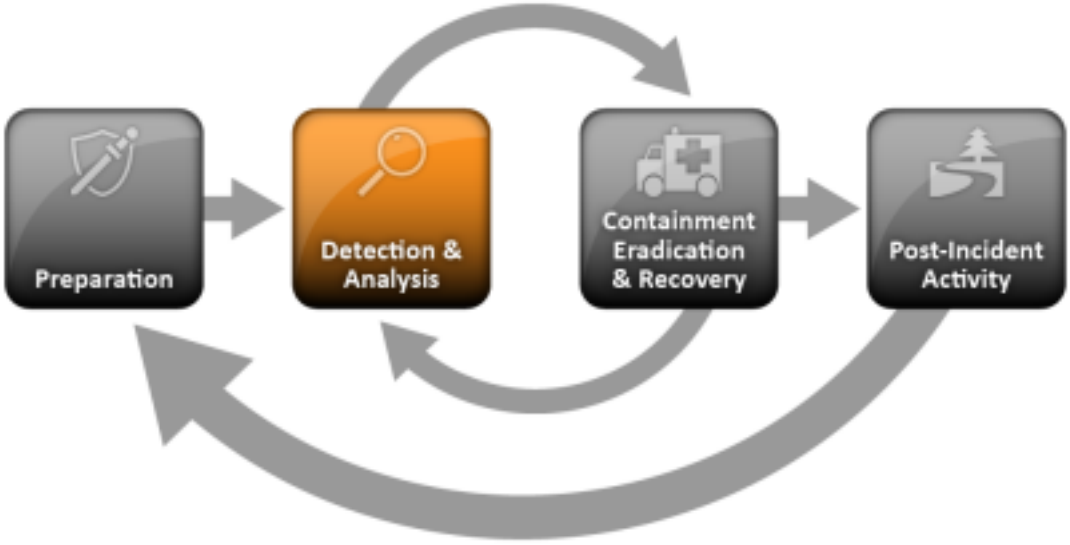

圖 3-2，事件應變生命週期(偵測和分析)

3.2.1 攻擊向量

事件可能以無數種方式發生，因此制定每一個事件的逐步處理說明是不可行的。組織應做好處理各種事件的準備，並優先專注於常見攻擊手法的事件處理。不同類型的事件需要不同的應變策略，以下列出攻擊向量目的並非提供事件的明確分類，僅是列出常見的攻擊方法，用作定義具體處理程序的基礎。

- **外部/可移動裝置：**從移動裝置或週邊設備執行的攻擊。例如，惡意程式碼從受感染的 USB 隨身碟傳播到系統。
- **損耗：**使用暴力方法來危害或破壞系統、網路或服務的攻擊。例如，目的在造成損害、拒絕服務或應用程式的存取的 DDOS、針對身份驗證機制的暴力攻擊。
- **網址：**從網站或 Web 應用程式執行的攻擊。例如，用於竊取憑證的跨網站腳本攻擊或重導向到利用瀏覽器漏洞並安裝惡意軟體的網站。

- **電子郵件：**透過電子郵件或附件執行的攻擊。例如，偽裝成電子郵件本文中的附件或夾帶惡意網站連結程式碼。
- **冒充：**涉及以惡意內容取代良性內容的攻擊。例如，欺騙、中間人攻擊、無線非法存取點和 SQL 注入攻擊。
- **不當使用：**被授權的使用者違反組織規定的使用政策而導致的安全事件，但不包括上述類別。例如，使用者安裝檔案共用軟體，導致機敏資料被讀取，或使用者在系統上刻意執行非法活動。
- **設備遺失或被竊：**組織使用的電腦、智慧型手機或識別證遺失或被盜。
- **其他：**不屬於任何其他類別的攻擊。

本節重點在介紹處理安全事件的建議做法，根據各種攻擊向量提供具體建議超出了本出版物的範圍，此類指南將在涉及其他事件處理主題的單獨出版物中提供，例如關於惡意軟體事件預防和處理的 NIST SP 800-83。

3.2.2 事件跡象

對於許多組織來說，事件應變流程中最具挑戰性的部分是準確地偵測和評估可能發生的事件以及確定是否發生了事件。如果不幸發生安全事件，如何確定問題類型、影響和嚴重程度。導致這項任務如此具有挑戰性有三個因素：

- **偵測方法太多：**事件可以透過許多不同的方式來偵測，其詳細程度和精確度各不相同。可以透過基於網路和主機的 IDPS、防毒軟體和日誌分析器進行自動偵測，也可以透過用戶通報問題或人為檢查進行手動方式偵測。有些事件有明顯的跡象很容易被發現，但有些事件卻幾乎不可能被發現。
- **資料量很大：**潛在事件跡象的數量通常很大，例如，組織每天收到數千甚至數百萬個入侵偵測感測器警報的情況是很常見的。
- **專精技術不易：**必需具有深入專業的技術知識和豐富的經驗才能正確有效地分析事件相關數據。

事件的跡象分為兩類：前兆和指標。前兆是未來可能發生事件的徵兆，指標是事件已經發生或可能正在發生的跡象。大多數攻擊沒有任何可識別或可偵測的前兆，但是如果可以偵測到前兆，組織就有機會透過改變其安全態勢來防止目標遭受攻擊或者更密切地監控涉及目標的活動。以下是幾種前兆的例子：

- Web 伺服器日誌顯示有被掃描的情況
- 新的資安情資顯示有攻擊與組織郵件伺服器相同軟體的事件發生。
- 來自某個團體的威脅，聲稱該團體將對組織發起攻擊。

前兆相對較少，指標卻很常見，下面列出了一些常見的指標：

- 網路入侵偵測感測器發出針對資料庫伺服器的緩衝區溢位攻擊的警報。
- 防毒軟體偵測到主機感染惡意軟體。
- 系統管理員看到包含異常字元的檔案名稱。
- 系統日誌紀錄了主機的組態配置被改動。
- 應用程式記錄來自不熟悉的遠端系統的多次嘗試登入失敗。
- 電子郵件管理員看到大量含有可疑內容的電子郵件。
- 網路管理員注意到與正常網路流量偏差的異常。

3.2.3 異常前兆和指標的來源

前兆和指標可以透過許多不同的來源來識別，最常見的來源是電腦安全軟體警報、日誌、公開資訊和人員，表 3-1 列出了幾種常見的前兆和指標來源。

表 3-1，前兆和指標的常見來源

來源	描述
警報	
IDPS	IDPS 產品能夠識別可疑事件並記錄偵測攻擊的日期時間、攻擊的類型、來源和目標 IP 位址以及使用者名稱。大多數 IDPS 產品使用攻擊簽章來識別惡意活動，因此簽章必須保持最新，以便能夠偵測到新的攻擊。IDPS 軟體經常會產生誤警報，分析師需仔細查看記錄的支援資料或從其他來源取得相關資料來手動驗證 IDPS 警報。
SIEM	安全資訊和事件管理 (SIEM) 產品與 IDPS 產品類似，但它們根據系統日誌資料分析和發報警報(請參閱下文)。
防毒和反垃圾郵件軟體	防毒軟體可偵測各種形式的惡意軟體、產生警報並防止惡意軟體感染主機。保持最新病毒碼，防毒軟體可以有效阻止許多惡意軟體。 反垃圾郵件軟體用於偵測垃圾郵件並防止其到達使用者的郵箱，垃圾郵件包含惡意軟體、網路釣魚攻擊和其他惡意內容。反垃圾郵件軟體發出的警報暗示有外部攻擊的跡象。
文件完整性檢查軟體	文件完整性檢查軟體可以偵測事件期間對重要文件所做的變更，它使用雜湊演算法來獲取指定檔案的加密 Checksum，若檔案被更改則新的 Checksum 和與舊的 Checksum 就會不符。透過定期計算 Checksum 並將其與先前的值做比較便可以檢測到文件的異動。
第三方監控服務	第三方提供各種基於訂閱的監控服務，例如詐欺偵測服務：如果組織的 IP 位址、網域名稱與涉及其他組織的當下異常事件活動有關聯，該服務將通知組織。第三方監控服務的另一個例子是中國證監會通知清單，這些清單可提供其他事件應變團隊偵測異常事件時使用。
紀錄	
作業系統、服務和應用程式紀錄	當事件發生時，作業系統、服務和應用程式的日誌紀錄就具有很大的價值。尤其是記錄存取了哪些帳戶以及執行了哪些操作的審計紀錄。 組織應要求所有系統制定安全 Baseline，日誌紀錄可用於關聯事件資訊與 Baline 進行差異分析，根據分析結果與事件資訊產生異常事件警報。
網路設備日誌	來自網路設備(防火牆、路由器)的日誌通常不是前兆或指標的主要來源。儘管這些設備通常預設會記錄阻止的連接嘗試，但它們提供的有關活動性質的資訊很少。儘管如此，它們在識別網路趨勢和關聯其他設備檢測到的事件方面仍然很有價值。
網路流量	網路流量是主機之間發生的特定通訊資料交換的數量。網路設備通常可以提供網路流量資料，這些資料可用於搜尋由惡意軟體、資料外洩和其他惡意行為引起的異常網路活動。網路流量的串流資料格式有許多標準，包括 NetFlow、sFlow 和 IPFIX 等。

公開資訊	
新漏洞和利用的資訊	隨時了解新的漏洞和利用漏洞攻擊的手法可以防止某些事件的發生，並且有助於偵測和分析新的攻擊。國家漏洞資料庫 (NVD) 包含有關漏洞的資訊。US-CERT 等組織和社區緊急應變小組 (CERT)®/CC 透過簡報、網路貼文和郵件清單定期提供威脅更新資訊。
人員	
組織內部人員	使用者、系統管理員、網路管理員、安全人員和組織內的其他人員可能會通報事件跡象，驗證所有此類通報非常重要。有一種方法是詢問提供此類資訊的人對資訊準確性的信心有多大，記錄此估計值以及提供的資訊可以在事件分析過程中提供很大幫助，特別是在發現資料衝突時。
組織外部人員	應嚴肅看待來自外部的事件通報，外部單位可能會聯繫組織，聲稱組織的系統正在攻擊其系統，外部使用者也可能通報網頁損壞或服務不可用，其他事件應變團隊也會互相通報事件。處理外部通報重要的是建立機制，讓外部各方有管道通報異常，並讓經過培訓的工作人員仔細監測這些機制。

3.2.4 事件分析

如果保證每一個前兆或指標都是準確的，事件偵測和分析就會很容易，可惜現實並非如此。用戶提供的資訊(例如，投訴伺服器無法連線)通常是不正確的，入侵偵測系統大部分都是誤警報。在理想情況下應評估每一項指標以確定其是否合法，然而糟糕的是每天的指標總數可能達到數千或數百萬，要從所有指標中找出真正發生的安全事件是一項艱鉅的任務。

