**資訊安全事件應變：6個步驟以及實現這些步驟的團隊和工具**

**了解事件回應計劃如何在事件造成重大損害前對其進行檢測和應變。**

## ****什麼是事件應變？****

事件應變是處理安全漏洞的一種方法，其目的是確定事件的範圍、控制損害並減輕或消除事件的根本原因。事件代表安全狀態的改變，可能源自於違反法律、政策或涉及資訊資產（例如網路、電腦或智慧型手機）異動的不可接受的行為，這些行為可能會導致需要向外發布重大報告。

隨著資料外洩頻率和類型增加，缺乏事件應變計畫可能會導致組織營運成本增加，並進一步損害資訊安全有效性，因此事件應變是所有重視資訊安全組織的關鍵活動。

**本文包含六章節：**

* [為什麼事件應變很重要](#_為什麼事件應變很重要？)
* [安全事件的類型](#_外部來源安全事件的類型)
* [事件應變的六個步驟](#_事件回應的六個步驟)
* [資安事件應變小組](#_誰負責事件響應？) (CSIRT，Cyber-Security Incident Response Team)
* [事件應變工具和技術](#_事件回應工具和技術)
* [成功事件應變的 5 個秘訣](#_成功回應事件的_5_個秘訣)

### ****為什麼事件應變很重要？****

當您的組織能夠快速應變事件時，可以減少損失、盡快復原工作流程和服務、縮小影響範圍，並減少可被利用的漏洞。未有效遏制的事件可能會導致資料洩露，並造成災難性後果。事件應變提供了針對安全事件的第一道防線，長遠來看，其有助於建立一套機制來防止損害發生。

如果您未能及時解決事件，它可能會提升為更嚴重的問題，造成重大損害，例如資料遺失、系統崩潰和昂貴的補救措施，甚至根據事件類型和所涉及的行業而受到外部經濟處罰。有效的事件應變可以阻止攻擊，並降低未來事件的風險。

事件應變對於維持業務連續性和保護敏感資料至關重要。可靠的事件應變計畫幫助組織為已知和未知的風險做好準備，可靠的事件應變程序將使您能夠在安全事件發生時立即識別它們，並實施最佳方法來阻止進一步的入侵。

應變策略應該預先設想包含廣泛的事件類型，即使是最簡單的事件也可能會長期影響您組織的業務運作和聲譽，解決這些問題，除了技術負擔和資料恢復成本之外，另一個風險是遭受法律和經濟處罰，讓您的組織蒙受營收損失 (可能達數百萬美元)。

### ****安全事件的類型****

以下是由惡意外部威脅行為者引起的幾種重大安全事件類型:

#### **網路釣魚與社會工程 (Phishing and Social Engineering)**

網路釣魚和社交工程是最常見的安全事件來源，這類攻擊通常是透過操縱個人洩露機密資訊，例如密碼或信用卡號。社交工程利用心理操縱來誘騙人們犯下違反資訊安全的錯誤或洩漏敏感資訊，例如聲稱來自可信來源的電子郵件、電話，甚至透過 AI偽造影像或聲音冒充當事人。

#### **DDoS 攻擊**

分散式阻斷服務 (DDoS) 攻擊是一種透過大量流量淹沒網路、系統或伺服器服務，造成使用者無法存取。這些攻擊可能會大量停機，對依賴網站或系統進行日常活動的組織造成嚴重損害，並可能導致營收損失和失去客戶信任，甚至在醫療業或製造業會造成人身傷害，例如: 醫療系統被攻擊，個人醫療紀錄被竄改、製造業 PLC 被控制導致機器失控。

由於DDoS 攻擊是由殭屍網路發起的，因此特別難以防禦。殭屍網路可能有數千或數百萬台受感染的電腦同時攻擊目標。此外這種類型的攻擊通常被用作其他惡意活動的煙幕彈，在發起其他攻擊或特洛伊木馬的同時分散安全團隊的注意力。