再者即使指標準確，也不一定代表事件發生。某些指標(例如伺服器當機或關鍵檔案被修改)可能是由安全事件以外的多種原因或人為錯誤發生。然而既然已經出現了跡象，我們就有理由懷疑正在發生事件並應立即採取對應的行動。確定特定徵兆是否實際上是異常事件有時需要與其他技術和資訊安全人員合作做出判斷。無論事件是否與安全相關，都應該以相同的方式處理情況，例如每隔 12 小時就會發生網路斷線，但沒有人知道原因，為了幫助員工會盡快解決問題，組織應該使用相同的安全事件應變資源來診斷問題，不管問題的根源是什麼。

有些事件很容易偵測到，例如明顯被破壞的網頁，但是更多事件並沒有如此明顯的症狀。例如系統設定檔中的一項小變更之類的微小跡象可能是偵測到的唯一跡象。在事件處理中，偵測可能是最困難的任務，儘管存在許多偵測相關技術的解決方案，實務上更簡單的方法是建立一支經驗豐富、業務熟練的工作人員團隊，他們能夠正確地、有效率地分析前兆和指標，並採取適當的行動。如果沒有訓練有素、技術能力強的團隊，事件偵測和分析的效率就會低落，並且會犯下代價高昂的錯誤。

事件應變團隊應能夠快速分析和驗證事件，遵循預先定義的流程並記錄所採取的每個步驟。當團隊懷疑發生安全事件時，團隊立即展開進行初步分析並確定事件的範圍(例如哪些網路、系統或應用程式受到影響，事件由何人或何事引起，以及事件是如何發生的)。初始分析和驗證為團隊提供資訊來決定後續活動的優先順序，以及應變方法(採取遏制事件和持續對事件影響進行更深入的分析)。執行初始分析和驗證具有很高的挑戰性。以下是使事件分析更容易、更有效的一些建議：

- **為網路和系統紀錄特徵。**特徵是指預期狀態的紀錄，用於與平時比較以便於更容易識別其變化。例如在主機上執行檔案完整性檢查以取得關鍵檔案的 Checksum、監控網路頻寬使用情況以確定不同日期和時間的平均值和峰值水準。組織應使用多種檢測和分析技術綜合判斷以提高辨識正確度。

- **了解正常行為。**事件應變團隊成員應該掌握網路、系統和應用程序的正常行為是什麼。沒有任何一個事件處理程序能夠全面了解整個環境中的所有行為，但處理程序中應該知道哪些資料可以填補空白，取得這些資料的其中一種方法是查看日誌條目和安全警報，隨著對日誌和警報越來越熟悉，團隊應該專注於那些無法解釋的條目，這些條目通常值得去調查。例行性審查日誌除了持續更新知識也要注意隨著時間推移的趨勢和變化。
- **建立日誌保留策略。**有關事件的資訊可能會記錄在多個位置，例如防火牆、IDPS 和應用程式日誌。建立並實施指定日誌資料保留時間的策略對分析資料非常有幫助。保留日誌的另一個原因是事件可能要在幾天、幾周甚至幾個月後才被發現，通常較舊的日誌紀錄會顯示偵察活動或先前類似的攻擊徵兆。維護日誌資料的時間長度取決組織的資料保留策略和資料量，建議可參考 NIST SP 800-92 電腦安全日誌管理指南有關日誌記錄的建議。
- **分析事件關聯。**事件的證據可能會在多個日誌中捕獲，不同日誌包含不同類型的資料，防火牆日誌包含來源 IP 位址，而應用程式日誌包含使用者名稱，網路 IDPS 可以偵測到針對特定主機發動的攻擊，但它可能不知道攻擊是否成功，分析人員除了檢查主機的日誌以確定事件，通常也會將多個指標來源之間的事件關聯起來以驗證特定事件是否發生。
- **保持所有主機對時同步。**網路時間協定 (NTP) 等協定可在主機之間同步時間。如果通報事件的設備時鐘設定不一致，分析事件關聯將會更加複雜。
- **維護和使用資訊知識庫。**知識庫應包括處理人員在事件分析期間快速參考所需的資訊，雖然可以建立具有複雜結構的知識庫，但簡單的方法也有幫助。文字文件、電子表格和相對簡單的資料庫為團隊成員之間共享資料提供了有效、靈活和易搜尋的機制。知識庫應包含各種訊息，包括對前兆和指標的重要性和有效性的解釋，例如 IDPS 警報、作業系統日誌和應用程式錯誤代碼。
- **使用網路搜尋引擎進行研究。**網路搜尋引擎可以幫助分析人員找到有關異常活動的資訊。例如，分析人員可能會看到一些針對 TCP 連接埠 22912 的異常連線嘗試。對術語「TCP」、「連接埠」和「22912」執行搜尋會傳回一些包含類似活動日誌的標的，甚至是對該事件的解釋以及連接埠號的重要性。請注意，應使用單獨的工作站進行研究，盡量降低組織進行這些搜尋所引發的風險。
- **運用資料擷取來收集其他資料。**有時候記錄的訊息不夠詳細，無法讓處理程序了解正在發生的情況。如果在網路上發生事件，收集必要資料最快的方法是使用封包擷取器擷取網路流量。配置資料封包擷取器來記錄符合指定條件的流量使資料量易於管理，並減少捕獲無意義的資訊。出於隱私考慮，有些組織要求事件處理程序在使用資料封包擷取器之前必須申請並獲得許可。
- **過濾數據。**實務上根本沒有足夠的時間來審查和分析所有指標，但至少要調查那些最可疑的活動。過濾掉不重要的指標類別或僅顯示最重要的指標類別是有效的策略。然而，這種方法存在著風險，因為新的惡意活動可能被過濾掉或者不屬於所選指標類別。
- **尋求他人的幫助。**有時候團隊無法確定事件的完整原因和性質，如果團隊缺乏足夠的資訊來遏制和消除事件，則應諮詢內部資源(例如資訊安全人員)和外部資源(例如 US-CERT、其他 CSIRT、具有事件應變專業知識的承包商)。

3.2.5 事件紀錄文件

當懷疑發生事件時，應變團隊應立即開始記錄有關事件的所有事實，日誌是一種有效且簡單的媒介，使用筆記型電腦、錄音機和數位相機也可以達到此目的。記錄系統事件、對話和觀察到的文件變更可以更有效、更系統性、較不易出錯地處理問題。從偵測到事件到最終解決所採取的每一步驟都應記錄下來並加蓋時間戳。有關事件的每份文件應由事件處理人員註明日期並簽署，當提起法律訴訟時，這種性質的資訊可以用於法庭證據。處理人員應盡可能至少兩人一組團隊工作，一人負責記錄事件，而另一人則執行技術任務。

事件應變團隊應保留有關事件狀態的記錄以及其他相關資訊。使用問題追蹤系統或資料庫有助於確保及時處理與解決事件，問題追蹤系統應包含以下資訊：

- 事件的當前狀態(新事件、正在進行中、轉發調查、已解決…等)。

- 事件概要。
- 與事件相關的指標。
- 與本次事件相關的其他事件。
- 所有事件處理者對此事件採取的行動。
- 監管鏈(CoC)，按時間順序記錄的文件或紙本記錄，記錄了包括物理或電子證據在內的材料的保管、控制、傳輸、分析和處置順序。
- 與事件相關的影響評估。
- 其他相關各方(例如系統所有者、系統管理員)的聯絡資訊。
- 事件調查期間收集的證據清單。
- 事件處理者的評論。
- 接下來要採取的步驟(重建主機、升級應用程式、更新修補程式…等)。

事件應變團隊負責保護事件資料並限制人員對資料的存取權，因為它通常包含敏感資訊，只有被授權的人員才能存取事件資料庫。事件通訊(例如電子郵件)和文件都應加密或以其他方式保護，只有被授權人員才能閱讀它們。

3.2.6 事件優先級

確定事件處理的優先順序是事件處理過程中最為關鍵的決策點。由於資源限制，不應該按照先進先出的原則處理事件，而是根據相關因素評估後決定處理的優先順序，這些因素包括：

- **該事件對業務功能的影響。**IT 系統的事件通常會影響這些系統提供的業務功能，對這些系統的使用者造成某些類型的負面影響。事件處理人員應評估事件如何影響系統的現有功能，以及評估事件若不立即遏制，未來可能造成的功能影響。
- **事件對組織資訊的影響。**事件會影響組織資訊的機密性、完整性和可用性。例如，惡意代理可能會洩漏敏感資訊。事件處理人員應考慮這種資訊外洩將如何影響組織的整體使命，如果任何資料與合作夥伴有關，敏感資訊外洩也會對其他組織造成影響。
- **從事件中恢復的能力。**事件的影響範圍及其影響的資源類型將決定從該事件中恢復所必須花費的時間和資源成本。敏感資訊的機密性一旦受到損害就無法從事件中恢復，除非可確保將來不再發生類似事件，才將有限的資源花費在延長事件處理週期。組織投入處理事件的資源有限，事件處理人員需考慮從事件中實際恢復所需的工作量，並仔細權衡恢復工作創造的價值以及與事件處理相關的任何要求。

結合對組織系統的功能影響和對組織資訊的影響來確定事件的業務影響，例如，針對公共 Web 伺服器的分散式阻斷服務攻擊可能會暫時降低嘗試存取伺服器的使用者的功能，而對公共 Web 伺服器進行未經授權的特權存取可能會導致個人識別資訊(PII) 洩露，這會對組織的聲譽產生長期影響。

事件的可恢復性決定了團隊在處理事件時可能採取的應變。具有較嚴重功能影響且恢復難度較低的事件是團隊應立即採取行動的理想選擇。然而，某些事件可能沒有順暢的恢復路徑，或需要排隊等待更具策略性的應變(例如，導致攻擊者洩露並公開發布敏感資料的事件沒有簡單的復原路徑，因為資料已經暴露)，在這種情況下，團隊可以將處理資料外洩事件的部分責任轉移給更具策略性的團隊，該團隊制定防止未來違規的策略，並制定計劃以向那些資料外洩的個人或組織發出警報。

對事件進行評級有助於確定投入有限資源的優先順序，組織可以依據其安全狀態的感知能力量化事件的影響。表 3-2 提供了組織可用於對其自身事件進行評級的功能影響類別的範例。

表 3-2，功能影響類別

類別	定義
無 (None)	不會影響組織向使用者提供服務的能力。
低 (Low)	組織仍然可以向使用者提供服務，但效率已下降。
中 (Medium)	組織失去了向使用者提供服務的能力。
高 (High)	組織不再能夠向任何使用者提供服務。

表 3-3 提供了可能的資訊影響類別的範例，描述了事件期間發生的資訊外洩的程度。在此表中，除「None」之外，其他類別並不互相排斥，組織可以同時選擇多個資訊影響類別。

表 3-3，資訊影響類別

類別	定義
無 (None)	沒有資訊被洩露、竄改、刪除。
違反隱私 (Privacy Breach)	機敏的個人識別資訊 (PII) 被違法存取或洩露。
違反所有權(Proprietary Breach)	受保護的關鍵基礎設施資訊 (PCII) 被存取或洩露。
失去完整性(Integrity Loss)	敏感性或專有資訊被更改或刪除。

表 3-4 顯示了可恢復性工作類別的範例，這些類別反映了從事件中復原所需的資源等級和類型。

表 3-4，可恢復性工作類別

類別	定義
一般的 (Regular)	利用現有資源可以預測恢復時間。
增補的 (Supplemented)	透過額外的資源和外部協助可以預測恢復時間。
擴充的 (Extended)	需要額外的資源和外部協助無法預測恢復時間。
不可恢復 (Not Recoverable)	無法從事件中恢復(例如，敏感資料外洩並被公開發布)。

組織應針對團隊若未在指定時間內對事件做出應變時的事件升級流程。發生這種情況的原因有很多，例如，因手機故障或者個人處理緊急私事而無法聯繫。升級流程應規範等待應變的時間以及如果沒有執行應變的後續處理流程。程序的第一步掌握聯繫管道，等待一段時間(例如 15 分鐘)後，通報者將事件升級到更高級別，通報應變團隊上一層主管，例如事件應變團隊經理，如果經理在一定時間內仍沒有回應，則該事件應再次升級至更高階的管理人員，重複此過程，直到有人做出回應。

3.2.7 事件通知

對事件進行分析和優先排序時，事件應變團隊需要通知適當的人員，以便讓所有參與的人都能發揮作用。事件應變政策應包括有關事件通報的規定：向誰通報、在什麼時間通報。通常通報的對象因組織要求而異，但收到通知的人員一般會包括：

- 資訊長。
- 資訊安全主管。
- 當地資訊安全官。
- 組織內的其他事件應變團隊。
- 外部事件應變團隊(必要時才通報)。
- 系統擁有者。
- 人力資源部門(涉及員工的案件)。

- 公共事務部門(可能引起公眾關注的事件)。
- 法務部門(具有潛在法律後果的事件)。
- US-CERT(代表聯邦政府運作的聯邦機構和系統需求)。
- 政府執法單位(必要時才通報)。

在事件處理期間，團隊需要向某些單位提供狀態更新，因此團隊應規劃和準備多種溝通方法，並選擇適合特定事件的方法進行溝通：

- 電子郵件。
- 網站(內部或外部網站或企業入口網站)。
- 電話。
- 親自出席簡報。
- 語音信箱問候語。
- 在佈告欄和門上張貼通知，在所有入口處分發通知。

3.3 遏制、根除和復原

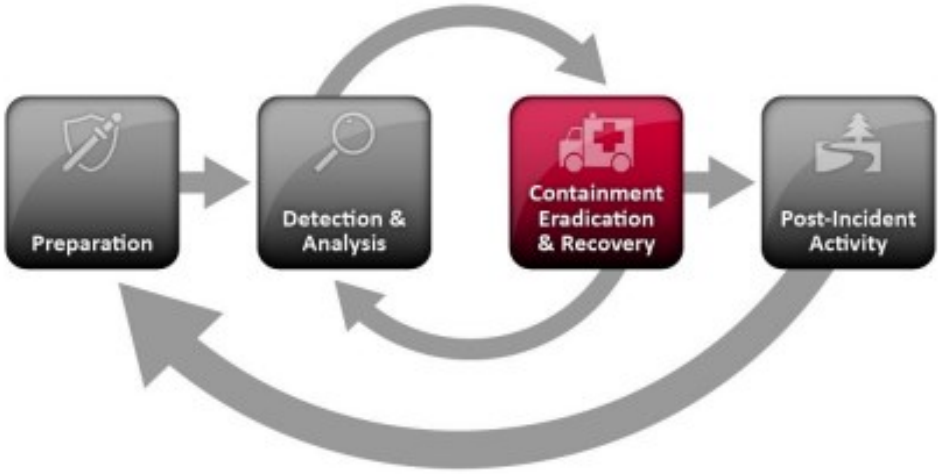

圖 3-3，事件應變生命週期(遏制、根除和復原)

3.3.1 選擇遏制策略

在事件導致資源不堪負荷或損害加劇之前就要將其遏制。大多數事件都需要先進行遏制，因此這是早期處理事件過程中最重要行動，遏制是為了執行量身訂做的補救策略提供緩衝時間。遏制最重要部分是決策(決定關閉系統、斷網、停用功能…等作為)。如果有預先決定的控制事件策略和程序，那麼做出決定就會容易得多，因此，組織應定義遏制事件時可接受的風險並制定相應的策略。

遏制策略根據事件類型而有所不同，遏制透過電子郵件傳播惡意軟體感染的策略與網路的 DDoS 攻擊的方法就有所不同。組織應為重大事件類型制定單獨的遏制策略，並明確定義其標準以促進決策。這些遏制策略的標準通常包括：

- 資源的潛在損壞和被盜竊的可能性。
- 證物保全的必要性。
- 服務可用性(例如網路連線、提供給外部各方的服務)。
- 實施遏制策略所需的時間和資源。
- 策略的有效性範圍(部分遏制或完全遏制)。
- 執行遏制方案的持續時間(例如，緊急方案實施後在四小時內可解除事件，臨時性解決方案實施後在

兩週內解除事件)。

某些情況下，可以嘗試將攻擊者重新導向到沙箱，以便監視攻擊者的活動，或者收集額外的證據。監測攻擊者行為不應該使用沙箱之外的環境，如果一個組織知道系統已被破壞並允許繼續破壞，那麼如果攻擊者使用受感染的系統攻擊其他系統，則該組織可能要承擔責任。延遲遏制策略很危險，因為攻擊者可能會擴大未經授權的存取或危害其他系統。

關於遏制的另一個潛在問題是，某些攻擊行為在被遏制後可能會造成額外的傷害。例如，受感染的主機定期對另一台主機執行 ping 操作的惡意程式，當事件處理程序嘗試透過中斷受感染主機與網路的連線來遏制事件時，後續 ping 將會失敗，由於失敗，惡意程式會開始覆蓋或加密主機硬碟上的所有資料以毀滅攻擊證據。事件處理程序不應該假設主機已與網路斷開連接，就可以防止惡意程式對該主機的進一步損壞。

3.3.2 證據蒐集與處理

儘管在事件期間收集證據的主要原因是為了解決事件，但也可能當走向法律訴訟時作為司法攻防的證據。在這種情況下，清楚記錄所有證據(包括受損系統)的保存方式非常重要，應根據先前與法律工作人員和適當執法機構討論制定的符合所有適用法律和法規的程序收集證據，以便任何證據都可以在法庭上被採信。任何時候都應考慮證據保全，當證據在人與人之間轉移時，證據鍊(Chain of custody，COC)表格應詳細說明轉移情況並包括各方的簽名，保留的證據應包括以下內容：

- 識別資訊(電腦的位置、序號、型號、主機名稱、MAC 和 IP 位址)。
- 調查期間收集或處理證據的每個人的姓名、職位和電話號碼。
- 每次證據處理發生的時間和日期(包括時區)。
- 證據存放地點。

一旦懷疑可能發生事件，就要開始從系統中取得相關證據，然而，事件處理過程通常會導致一系列動態事件的發生，與此階段可以採取的大多數其他操作結果相比，初始系統快照可能更有助於識別問題及其根源。從證據的角度來看，最好按原樣獲取系統快照，而不是在事件處理程序、系統管理員和其他人在調查過程中無意中更改了機器狀態後才獲取系統快照。使用者和系統管理員應了解他們應採取的保存證據的步驟，這部分可參考 NIST SP 800-86，將取證技術整合到事件應變中的指南，了解有關保存證據的更多資訊。

3.3.3 識別攻擊主機

在事件處理過程中，系統擁有者和應變團隊有時會希望或需要先識別攻擊主機。儘管這些資訊可能很重要，但事件處理人員應優先專注於遏制、根除和復原。識別攻擊主機可能是一個耗時且徒勞無功的過程，甚至影響團隊實現盡快減少業務衝擊的主要目標。當需要時，可透過以下建議的活動識別攻擊主機：

- **驗證攻擊主機的 IP 位址。**事件處理程序通常會專注於攻擊主機的 IP 位址，處理程序中會嘗試透過驗證與該位址的連線來確認該位址是否被欺騙，然而，這方法只能證實該位址的主機是否回應請求，主機未能回應並不意味著該位址不真實，例如，攻擊主機可能被設定忽略 ping 和追蹤路由，或者攻擊者隨機重新指派動態位址。
- **透過搜尋引擎研究攻擊主機。**使用攻擊的來源 IP 位址執行 Internet 搜尋有可能獲得有關該攻擊的更多資訊。
- **使用事件資料庫。**將多個應變小組收集來自不同組織的事件資料並將其整合到事件資料庫中。這種資訊共享可以透過多種形式進行，例如事件追蹤器、即時黑名單、檢查自己的知識庫或導入相關的問題追蹤系統。
- **監控可能的攻擊者通訊管道。**事件處理程序可以監視攻擊主機可能使用的通訊通道。例如，許多機器

人使用 IRC 作為主要通訊方式。攻擊者可能會聚集在某些 IRC 頻道上吹噓他們的妥協並分享資訊，關於這類消息，事件處理者應該僅視為潛在的線索，而不是事實。

3.3.4 根除和復原

事件被遏制後，接著需要採取根除措施來消除事件根源，例如，刪除惡意軟體和被破壞的使用者帳戶，以及識別和修補被利用的漏洞。在根除過程中，識別組織內所有受影響的主機非常重要，以便可以徹底對事件影響進行修復。

在復原過程中，管理員將系統復原至正常狀態、確認系統正常運行，並修復漏洞以防止類似事件復發。復原程序通常包括從乾淨的備份復原系統、從頭開始重建系統、用乾淨的版本替換受損檔案、安裝修補程式、更改密碼以及加強網路外圍安全(防火牆規則集、邊界路由器存取控制清單)等操作。加強系統日誌記錄或網路監控也是復原過程的一部分，一旦某個資源被成功攻擊，它通常會再次受到攻擊，或者組織內的其他資源以類似的方式受到攻擊，因此需加強監控。

根除和復原應分階段進行，對於大規模事件，完全復原可能需要數個月時間，早期階段的目的應該是透過相對快速(數天內)的快速應變來提高整體安全性，以防止未來發生事件。後期階段則專注於長期架構改變(例如基礎設施變化)以盡可能確保企業的安全。由於根除和復原操作通常是特定於作業系統或應用程式的，詳細說明和建議不在本文件範圍。