#### **供應鏈攻擊**

當可以透過網路連線存取您的系統和資料的外部合作夥伴或供應商滲透您的系統時，就會發生軟體供應鏈攻擊，也稱為價值鍊 (value-chain)或第三方攻擊 (third-party attack)。這種類型的網路攻擊特別具有破壞性，因為它可以繞過傳統的安全措施，並使攻擊者深入存取敏感資料或智慧財產權。

因為它們利用了公司與其供應商之間的信任關係，所以這類攻擊很難預測或預防，它強調了審查和監控第三方提供者是否存在潛在安全風險的重要性，需仔細決定哪些服務帳號有權存取內部網路以及為何他們被授權執行操作。

#### **勒索軟體**

勒索軟體是一種加密受害者檔案的惡意軟體，攻擊者向受害者勒索贖金，以便在付款後恢復對資料的存取，若是關鍵系統或資料受到影響，勒索軟體攻擊可能會導致重大業務中斷和財務損失。

這些攻擊可以透過各種媒介（尤其是社交工程）來傳播，包括電子郵件附件、軟體漏洞或受感染的網站。事件應變計畫對於處理勒索軟體事件並最大程度地減少影響至關重要，甚至還要包括與最高層討論您的組織是否準備為取得密鑰支付贖金，或者這樣做是否合法。

是否支付贖金的這種灰色地帶的例子是 2020 年的一項裁決: 美國財政部外國資產管制辦公室和金融犯罪執法網絡宣佈在某些（大多數）案件中支付贖金是非法的。某些情況下，支付贖金並沒有被交付解密金鑰，甚至出現像 NotPetya 這樣的惡意軟體，對受害者進行勒索並同時破壞資料。

#### **內部威脅**

內部威脅是源自組織內部的安全威脅，可能來自粗心和心懷不滿的員工、承包商或任何被授予內部存取公司網路和資料權限的人。

這些威脅的管理和檢測尤其具有挑戰性，因為這些人通常已經擁有對公司係統的合法存取權，此類事件可能會導致重大損害，包括智慧財產權被盜取、財務詐欺和公司聲譽受損。

### ****事件應變的六個步驟****

#### **1. 準備工作 (Preparation)**

以下是您的事件回應團隊應採取網路安全事件的步驟：

* 組成內部事件應變團隊並制定遭遇網路攻擊時實施的政策，檢查防禦各種事件類型所需的資源並集中管理所需的工具。
* 審查安全策略並針對外部攻擊、內部誤用/內部攻擊以及外部報告潛在漏洞和利用的情況進行風險評估。
* 優先考慮無法立即修復的已知安全問題或漏洞，掌握最有價值的資產，以便能夠專注於針對關鍵基礎設施處理關鍵安全事件。
* 制定內部和外部（如有必要）公開違規報告的溝通計畫。美國證券交易委員會最近要求上市公司在確定網路攻擊屬於重大事件後的四個工作天內揭露資訊。台灣金管會證期局表示，證交所及櫃買中心已修訂相關法規，要求上市櫃公司，於發生重大資安事件時，應即時發布重大訊息，最晚要在次一營業日開盤前2小時重訊公告，台股是上午9時開盤，就應該要在7時前公告。若有違反，依照證交所的規定，可處以違約金3萬到500萬元。
* 概述即時事件應變團隊的角色、職責和程序，擴大組織的資安危機意識。
* 招募和培訓團隊成員，並確保他們能夠使用相關系統、技術和工具。
* 對內部員工和外包人員(包括合作夥伴和供應鏈主要及次要供應商)進行教育訓練，讓他們了解如何通報潛在的安全事件或資訊，並且納入外包需求和服務協議的一部分。