3.4 事件後活動

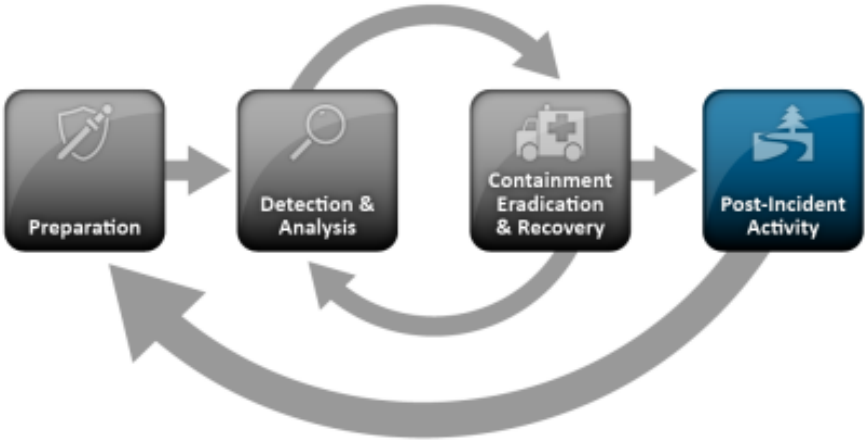

圖 3-4，事件應變生命週期(事件後活動)

3.4.1 經驗教訓

事件應變最重要的部分也是最常被忽略的就是學習和改進。事件應變團隊應該不斷進步，持續精進技術和所學到的經驗教訓以應付新的威脅。在事件發生後定期與所有相關單位舉行「經驗教訓」會議，對於改進安全措施和事件處理流程本身非常有幫助。一次經驗教訓會議可以涵蓋多個事件，透過檢視發生的情況、採取的干預措施以及介入效果的成效來介紹事件處理經驗。經驗教訓會議應在事件處理結束後幾天內舉行，會議主題包含以下問題：

- 究竟發生了什麼事、在什麼時間發生？
- 員工和管理階層在處理事件方面表現如何？是否遵循了書面程序？這些程序足夠嗎？
- 事件處理過程需要什麼即時資訊？
- 是否採取了任何可能阻礙復甦的步驟或行動？
- 下次發生類似事件時，員工和管理階層會採取哪些不同的做法？
- 如何改善與其他組織的資訊共享？

- 哪些改善措施可以防止將來發生類似事件？
- 未來該關注哪些徵兆或指標來發現類似事件？
- 需要哪些額外的工具或資源來偵測、分析和緩解未來的事件？

小事件只需要小型的事後分析，但引起廣泛關注和興趣的新型攻擊方法的事件除外。發生嚴重攻擊後，必需召開跨團隊和組織邊界的事後分析會議，以提供資訊共享。召開此類會議的首要考慮因素是確保合適的人員參與，不僅邀請參與正在分析的事件的人員很重要，而且也應該邀請可促進未來的合作的對象。

會議的成功也取決於議程，在會議之前收集參與者期望和需求的意見可以增加滿足參與者需求的可能性，在會議開始之前或會議期間制定議事規則可以減少混亂和不和諧。擁有一名或多名擅長團體協調的主持人可以帶來很高的會議成效。最後，紀錄會議記錄和 AR 並將其傳達給無法出席會議的各方。

經驗教訓會議還有其他好處。這些會議的報告是培訓新團隊成員的良好材料，可以向他們展示經驗豐富的團隊成員如何應對事件。更新事件應變政策和程序是吸取經驗教訓的另一個重要部分。事件處理後的分析通常會發現程序中缺少的步驟或不精確的地方，從而為變革提供動力。由於資訊科技的進步和人員的異動，事件應變團隊應按指定的時間定期審查處理事件所有文件和程序的適用性。

另一個重要的事件後活動是為事件建立後續報告，這對於未來的使用非常有價值。該報告為協助處理類似事件提供了參考。考量法律相關的規定，建立正式的事件時序表和事件造成的損害估計也很重要，這些資料可做為美國司法部後續訴訟的參考，所有報告應依照記錄保留政策的規定保存。

3.4.2 使用收集的事件數據

經驗教訓活動會產生有關事件的客觀和主觀數據。隨著時間的推移，收集到的事件資料應該可以在多個方面發揮作用。這些數據，特別是參與的總時間和成本，可用於證明為事件應變團隊提供額外資金的合理性。對事件特徵的研究可以顯示系統的安全弱點、潛在威脅，以及安全事件的趨勢變化。這些數據可以回饋到風險評估流程中，輔助選擇和實施額外的控制措施。數據的另一個很好的用途是衡量事件應變團隊的成效，如果事件資料被正確收集和儲存，它應該能夠提供事件應變團隊成功的多種衡量標準。這些數據也可以用來衡量事件應變團能力的變化是否會與團隊績效的變化一致(例如效率提高、成本降低)，除此之外，負責通報事件的組織也需要必要的數據來滿足他們的要求。有關與其他組織共享事件資料的更多信息，請參閱第 4 節。

組織應該專注於收集可用於操作或改善的數據，而不是僅僅為了收集數據而收集數據，例如收集每週發生的網路連接埠掃描數量並在年底產生的圖表顯示連接埠掃描增加了 8%，這樣的資訊並沒有很大的幫助，而且收集這些資料可能非常耗時。只有絕對數字並不能提供資訊，重要的是了解這些數字如何反應在對組織業務流程的威脅。組織應根據通報要求和數據的預期投資回報(例如，識別新威脅並在相關漏洞被利用之前減輕相關漏洞)來決定收集哪些事件數據。應該收集的事件相關數據包括：

- **處理的事件數量。**處理越多事件不一定越好，處理的事件數量可能會因為更好的網路和主機安全控制而減少，而不是因為事件應變團隊的疏忽而減少了處理的件數。處理的事件數量最好作為事件應變團隊必須執行的相對工作量的衡量標準，而不是作為團隊品質的衡量標準。為每一個事件類別產生單獨的事件計數作為工作品質指標會更有效。
- **事件處理的時間。**對於每一個事件，可以透過多種方式測量時間：
  - 處理該事件所花費的勞動力總投入時間。
  - 從事件開始到事件被發現、初始影響評估以及事件處理過程的各階段所花費的時間。
  - 事件應變團隊花了多長時間對事件的初步通報做出回應。
  - 向管理階層以及必要時向適當的外部實體(例如 US-CERT) 通報事件需要多長時間。
- **對事件的客觀評估。**分析已解決事件的應變以確定其有效性，以下是一些範例：

- 審查日誌、表格、通報和其他文件，以確保遵守既定的事件應變政策和程序。
- 確定記錄了哪些事件前兆和指標，以確定記錄和識別事件的有效性。
- 在事件被發現之前確定事件是否造成損害。
- 確定是否已識別事件的實際原因，並識別攻擊媒介、利用的漏洞以及目標或受害系統、網路和應用程式的特徵。
- 確認該事件是否為先前事件的重複發生。
- 計算事件造成的損失。
- 衡量初始影響評估和最終影響評估之間的差異(見第 3.2.6 節)。
- 確定哪些措施可以避免該事件的發生。

■ **對事件的主觀評估。**事件應變團隊成員會被要求評估自己以及其他團隊成員和整個團隊的表現。其中一個有價值的資訊來源是訪談所有受到攻擊的資源擁有者，確認是否擁有者認為事件得到了有效處理以及是否滿意處理結果。

除了使用這些指標來衡量團隊的成效之外，組織可以定期審查其事件應變計畫，透過審查可發現問題和缺陷，然後予以糾正。事件應變審查應根據適用的法規、政策和普遍接受的做法評估以下項目：

■ 事件應變政策、計劃和程序。
■ 工具和資源。
■ 團隊模式與架構。
■ 事件處理人員訓練與教育。
■ 事件文件和報告。
■ 應變成效的衡量標準。

3.4.3 證據保留

組織應制定政策規定事件證據保留期限，大多數組織選擇在事件結束後數月或數年保留所有證據。制定政策時應考慮以下因素：

■ **法律訴訟。**如果攻擊者有可能被起訴，則證據需要保留到所有法律行動完成為止。某些情況下訴訟可能需要經過幾年的時間。現在看來無關緊要的證據將來可能會變得非常重要，例如若攻擊者能夠使用第一次攻擊中收集的知識來執行以後更嚴重的攻擊，那麼第一次攻擊的證據可能是解釋第二次攻擊是如何完成的關鍵。
■ **保留天數。**大多數組織都有資料保留策略，規定某些類型的資料可以保留多久。一般記錄表(GRS)規定事件處理記錄應保存至少三年。
■ **儲存成本。**保留原始受損的硬體以及保存磁碟映像檔的硬碟和移動儲存裝置通常成本不高，但是如果組織將許多此類相關證據保留多年，則會提高儲存成本。

■ **事件處理清單**

表 3-5 提供了處理事件時要執行的主要步驟。請注意，實際執行的步驟可能會根據事件類型和個別事件的性質而有所不同。例如，如果處理程序根據指標分析確切地知道發生了什麼(步驟 1.1)，則可能不需要執行步驟 1.2 或 1.3 來進一步研究該活動。這件清單僅為處理人員提供了執行主要步驟的指南，沒有規定應該始終遵循此步驟。

表 3-5，事件處理清單

	行動	已完成
檢測分析		
1.	判斷事件是否發生	
1.1	分析前兆和指標	
1.2	尋找相關資訊	
1.3	進行研究(善用搜尋引擎、知識庫)	
1.4	一旦處理人員認為發生了事件，就開始記錄調查並收集證據	
2.	根據相關因素(功能影響、資訊影響、是否可恢復工作…等)優先處理事件	
3.	向適當的內部人員和外部組織通報事件	
遏制、根除和恢復		
4.	取得、保存、保護和記錄證據	
5.	遏制事件	
6.	消滅事件	
6.1	識別並緩解所有被利用的漏洞	
6.2	刪除惡意軟體、不適當的資料和其他不應該存在的元件	
6.3	如果發現更多受影響的主機或新的惡意軟體感染，則重複偵測和分析步驟(1.1、1.2)以識別所有其他受影響的主機，然後遏制(5)並根除(6)它們	
7.	從事件中恢復	
7.1	將受影響的系統恢復到操作就緒狀態	
7.2	確認受影響的系統正常運作	
7.3	如有必要，實施額外的監控以強化未來的相關活動	
事件後活動		
8.	建立後續報告	
9.	召開經驗教訓會議(重大事件務必召開)	

3.5 建議

本節中提出的處理事件的主要建議總結如下。

- **取得在事件處理過程中有價值的工具和資源。**如果團隊擁有各種可用的工具和資源，例如聯絡人清單、加密軟體、網路圖、備份設備、數位取證軟體和連接埠清單，他們將能夠更有效率地處理事件。
- **確保網路、系統和應用程式足夠安全，防止事件發生。**預防勝於治療，定期進行風險評估並將已識別的風險降低至可接受的程度可有效減少事故數量。使用者、IT 人員和管理階層對安全策略和程序的認知也非常重要。
- **透過多種類型的安全軟體產生的警報來識別前兆和指標。**入侵偵測和防禦系統、防毒軟體和檔案完整性檢查對於偵測事件跡象非常有用。每種類型的軟體都可以偵測到其他類型的軟體無法偵測到的事件，因此強烈建議使用多種類型的電腦安全軟體或採購第三方監控服務。
- **建立外部各方通報事件的機制。**外部各方可能希望向組織通報事件，例如，他們可能認為組織的特定使用者正在攻擊他們，組織應公佈聯絡電話號碼和電子郵件地址，供外部各方通報資訊安全事件。
- **要求所有系統上的日誌記錄和審核 Baseline，以及所有關鍵系統上的更高 Baseline。**來自作業系統、服務和應用程式的日誌經常在事件分析過程中提供有用的資訊，特別是在啟用 Audit 機制的情況下。日誌可以提供諸如查詢了哪些帳戶以及執行了哪些操作等資訊。
- **網路和系統的活動特徵。**分析及測量活動的特徵，以便於更容易識別與預期情況不同的變化。如果分析過程是自動化的，則可以快速檢測到與預期活動水平的偏差並向系統管理員通報，從而更快地檢測事件和操作問題。
- **了解網路、系統和應用程式的正常行為。**掌握正常行為的團隊成員應該能夠更輕鬆地識別異常行為。建議透過件查相關日誌和安全警報來獲取這些知識，處理人員應該熟悉典型的數據並調查不尋常的項目以掌握更多資訊。
- **建立日誌保留策略。**有關事件的資訊可能會記錄在多個位置。因為較舊的日誌條目可能會顯示偵察活動或類似攻擊的先前跡象，建立和實施指定日誌資料保留策略對資料分析非常有幫助。
- **執行事件關聯分析。**事件的證據可能會記錄在多個日誌中，在收集事件的所有可用資訊並驗證事件是否發生時，將多個來源之間的事件關聯起來非常有價值。
- **保持所有主機時鐘同步。**如果通報事件的裝置時鐘設定不一致，事件關聯會更加複雜。從證據的角度來看，時鐘差異也可能會造成問題。
- **維護和使用資訊知識庫。**處理人員在事件分析過程中需要快速查閱資訊，集中的知識庫可提供一致、有維護的資訊來源。知識庫應包括詳細訊息，例如關於先前事件的前兆和指標的數據。
- **一旦團隊懷疑發生了事件，就開始記錄所有資訊。**從事件被發現到最終解決完畢，所有採取的步驟都應該記錄下來並加蓋時間戳。如果提出法律訴訟，此類資訊可以作為法庭證據。記錄執行的步驟還可以讓處理問題過程更有效、更有系統性、更不易出錯。
- **保護事件資料。**包含有關安全漏洞和可能執行不當操作的用戶等敏感資訊。團隊應確保對事件資料的存取在邏輯和物理上都受到適當的限制。
- **根據相關因素，對事件進行優先處理。**由於資源限制，事件不應按照先到先服務的原則進行處理。組織應該建立準則，根據事件的功能和資訊影響以及事件的可能恢復性等相關因素，規範團隊必須以多快的速度回應事件以及應執行哪些操作。這節省了事件處理程序的時間，並為管理層和系統所有者的操作提供了合理的理由。當團隊未在指定時間內對事件做出回應時，組織也應針對這些情況建立升級流程。
- **將有關事件通報的規定納入組織的事件應變政策中。**組織應明確規範必須通報哪些事件、何時通報以及向誰通報。最常收到通報的對象是 CIO、資訊安全主管、本地資訊安全長、組織內的其他事件應變團隊和系統所有者。
- **制定遏制事件的策略和程序。**快速有效地遏制事件以限制其業務影響非常重要，組織應定義遏制事件的可接受風險，並相應制定策略和程序。遏制策略應根據事件類型而有所不同。

- **遵循既定的證據收集和處理程序。**團隊應清楚記錄所有證據是如何保存的，任何時候都應考慮證據保全。團隊應與法務人員和執法機構討論證據處理，然後根據這些討論結果制定證據保全程序及規範。
- **從系統中捕獲易失性數據作為證據。**這包括網路連接、執行程式、登入連線、開啟檔案、網路介面配置和記憶體內容的清單。以不會損壞系統為原則，從可信任的裝置執行指令收集必要的數據證據。
- **透過完整的取證磁碟映像取得系統快照，而不是檔案系統備份。**磁碟映像檔應製保存於經過 Format 的可寫入保護或一次性寫入媒體，從調查和做為證據的角度來看，此類當下狀況的快照優於檔案系統備份。映像檔的價值還在於，分析映像檔比對原始系統進行分析要安全得多，因為分析可能會無意中改變原始系統。
- **重大事件發生後召開總結經驗教訓會議。**經驗教訓會議對於改善安全措施和事件處理流程本身非常有幫助。

4 協調和資訊共享

當代威脅和攻擊的本質使得組織在事件應變期間的合作比以往任何時候都更加重要。組織應確保與適當的合作夥伴有效協調事件應變活動，而事件應變協調最重要的方面是資訊共享，不同的組織相互共享威脅、攻擊和漏洞訊息，讓組織知識使另一個組織受益。事件資訊共享通常是互惠互利的，因為相同的威脅和攻擊通常會同時影響多個組織。

如第 2 節所述，與合作夥伴組織協調和分享資訊可以增強組織有效應變 IT 事件的能力。如果一個組織識別出其網路上的某些看似可疑的行為，並將有關該事件的資訊發送給一組可信任的合作夥伴，則該網路中的其他人可能已經看到了類似的行為，並且能夠透過其他有關可疑行為的詳細資訊進行應變活動，包括變更數位簽章、尋找其他指標或建議的補救措施。與孤立運作的組織相比，與值得信賴的合作夥伴的協作可以使組織更快、更有效地應變事件。

標準事件應變技術效率的提升並不是跨組織協調和資訊共享的唯一動力。資訊共享的另一個動機是能夠使用單一組織可能無法使用的技術來應變事件，特別是如果該組織是中小型組織。小型組織可能沒有內部資源來全面分析特別複雜的惡意軟體並確定其對系統的影響，在這種情況下，組織可以利用可信任資訊共享網路有效地將惡意軟體的分析外包給具有足夠技術能力來執行惡意軟體分析的第三方資源。

本章說明協調和資訊共享。4.1 節概述了事件應變協調，並專注於跨組織協調的需求，以補充組織事件應變流程。第 4.2 節討論了跨組織資訊共享的技術，第 4.3 節研究如何限制與其他組織共享或不共享的資訊。

4.1 協調

如同第 2.3.4 節所討論的，組織在進行事件應變活動的過程中可能需要與多種類型的外部組織互動。這些組織的例子包括其他事件應變團隊、執法機構、網路服務供應商以及民眾和客戶。組織的事件應變團隊應在事件發生之前規劃與各方的事件協調，以確保所有各方都了解自己的角色並建立有效的溝通管道。圖 4-1 提供了組織在事件應變命週期的各階段執行協調的範例視圖，強調協調在整個生命週期的價值。

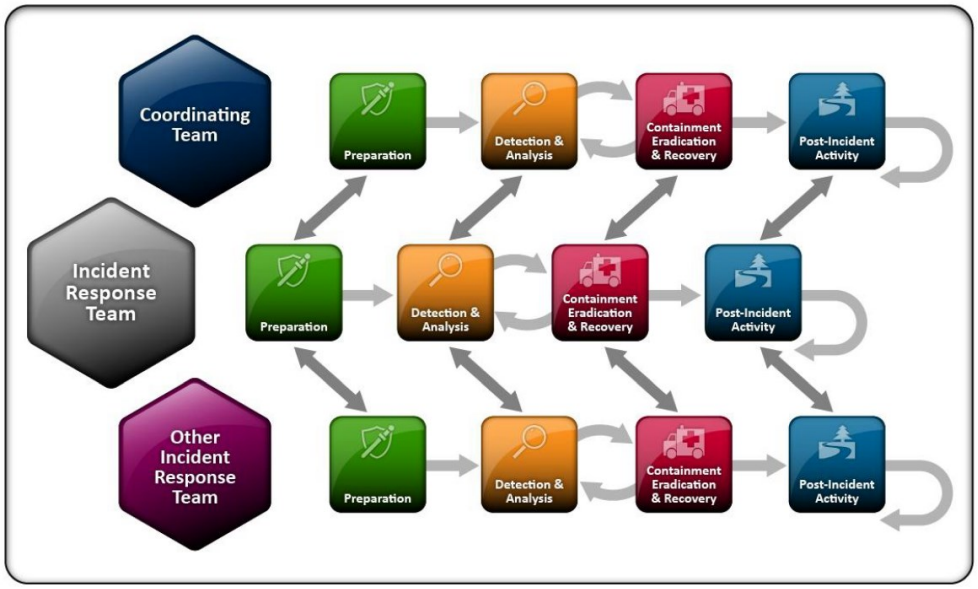

圖 4-1，事件應變協調

4.1.1 協調關係

組織內的事件應變團隊可以參與不同類型的協調安排，這取決於與之協調的組織類型。例如，負責事件應變技術細節的團隊成員可以與合作夥伴組織的營運同事協調，分享緩解跨多個組織的攻擊的策略。或者在同一個事件處理期間，事件應變團隊經理可以與 ISAC 協調以滿足必要的通報要求，並尋求建議和額外資源以強化事件應變。表 4-1 提供了與外部組織協作時可能存在的協調關係的一些範例。

表 4-1，協調關係

類別	定義	資訊共享
團隊對團隊	只要不同組織中的技術事件應變人員在事件處理生命週期的任何階段互相合作就存在團隊與團隊之間的關係。參與這種關係的組織通常是同行，彼此之間沒有任何權力，並選擇共享資訊、匯集資源和重複使用知識來解決兩個團隊共同的問題。	團隊間關係中最常分享的資訊是戰術和技術資訊(例如，妥協的技術指標、建議的補救措施)，但如果作為準備工作的一部分進行，也可能包括其他類型的資訊(計劃、程序、經驗教訓)。
團隊對協調小組	團隊與協調團隊的關係存在於組織事件應變團隊和充當協調事件應變和管理中心點的獨立組織(例如 US CERT 或 ISAC)之間。這種類型的關係可能包括協調機構要求成員組織進行某種程度的通報，以及期望協調小組向參與的成員組織傳播及時和有用的信息。	團隊和協調團隊經常分享戰術、技術資訊以及有關協調團隊所服務的社區的威脅、漏洞和風險的資訊。協調團隊還需要提供有關事件的具體影響訊息，以幫助決定將資源和注意力集中在哪裡。
協調團隊對協調團隊	US-CERT 和 ISAC 等多個協調團隊之間存在關係，以分享與可能影響多個領域的跨領域事件相關的資訊。 協調團隊代表各自的社群成員組織行事，分享有關跨領域事件的性質和範圍以及可重複使用的緩解策略的信息，以協助社群間的事件應變。	協調團隊與其對應方共享的資訊類型通常包括「恆定狀態」期間的定期摘要，並在協調的事件應變活動期間交換戰術、技術細節、應變計劃以及影響或風險評估資訊。