#### **2. 鑑定 (Identification)**

確定事件應變團隊採取行動的標準程序，並為事件焦點建立分類或資訊收集的文件（如果所有安全事件都回報安全營運團隊，則團隊需要知道如何提出正確的問題來執行基本分類）。

IT 系統從監控工具、日誌檔案、錯誤訊息、防火牆和入侵偵測系統收集事件資訊，這些資料應由自動化工具和資訊安全分析師進行分析，以確定異常事件是否資訊安全事件。例如，僅僅看到有人對網頁伺服器進行攻擊並不能保證組織已受到損害，資訊安全分析師應該尋找多種因素、行為變化、進出站流量以確認事件類型。

當安全事件已被確認並隔離時，應向資安事件應變團隊發出警報，由團隊成員協調並對事件做出適當的應變：

* 識別和評估事件並收集相關證據。
* 確定事件的嚴重性和類型，並在必要時提升資安等級。
* 用5W1H方式(Who、When、Where、When、Why、How) 記錄所採取的行動，如果事件涉及法律告訴，保全相關紀錄將可在後續法律攻防作為證據。

系統日誌、電子郵件、電話通聯記錄和涉及的人員，都會成為調查記錄的一部分。確保事件應變團隊和安全分析師了解記錄整個過程中涉及的每個人的姓名、日期、時間和通訊的重要性！

#### **3. 遏制（Containment）**

一旦團隊隔離了安全事件，接下來目標就是阻止進一步的損害，包括：

* **短期遏制**：採取即時應變讓威脅不會造成進一步損害，這包括關閉已被駭客攻擊的生產伺服器或隔離受到攻擊的網段。
* **系統備份**：在刪除和重建映像檔以恢復「正常狀態」之前，您應該備份所有受影響的系統以保留硬碟或特定磁碟分割區的副本作為留存證據。證據映像檔是在事件發生後建立的，用於保持特定時間點的磁碟狀態，從而提供靜態“快照”。您可以將其做為安全事件的證據，並用以調查系統如何受到攻擊與受到的損害。
* **長期遏制**：重建乾淨的系統恢復上線，並採取防止事件再次發生的措施，例如，在受影響及相關系統上安裝安全更新、刪除攻擊者創建的帳戶和後門、更改防火牆規則，並將被攻擊者利用的路由更改為空路由等。
* **建立文件**：為詳細了解事件涉及哪些憑證、服務帳戶、端點、伺服器，建立一個文件庫，儲存磁碟映像檔、影響清單和事件說明報告對於調查和證據非常重要。

#### **4. 根除（Eradication）**

此步驟主要是遏制威脅並將系統恢復到初始狀態或接近初始狀態。資訊安全應變團隊應隔離事件攻擊的根本原因、消除威脅和惡意軟體、識別及緩解以阻止未來被利用作為攻擊的漏洞。這些步驟可能會改變組織的環境配置，其目的是進行變革，同時盡量減少對組織運作的影響。您可以透過止血和限制暴露的資料量來實現：

* 識別並修復所有受影響的主機 (包括組織內部和外部的主機)
* 隔離攻擊根源以刪除該軟體的所有實例 (Instance)
* 進行惡意軟體分析以確定損壞的程度
* 查看攻擊者是否對您的操作做出反應，追朔最後上版後系統是否建立了任何新憑證或提權
* 確保沒有發生持續性感染，如果有，立刻將其清除
* 留出時間確保網路安全並確認攻擊者沒有進一步的活動

確保您的團隊徹底刪除惡意內容並檢查受影響的系統已經恢復乾淨。如果攻擊者使用了漏洞，則應對其進行修補，或者如果攻擊者利用弱身份驗證機制，則應將其替換為強身份驗證。這可能需要與架構、營運和工程團隊密切合作，因此請確保將他們包含在您的溝通計劃中。

#### **5. 恢復 (Recovery)**

此階段的目的是小心地將受影響的系統帶回生產環境，以確保它們不會導致另一個事件。始終保持從乾淨的備份中恢復系統，用乾淨的版本替換受損的文件或 Docker 容器。重建系統、安裝修補程式、變更密碼，以及加強網絡外圍安全（例如，邊界路由器ACL、防火牆規則等）

確定需要監控受影響的網路和端點系統多長時間，以及如何驗證受影響的系統是否正常運作。計算相關的生產力損失、故障排除所需的人力時間以及採取措施進行完全恢復所耗費的成本。

#### **6. 經驗教訓 (Lesson Learned)**

發生任何事件後，重要的是召開事件報告或總結經驗教訓會議，以記錄發生的情況、事件處理的過程，並評估改進的可能性，事件應變團隊和利害關係人應進行溝通以改善未來的流程。

經驗教訓報告提供了整個事件的清晰回顧，可以在會議中使用，作為比較基準或作為新人員的培訓資訊。

### ****資安事件應變小組****

為了準備和處理事件，您應該組建一個集中的事件回應團隊，負責識別安全漏洞並採取回應措施。在大型組織中，這是一個專門的團隊，稱為電腦安全事件應變小組（CSIRT）。CSIRT 成員為全職安全人員，包括任何專門的內部威脅團隊，這些人分析有關事件的資訊並做出回應。

在較小的組織中，事件應變團隊可以由接受過一些安全訓練的 IT 人員組成，並由內部或外包安全專家協助應變。

事件應變團隊也要與組織內的利害關係人進行溝通，並參與媒體、法律顧問、受影響的客戶和執法部門等外部團體的初步書面溝通。團隊成員應包括：

* **事件回應主管（團隊負責人）**，協調所有團隊行動並確保團隊專注於最大程度地減少損失並快速恢復。確定事件隔離、分析和遏制期間行動的優先順序，在事件應變期間監督所有行動並指導團隊。
* **資訊安全分析主管**，由跨部門工作的安全分析師團隊協助，以隔離和糾正組織安全系統、解決方案和應用程式中的缺陷，以提出改善整體安全狀況的具體措施。
* **首席研究員**，隔離根本原因，分析所有證據，管理其他安全分析師，並進行快速系統和服務復原。
* **威脅研究員**，提供事件背景和威脅情報，利用這些資訊和先前事件的記錄來創建內部情報資料庫。在許多安全團隊中，威脅研究人員逐漸被自動化威脅情報工具取代。
* **溝通主管**，與公司內外的所有群眾進行溝通，包括管理階層、內部利害關係人、高階主管和/或董事會成員、法務人員、媒體和客戶。
* **文件和事件時間軸紀錄人員**，記錄團隊的調查、發現和恢復工作，並且為事件的每一個階段建立時間表 (新一代安全資訊和事件管理 (SIEM)系統能夠自動產生文件和事件時間表)。
* **人力資源/法律代表**，當事件最終涉及刑事指控（這也是保持乾淨的證據鍊和調查記錄的原因），您應該獲得人力資源和法律指導。

### ****事件應變工具和技術****

#### **SIEM**

安全資訊和事件管理 (SIEM) 解決方案收集並整合組織 IT 環境中的應用程式、伺服器和網路設備產生的日誌資料，然後對這些數據進行分析和關聯，以識別可能暗示安全事件的徵兆。SIEM 工具不僅有助於偵測潛在威脅，還可以透過提供可操作的情報來幫助進行事件應變。它們根據預先定義的規則和嚴重性等級產生警報，使安全團隊能夠更有效地確定事件的優先順序並回應事件，此外，SIEM 解決方案透過提供安全措施的證據來產生合規性報告。

#### **安全性協調流程、自動化和回應 (SOAR)**

安全性協調流程、自動化和回應 (SOAR) 是一組安全解決方案，可讓組織從多個來源收集有關安全威脅的數據，並在無需人工協助的情況下回應安全事件。SOAR 工具可以自動執行常見的回應操作，從而減少安全團隊需要執行的手動任務的數量。他們還可以簡化事件回應工作流程，使團隊更輕鬆地追蹤、管理和解決事件，此外，SOAR 工具可與各種安全工具整合，為管理事件回應提供一個集中式的平台。