組織可能會發現建立協調所需的關係具有挑戰性，建立社群可以從組織所屬的產業部門和組織運作的地理區域開始。組織的事件應變團隊可以嘗試與自己的產業部門和區域內的其他團隊(在團隊到團隊層級)建立關係，或加入產業部門內已經促進資訊共享的既定機構。建立關係的另一個考慮因素是，有些關係是強制性的，有些是自願的，例如，團隊與協調團隊之間的關係通常是強制性的，而團隊與團隊之間的關係通常是自願的。組織追求自願關係是因為它們滿足共同的自身利益，強制性關係通常由行業內的監管機構所規定。

4.1.2 共享協議和通報要求

試圖與外部組織分享資訊的組織應在開始任何協調工作之前諮詢法務部門。在合作之前需要簽訂合約或其他協議，例如用於保護組織最敏感資訊機密性的保密協議 (NDA)。組織還應考慮任何現有的通報要求，例如與 ISAC 共享事件資訊或向更高級別的 CSIRT 通報事件。

4.2 資訊共享技術

資訊共享是實現跨組織協調的關鍵要素。即使是最小的組織也需要能夠與同行和合作夥伴共享事件

訊息，以便於有效地處理許多事件。組織應在整個事件應變生命週期中執行此類資訊共享，而不是等到事件完全解決後再與其他人共享詳細資訊。第 4.3 節討論了組織可能願意或不願意與他人分享的事件資訊類型。

本節重點介紹資訊共享技術。 4.2.1 節著重於臨時方法，4.2.2 節則研究部分自動化的方法，第 4.2.3 節討論了與資訊共享相關的安全注意事項。

4.2.1 臨時方法

傳統上，大多數事件資訊共享都是透過臨時性的方法進行的，例如透過電子郵件、即時通訊用戶端和電話。臨時資訊共享機制通常依賴單一員工與合作夥伴組織的事件應變團隊中的員工的聯繫。員工透過這些手動方式與其他人分享訊息，並與他們協調制定應變事件的策略。根據組織的規模，這些臨時技術可能是與合作夥伴組織分享資訊的最具成本效益的方式。然而，由於臨時資訊共享的非正式性質，不可能保證資訊共享過程始終有效。例如，如果人脈特別廣的員工從事件應變團隊辭職，該團隊可能會暫時失去與外部組織有效協調所依賴的大部分資訊共享管道。

臨時資訊共享方法在傳達什麼訊息以及如何進行溝通方面也基本上沒有標準化。由於缺乏標準化，它們往往需要手動干預，相較於自動化方法，手動更耗費資源。因此只要有可能，組織就應該嘗試透過與合作夥伴組織的正式協議和自動化資訊共享的技術機制來建立其資訊共享策略。

4.2.2 半自動化方法

組織應盡可能嘗試實現資訊共享流程的自動化，以提昇跨組織協調效率及降低成本。實際上，完全自動化地共享所有事件資訊是不可能的，考量出於安全和信任的考慮，這也是不可取的。組織應嘗試實現自動化資訊共享與以人為中心的管理資訊流程之間的平衡。

在設計自動化資訊共享解決方案時，組織應先考慮他們將與合作夥伴交流哪些類型的資訊。組織可能希望建立一個正式的資料字典，列舉他們希望共享的所有實體以及實體之間的關係。一旦組織了解他們將共享的資訊類型，就有必要建立正式的、機器可處理的模型來捕獲這些資訊。只要有可能，組織就應該使用現有的資料交換標準來表示他們需要的資訊分享。在決定資料交換模型時，組織應與其合作夥伴組織合作，以確保所選標準與合作夥伴組織的事件應變系統相容。在選擇現有資料交換模型時，組織可能更願意選擇對事件回應域的不同面向進行建模的多個模型，然後以模組化方式利用這些模型，僅傳達生命週期中特定決策點所需的訊息。

除了選擇用於共享事件資訊的資料交換模型之外，組織還必須與其夥伴組織合作，就技術傳輸機制達成一致，以使資訊交換能夠以自動化方式進行。這些傳輸機制至少包括用於交換資訊的傳輸協定、用於與資訊資源通訊的體系結構模型以及用於存取特定組織中的資訊資源的適用連接埠和網域名稱。例如，合作夥伴組織決定使用 Restful 架構來交換事件訊息，透過 HTTPS 在連接埠 4590 上通過組織 DMZ 內的特定網域交換 IODEF/即時網間防禦(RID) 數據。

4.2.3 安全考量

事件應變團隊在規劃資訊共享時應考慮幾個安全注意事項。一是能夠指定誰可以查看哪些事件資訊，其次需要定期執行數據清理以從事件資訊中刪除敏感數據，而不干擾前兆、指標和其他技術的資訊。有關精緻化資訊共享的更多參考，請參閱第 4.3 節。事件應變團隊也應確保採取必要的措施來保護其他組織與團隊分享的資訊。關於數據共享還需要考慮許多法律問題，這些資訊請參閱第 4.1.2 節。

4.3 細粒度資訊共享

組織需要平衡資訊共享的好處與共享敏感資訊的缺點，最理想情況是與適當的各方共享資訊但僅共享必要的訊息。組織可以將其事件資訊視為由兩種類型的信息組成：業務影響和技術。業務影響資訊通常在第 4.1.1 節中定義的團隊與協調團隊關係的背景下共享，而技術資訊通常在所有三種類型的協調關係

中共享。本節討論這兩種類型的訊息，並提供執行精緻化資訊共享的建議。

4.3.1 業務影響資訊

業務影響資訊涉及事件如何在業務、財務等方面影響組織。此類資訊通常會通報給更高層級的協調事件應變團隊，以傳達該事件造成的估計損失。協調應變團隊需要此影響資訊來做出對其他組織提供的協助程度。協調團隊還可以使用這些資訊來做出與特定事件將如何影響他們所代表的社區中的其他組織相關的決策。

業務影響資訊僅適用於向對經歷事件感興趣的組織進行通報，大部分情況下，事件應變團隊應避免與外部組織分享業務影響訊息，除非有明確的價值主張或正式的通報要求。與同儕和合作夥伴組織分享資訊時，事件應變團隊應專注於交換第 4.3.2 節中概述的技術資訊。

4.3.2 技術資訊

有許多不同類型的技術指標反應組織內發生安全事件，這些指標源自於與事件相關的各種技術訊息，例如攻擊主機的主機名稱和 IP 位址、惡意軟體樣本、類似事件的前兆和指標以及事件中利用的漏洞類型。

雖然組織可以透過收集自己的內部指標來獲得價值，但他們也可以透過分析從合作夥伴組織收到的指標以及共享內部指標以供外部分析和使用來獲得額外的資訊。如果組織收到與他們未見過的事件相關的外部指標數據，他們可以使用該指標數據在事件開始發生時識別該事件。同樣，組織可以使用外部指標數據來檢測由於缺乏內部資源來捕獲特定指標數據而掌握正在進行的事件。組織還可以從與外部組織共享其內部指標數據中受益，例如，共享他們正在經歷的事件相關的技術資訊，合作夥伴也可能會提供處理該事件的建議補救策略協助進行應變。

組織應盡可能共享此類資訊，然而，出於安全和責任原因，組織可能不想透露被利用漏洞的詳細資訊。關於攻擊的一般特徵和攻擊主機的身份這類外部指標通常可以安全地與其他人共享。組織應考慮哪些類型的技術資訊應該或不應該與各方共享，然後努力與其他組織分享盡可能多的適當資訊。

技術指標雖然能夠幫助組織識別實際事件，然而，並非所有從外部來源收到的指標資料都與接收該資料的組織有關。在某些情況下，這些外部資料可能產生誤報，並可能導致資源花費在不存在的問題上。

參與事件資訊共享的組織應擁有熟練的員工，能夠從共享社區獲取技術指標訊息，並最好以自動化方式在整個企業內傳播該訊息。組織還應嘗試確保他們僅分享他們對其表示實際事件具有相對較高信心的指標。

4.4 建議

本節中提出的處理事件的主要建議總結如下。

- **在事件發生之前規劃與外部各方的事件協調。**外部各方的範例包括其他事件應變團隊、執法機構、網路服務供應商以及客戶，此規劃有助於確保所有各方都了解自己的角色並建立有效的溝通管道。
- **在開始任何協調工作之前，請諮詢法律部門。**互相合作可能需要簽訂合約或其他協議。
- **在整個事件應變生命週期中就開始共享事件資訊。**資訊共享是實現跨組織協調的關鍵要素，組織不應等到事件完全解決後才與其他人分享事件的詳細資訊。
- **盡可能讓資訊共享過程自動化。**這使得跨組織協調變得有效率且具有成本效益，組織應在自動化資訊共享與以人為中心的資訊流管理流程之間取得平衡。
- **平衡資訊共享的好處與共享敏感資訊的缺點。**理想情況下，組織應與適當的各方共享必要的信息，並且僅共享必要的資訊。業務影響資訊通常只在團隊與協調團隊關係中共享，而技術資訊通常在所有類型的協調關係中共享。在與同儕和合作夥伴組織分享資訊時，事件應變團隊應專注於交換技術資訊。

- **與其他組織分享盡可能多的適當事件資訊。**組織需考慮哪些類型的技術資訊應該或不應該與各方共用。外部指標通常可以安全地與其他人共享，但出於安全和責任原因，組織可能不想透露被利用的弱點詳細資訊。

附錄 A 事件應變處理情境

事件應變處理情境提供了一種便宜且有效的方法來訓練事件應變技能並識別事件應變流程中的潛在問題。其做法是向事件應變團隊或團隊成員提供一個場景和一系列相關問題，然後團隊討論每一問題並確定最有可能的答案，其目標是確認團隊要做的事情，並將其與政策、程序和建議的實作進行比較，以發現差異或缺陷。

下面列出的問題幾乎適用於任何場景，每一題後面都附有文件相關部分的引用。問題後面是情境，每一個情境後面都有其他特定事件的問題。強烈鼓勵組織調整這些問題和情境，以便於練習中使用。

A.1 情境問題

準備：

1. 組織是否會將此活動視為事件？如果是，此活動違反了組織的哪些政策？(第 2.1 節)
2. 採取了哪些措施來防止此類事件的發生或限制其影響？(第 3.1.2 節)

檢測分析：

1. 組織可能會偵測到哪些事件先兆？是否有任何前兆導致組織在事件發生前採取行動？(第 3.2.2、3.2.3 節)
2. 組織可能偵測到哪些事件指標？哪些指標會讓某人認為可能發生了事件？(第 3.2.2、3.2.3 節)
3. 可能需要哪些額外工具來偵測此特定事件？(第 3.2.3 節)
4. 事件應變團隊將如何分析和驗證該事件？哪些人員將參與分析和驗證過程？(第 3.2.4 節)
5. 團隊將向組織內的哪些人員和團體通報該事件？(第 3.2.7 節)
6. 團隊將如何優先處理此事件？(第 3.2.6 節)

遏制、根除和恢復：

1. 組織應採取什麼策略來控制事件？為什麼這個策略比其他策略更可取？(第 3.3.1 節)
2. 如果事件得不到遏制，會發生什麼事？(第 3.3.1 節)
3. 可能需要哪些額外工具來應付這特定事件？(第 3.3.1、3.3.4 節)
4. 哪些人員將參與遏制、根除和/或復原過程？(第 3.3.1、3.3.4 節)
5. 組織應取得哪些證據來源(如果有)？證據如何取得？它會儲存在哪裡？應該保留多久？(第 3.2.5、3.3.2、3.4.3 節)

事件後活動：

1. 誰將參加有關此事件的經驗教訓會議？(第 3.4.1 節)
2. 今後可以採取哪些措施來防止類似事件發生？(第 3.1.2 節)
3. 可以採取哪些措施來改善類似事件的偵測？(第 3.1.2 節)

一般的問題：

1. 有多少事件應變團隊成員參與處理此事件？(第 2.4.3 節)
2. 除了事件應變團隊之外，組織內的哪些團隊將參與處理此事件？(第 2.4.4 節)
3. 團隊將向哪些外部方通報該事件？每份通報何時發生？每份通報如何製作？您會通報或不通報哪些訊息，為什麼？(第 2.3.2 節)
4. 還可能與外部各方進行哪些其他溝通？(第 2.3.2 節)5. 團隊將使用哪些工具和資源來處理此事件？(第 3.1.1 節)
5. 如果事件發生在不同的日期和時間(上班時間與下班時間)，處理的哪些面向會有所不同？(第 2.4.2 節)
6. 如果事件發生在不同的實體地點(現場與場外)，處理的哪些面向會有所不同？(第 2.4.2 節)

A.2 場景

場景 1：網域名稱系統 (DNS) 伺服器拒絕服務 (DoS)

週六下午，外部用戶在瀏覽該組織的公共網站時開始遇到問題。在接下來的一個小時裡，問題變得更加嚴重，幾乎每次瀏覽嘗試都失敗了。同時，該組織的網路工作人員回應來自 Internet 邊境路由器的警報，並確定該組織的 Internet 頻寬正被往返於該組織公共 DNS 伺服器的異常大量使用者資料封包協定(UDP)封包佔用。流量分析顯示 DNS 伺服器正在從單一外部 IP 位址接收大量請求，而且該位址的所有 DNS 請求都來自相同來源連接埠。

以下是針對此場景的其他問題：

1. 對於有問題的外部 IP 位址，組織應該聯絡誰？
2. 假設在採取初步遏制措施後，網路管理員偵測到九個內部主機也在嘗試向 DNS 伺服器發出相同的異常請求，這會對本次事件的處理產生怎樣的影響？
3. 假設要將九個內部主機中的兩個在識別其系統所有者之前與網路斷開連接，應該如何識別系統所有者？

場景 2：蠕蟲和分散式阻斷服務 (DDoS) 代理感染

週二早上，發布了一種新蠕蟲病毒；它透過可移動媒體傳播，並且可以將自身複製到開啟的 Windows 共用中。當蠕蟲感染主機時，它會安裝 DDoS 代理程式。這在蠕蟲病毒開始傳播幾個小時後，在防毒簽名可用之前，該組織已經遭受了廣泛的感染。

以下是針對此場景的其他問題：

1. 事件回應團隊如何辨識所有受感染的主機？
2. 在防毒簽章發布之前，組織將如何嘗試阻止蠕蟲進入組織？
3. 在防毒簽章發布之前，組織將如何嘗試阻止蠕蟲病毒被受感染的主機傳播？
4. 組織是否會嘗試修補所有易受攻擊的機器？如果是這樣，這將如何完成？
5. 如果已接收 DDoS 代理程式的受感染主機被配置為在第二天早上攻擊另一個組織的網站，則此事件的處理將如何變更？
6. 如果一台或多台受感染的主機包含有關組織員工的敏感個人識別訊息，對此事件的處理將如何變化？
7. 事件回應團隊如何讓組織的使用者了解事件的狀態？
8. 團隊將對目前未連接網路的主機(例如，正在度假的員工、偶爾連接的異地員工)執行哪些額外措施？

場景 3：文件被盜

週一早上，該組織的法律部門接到聯邦調查局 (FBI) 的電話，稱該組織的系統存在一些可疑活動。當天晚些時候，一名聯邦調查局特工與管理層和法律部門成員會面，討論該活動。

聯邦調查局一直在調查涉及公開發布敏感政府文件的活動，據報導其中一些文件屬於該組織。特工請求組織的協助，管理層請求事件回應團隊協助取得必要的證據，以確定這些文件是否合法以及它們是如何洩露的。

以下是針對此場景的其他問題：

1. 事件回應團隊可以從哪些來源收集證據？
2. 團隊將採取什麼措施保密調查？
3. 如果團隊確定了負責洩密的內部主機，事件的處理方式又會如何改變？

4. 如果團隊發現導致洩漏的內部主機上安裝了 Rootkit，則此事件的處理將如何改變？

場景 4：資料庫伺服器被駭

週二晚上，資料庫管理員在下班時間對多台生產資料庫伺服器執行一些維護。管理員注意到其中一台伺服器上有一些不熟悉且不尋常的目錄名稱。在檢查目錄列表並查看一些文件後，管理員得出結論，伺服器已受到攻擊，並致電事件回應團隊尋求協助，該團隊的調查確定攻擊者在六週前成功獲得了伺服器的最高存取權限。

以下是針對此場景的其他問題：

1. 團隊可以使用哪些來源來決定攻擊何時發生？
2. 如果團隊發現資料庫伺服器一直在運行封包探測器並從網路擷取密碼，對此事件的處理將如何改變？
3. 如果團隊發現伺服器正在執行一個程式，該程式會每晚複製包含敏感客戶資訊(包括個人識別資訊)的資料庫並將其傳輸到外部位址，那麼對此事件的處理將如何改變？
4. 如果團隊在伺服器上發現 Rootkit，此事件的處理方式會如何改變？

情境 5：未知滲漏

週日晚上，該組織的一個網路入侵偵測感測器針對涉及大檔案傳輸的異常出站網路活動發出警報。入侵分析師審查警報發現似乎有數千個 .RAR 檔案正在從內部主機複製到外部主機，而外部主機位於另一個國家。分析師聯繫事件回應團隊，以便其進一步調查該活動。團隊無法查看 .RAR 檔案的內容，因為它們的內容已加密，對包含 .RAR 檔案的內部主機的分析顯示了被安裝了機器人程式的跡象。

以下是針對此場景的其他問題：

1. 團隊如何確定 .RAR 檔案中最有可能的內容是什麼？哪些其他團隊可以協助事件回應團隊？
2. 如果事件回應團隊確定最初的攻擊是透過內部主機中的無線網路卡進行的，那麼該團隊將如何進一步調查此活動？
3. 如果事件回應團隊確定內部主機被用來暫存企業內其他主機的敏感文件，團隊將如何進一步調查此活動？

場景 6：未經授權存取員工薪資記錄

週三晚上，該組織的實體安全團隊接到員工薪資管理員的電話，她看到一名身份不明的人離開她的辦公室，跑過走廊，然後離開了大樓。管理員只讓她的工作站解鎖且無人看守幾分鐘。薪資程式仍然處於登入狀態並位於主選單上，就像她離開時一樣，但管理員注意到滑鼠似乎已被移動。事件應變團隊已被要求獲取與事件相關的證據並確定採取了哪些行動。

以下是針對此場景的其他問題：

1. 團隊如何確定已執行哪些操作？
2. 如果薪資管理人員承認離開辦公室的人是前薪資部門員工，那麼此事件的處理會有什麼不同？
3. 如果團隊有理由相信此人是現任員工，此事件的處理會有什麼不同？
4. 如果實體安全團隊確定此人使用了社交工程進入建築物，則事件的處理會有什麼不同？
5. 如果上週的日誌顯示使用薪資管理員的使用者 ID 進行遠端登入嘗試失敗的次數異常多，則此事件的處理會有什麼不同？
6. 如果事件應變團隊兩週前發現電腦上安裝了按鍵記錄器，則此事件的處理會有什麼不同？

場景 7：主機消失

週四下午，網路入侵偵測感測器記錄了由內部 IP 位址產生的針對內部主機的漏洞掃描活動。由於入

侵偵測分析師不知道有授權的、計劃的漏洞掃描活動，因此她將該活動通報給事件應變團隊。當團隊開始分析時，發現活動已停止，並且不再有主機使用該 IP 位址。

以下是針對此場景的其他問題：

1. 哪些資料來源可能包含漏洞掃描主機身分的資訊？
2. 團隊如何辨識誰在執行漏洞掃描？
3. 如果漏洞掃描針對組織最關鍵的主機，此事件的處理會有什麼不同？
4. 如果漏洞掃描針對外部主機，此事件的處理有何不同？
5. 如果內部 IP 位址與組織的無線訪客網路有關，此事件的處理會有什麼不同？
6. 如果實體安全人員在漏洞掃描發生前半小時發現有人闖入設施，則此事件的處理會有什麼不同？

場景 8：遠距辦公

週六晚上，網路入侵偵測軟體記錄了源自監視清單 IP 位址的連線。入侵偵測分析師確定正在與組織的 VPN 伺服器建立連接，並聯繫事件應變團隊。該團隊檢查入侵偵測、防火牆和 VPN 伺服器日誌，並識別針對連線進行驗證的使用者 ID 以及與該使用者 ID 關聯的使用者名稱。

以下是針對此場景的其他問題：

1. 團隊的下一步應該是什麼(例如，打電話給家裡的使用者、停用使用者 ID、斷開 VPN 會話)？為什麼要先執行這一步？第二步驟應該執行什麼步驟？
2. 若外部 IP 位址屬於開放代理，此事件的處理有何不同？
3. 如果在使用者不知情的情況下使用該 ID 從多個外部 IP 位址啟動 VPN 連接，則此事件的處理會有什麼不同？
4. 假設已識別使用者的電腦已被家庭成員下載的包含特洛伊木馬的遊戲破壞。這將如何影響團隊對事件的分析？這將如何影響證據收集和處理？為了從使用者電腦中消除該事件，團隊應該做什麼？
5. 假設使用者安裝了防毒軟體並確定特洛伊木馬包含鍵盤記錄器。這會對事件的處理產生怎樣的影響？如果使用者是系統管理員，這將如何影響事件的處理？如果使用者是組織中的高階管理人員，這將如何影響事件的處理？

場景 9：匿名威脅

週四下午，該組織的實體安全團隊接到 IT 經理的電話，通報她的兩名員工剛收到針對該組織系統的匿名威脅。根據調查，實體安全團隊認為應認真對待威脅，並將威脅通知相應的內部團隊，包括事件應變團隊。

以下是針對此場景的其他問題：

1. 事件回應團隊應該採取哪些不同的措施(如果有的話)來回應威脅通知？
2. 加強實體安全控制會對團隊的事件回應產生什麼影響？

場景 10：點對點檔案共享

組織禁止使用點對點文件共享服務，入侵偵測分析師注意到過去三個小時內發生了多個檔案共享警報，所有警報都涉及相同內部 IP 位址。

以下是針對此場景的其他問題：

1. 應根據哪些因素來優先處理此事件(例如，正在共享的文件的內容)？
2. 哪些隱私考量可能會影響此事件的處理？
3. 如果執行點對點文件共享的計算機還包含敏感的個人識別信息，此事件的處理會有什麼不同？

場景 11：未知無線存取點

週一早上，該組織的服務台接到同一棟大樓同一樓層的三名用戶的電話，他們表示無線網路遇到了問題。被要求協助解決問題的網路管理員將一台具有無線存取功能的筆記型電腦帶到使用者樓層，他查看無線網路配置時，他注意到有一個新的接入點列為可用。他與隊友檢查後確定該接入點不是他的團隊部署的，因此很可能是未經許可建立的惡意存取點。

以下是針對此場景的其他問題：

1. 處理此事件的第一個主要步驟應該是什麼(物理上找到惡意存取點，邏輯上連接到存取點)？
2. 定位存取點的最快方法是什麼？定位存取點最隱密的方法是什麼？
3. 如果存取點是由臨時在組織辦公室工作的外部方(例如承包商)部署的，則此事件的處理會有什麼不同？
4. 如果入侵偵測分析師通報涉及建築物同一樓層的某些工作站的可疑活動跡象，對此事件的處理會有什麼不同？
5. 如果在團隊在嘗試實體定位存取點時該存取點已被移除，則此事件的處理會有什麼不同？

附錄 B 事件相關資料元素

組織應規範事件收集的標準的相關資料元素。這項工作不僅有助於更有效和一致的事件處理，而且有助於組織完成合規的事件報告。組織應指定在通報事件時收集的基本元素以及事件處理者在應變期間收集的附加元素。這兩組元素將成為事件通報資料庫的基礎，先前已在第 3.2.5 節中討論過。下面的清單提供了針對事件收集哪些資訊的建議，除了這些元素之外，每個組織都應根據多個因素建立自己的元素列表，包括其事件回應團隊模型和結構以及「事件」一詞的定義。

B.1 基本資料元素

- 事件通報者和處理者的聯絡訊息
  - 姓名
  - 角色
  - 組織單位(例如機構、部門、部門、團隊)和隸屬關係–電子郵件地址
  - 電話號碼
  - 地點(例如郵寄地址、辦公室房間號碼)
- 事件詳情
  - 狀態變更日期/時間戳記(包括時區)：事件開始的時間、發現/偵測到事件的時間、通報事件的時間、事件解決/結束的時間等
  - 事件發生的實際位置(例如城市、州)
  - 事件的當前狀態(例如，正在進行的攻擊)
  - 事件的來源/原因(如果已知)，包括主機名稱和 IP 位址
  - 事件描述(例如，如何偵測到事件、發生了什麼)
  - 受影響資源(例如網路、主機、應用程式、資料)的描述，包括系統的主機名稱、IP 位址和功能
  - 事件類別、與事件相關的攻擊向量以及與事件相關的指標(流量模式、登錄項目等)
  - 優先考慮因素(功能影響、資訊影響、可恢復性等)
  - 緩解因素(例如，被盜的包含敏感資料的筆記型電腦使用全盤加密)
  - 執行的回應操作(例如，關閉主機、中斷主機與網路的連線)
  - 其他聯繫的組織(例如軟體供應商)
- 其他備註

B.2 事件處理程序資料元素

- 事件響應的當前狀態
- 事件概要
- 事件處理措施
  - 所有處理程序所採取操作的日誌
  - 所有相關方的聯絡資訊
  - 收集到的證據清單
- 事件處理程序評論
- 事件原因(例如應用程式設定錯誤、主機未打補丁)
- 事件成本
- 該事件的業務影響

常見問題解答

使用者、系統管理員、資訊安全人員和組織內的其他人員可能對事件回應有疑問。以下是常見問題(FAQ)，我們鼓勵組織自訂此常見問題解答並將其提供給其用戶社群。

1. 什麼是事件？

事件是指違反電腦安全策略、可接受的使用策略或標準電腦安全實務的行為。事件的例子有：

- 攻擊者命令殭屍網路向組織的其中一台 Web 伺服器發送大量連線請求，導致其當機。
- 用戶被誘騙打開透過電子郵件發送的"季度報告"，而該報告實際上是惡意軟體，執行該工具後感染了他們的電腦並與外部主機建立了連線。
- 駭客未經授權存取機敏數據，並威脅如果組織不支付指定金額就向媒體公佈詳細資訊。
- 使用者透過點對點文件共享服務向他人提供非法軟體。

2. 什麼是事件處理？

事件處理是偵測和分析事件並限制事件影響的過程。如果攻擊者透過網路侵入系統，事件處理過程應該會偵測到安全漏洞，然後事件處理人員將分析相關數據並確認攻擊的嚴重程度及決定事件優先處理順序，接著事件處理人員採取行動遏制事件，並盡快讓受影響的系統恢復正常運作。

3. 什麼是事件應變？

「事件處理」和「事件應變」在本文檔中是同義詞。

4. 什麼是事件應變團隊？

事件應變團隊(也稱為電腦安全事件應變團隊，CSIRT)，負責向組織提供事件的應變服務，該團隊接收所有可能發生的事件的資訊，展開調查，並採取行動以確保將事件造成的損失降至最低。

5. 事件應變團隊提供哪些服務？

事件應變團隊提供的服務在不同組織之間存在很大差異。平時除了執行事件應變處理之外，大多數團隊還承擔入侵偵測、系統監控和系統管理的責任，團隊也要負責公告有關新威脅的知識與防禦建議，以及教育使用者和 IT 員工了解他們在事件預防和處理中的角色。

6. 應該向誰通報事件？

組織應建立明確的聯絡點 (POC) 以用於內部事件通報。有一些組織將所有事件直接通報給事件應變團隊，也有組織使用現有的 IT Helpdesk 機制通報。組織應該了解有時候需要與外部各方(例如其他事件回應團隊)通報事件。在美國，根據法律要求，聯邦機構必須向美國電腦緊急準備小組 (US-CERT) 通報所有事件。鼓勵所有組織向其相應的電腦安全事件回應團隊 (CSIRT) 通報事件，如果組織沒有自己的 CSIRT 可以聯繫，它可以向其他組織通報事件，包括資訊共享和分析中心 (ISAC)。

7. 如何通報事件？

大多數組織都有多種通報事件的方法。由於通報人的技術能力、通報事件的緊急程度以及事件的敏感性的不同，應該規劃多種不同的通報方法。設立緊急電話號碼、提供電子郵件地址、透過網頁表格都可用於通報事件。若涉及敏感資訊，可以透過團隊發布的公鑰對內容進行加密後向團隊提供敏感資料。

8. 通報事件時應提供哪些資訊？

資訊越準確越好，事件通報盡可能包含以下數據：

- 使用者的姓名、使用者 ID 和聯絡資訊(例如電話號碼、電子郵件地址)
- 工作站的位置、型號、序號、主機名稱和 IP 位址
- 事件發生的日期和時間
- 逐步解釋所發生的情況，包括發現感染後對工作站進行的操作，以及惡意軟體或防毒軟體警報顯示的訊息。

9. 事件回應團隊對事件通報的反應速度有多快？

回應時間取決於多個因素，事件類型、受影響的資源和資料的重要性、事件的嚴重性、受影響資源的現有服務等級協定 (SLA)、時間和發生在星期幾、團隊是否正在處理的其他事件，這些都會影響事件應變速度。一般來說，最高優先事項是處理對組織或其他組織造成最大損害的事件。

10. 事件相關人員應何時聯繫執法單位？

與執法機構的溝通應由事件應變團隊成員、資訊長 (CIO) 或其他指定官員發起，使用者、系統管理員、系統擁有者和其他人都不應與執法單位聯繫。

11. 發現系統受到攻擊時該做什麼？

該人應立即停止使用該系統並聯繫事件應變團隊，人員立即協助事件的初步處理，例如，對設備進行監控不讓其他人碰觸，直到事件處理人員到達以保護系統及物理的證據。

12. 媒體就某事件聯絡某人時該做什麼？

個人可以根據組織有關事件和外部各方的政策回答媒體的問題，但是如果該人沒有資格代表該組織討論該事件，則該人不應就該事件發表評論，應該將來電轉介給該組織的公共事務辦公室，讓公共事務辦公室向媒體和公眾提供準確一致的資訊。

危機處理步驟

這是當技術專業人員認為發生了嚴重事件而組織沒有可用的事件應變能力時應執行的主要步驟清單。對於面臨危機但沒有時間閱讀整份文件的人來說，這可以作為該做什麼的基本參考。

1. **記錄一切。**這項工作包括所執行的每項操作、每項證據以及與使用者、系統擁有者和其他人就該事件進行的每一項活動。
2. **尋找可以提供幫助的同事。**如果兩個或更多人一起工作，處理事件會容易得多。讓一個人執行操作，而另一個人可以記錄這些操作。
3. **分析證據以確認事件已經發生。**根據需要進行深入的研究(例如網路搜尋引擎、軟體文件)，或向組織內的其他技術專業人員尋求更多協助，以更精確地理解證據。
4. **通知組織內的適當人員。**包括資訊長 (CIO)、資訊安全主管和本地安全經理。與他人討論事件細節時要謹慎，僅告訴需要了解和使用安全的通訊機制的人(如果攻擊者破壞了電子郵件服務，請勿發送有關該事件的電子郵件)。
2. **通知 US-CERT 和/或其他外部組織尋求協助處理該事件。**
3. **如果事件仍持續影響，請立即停止該事件。**最常見的方法是斷開受影響的系統與網路的連接。在某些情況下，這可能需要修改防火牆和路由器設定以阻止事件攻擊。
4. **保存事件證據。**對受影響的系統進行備份(最好是磁碟映像備份，而不是檔案系統備份)。製作包含與事件相關的證據的日誌檔案的副本。
5. **消除事件造成的影響。**這項工作包括被惡意軟體感染的主機、不適當的材料(例如盜版軟體)、特洛伊木馬檔案以及事件對系統所做的任何其他更改。如果系統已完全受到損害，請從頭開始重建它或從已知良好的備份中還原。
6. **識別並緩解所有被利用的漏洞。**該事件可能是利用作業系統或應用程式中的漏洞，識別此類漏洞並消除或以其他方式緩解它們，讓事件不會再次發生。
7. **確認系統已恢復正常。**確保受事件影響的資料、應用程式和其他服務已恢復正常運作。
8. **建立最終報告。**該報告應詳細說明事件處理過程、執行的摘要，說明所發生的情況以及正式的事件應變能力如何幫助處理這種情況、如何減輕風險並快速地限制損害。