#### **EDR 和 XDR**

端點偵測和回應（EDR）和擴展偵測和回應（XDR）是提供全面威脅偵測和回應能力的安全技術。EDR 專注於筆記型電腦、桌上型電腦和行動裝置等端點，監控它們是否有安全事件的跡象。XDR 擴大了覆蓋範圍，包括網路流量、雲端環境和其他潛在的攻擊媒介。EDR 和 XDR 都可以在事件回應中發揮關鍵作用，提供快速有效地偵測、調查和回應進階威脅所需的可見性和控制。

#### **使用者和實體行為分析 (UEBA)**

使用者和實體行為分析 (UEBA) 分析使用者、端點和系統的正常行為，並用它來偵測偏離「規範」的異常行為。這些工具使用機器學習、演算法和統計分析來檢測 IT 環境中使用者、機器和網路的行為中有意義的異常。

在事件應變中，UEBA 工具可以協助安全團隊識別可能顯示安全事件的異常或可疑行為。例如，如果使用者突然開始存取他們通常不與之互動的敏感數據，這可能是內部威脅或帳戶受損的跡象。透過偵測此類異常，UEBA 工具可以幫助團隊在事件造成重大損害之前對其做出回應。

#### **入侵防禦系統 (IPS) 和入侵偵測系統 (IDS)**

入侵防禦系統 (IPS)入侵偵測系統 (IDS) 是偵測和預防安全事件的工具。IDS 監視網路流量是否有潛在事件的跡象，例如惡意負載或可疑行為。如果偵測到事件，IDS 可向安全團隊發送警報。IPS 更進一步積極預防事件，當 IPS 偵測到嘗試的安全漏洞，它可以採取措施阻止攻擊，例如，關閉網路連線或變更防火牆規則。

### ****成功事件應變的 5 個秘訣****

#### **1. 隔離異常**

僅靠技術無法成功偵測安全漏洞，還需要依靠人類的洞察力。以下是日常需要注意的一些情況：

* **流量異常**，內部使用的敏感連線和伺服器通常具有穩定的流量，如果您發現受監控的流量突然增加或減少，請立即確認。
* **未經許可存取帳戶**，特權或管理員帳戶比普通員工可以存取更多資訊和系統。然而，員工往往是網路犯罪最容易的切入點。密切監視特權帳戶並觀察普通使用者帳戶的提權活動。權限提升是一種常見的惡意軟體特徵，應透過規則或異常快速識別。
* **過度使用資源和可疑文件**，如果您發現公司記憶體或硬碟的效能有所提高，則可能是有人非法存取它們或洩漏資料。

透過現代化安全工具，例如，使用者和實體行為分析 (UEBA) 自動化這些流程，並自動識別使用者行為或文件存取中的異常情況。這可以更完整地覆蓋可能的安全事件，並為安全團隊節省時間。

#### **2. 使用集中式方法**

從安全工具和 IT 系統收集信息，並將其保存在集中的位置，例如 SIEM。使用這些資訊建立事件時間表，並在一個集中的地方使用所有相關數據對事件進行調查。

您也可以使用集中式方法來實現快速自動回應，使用來自安全工具的數據，應用高級分析，並使用諸如防火牆和電子郵件伺服器之類的技術在系統上協調自動回應 (SOAR)。

#### **3.依照事實斷定事件，不要做假設**

不要基於事件或事件存在的假設來進行調查，而是根據您可以評估和驗證的問題做出事實斷定。根據您管理系統、開法軟體、網路配置、建置系統等的經驗，從攻擊者的角度想像系統和流程，創建您的事件推論主張。

#### **4. 消除不可能的事件**

您可能並不確切知道在尋找什麼，在這些情況下，消除可以用邏輯解釋的事件。然後你將面臨沒有明確解釋的事件。這些通常出現在事件剛開始分類時，此時人們會通報影響狀況但不知道是什麼原因造成的。例如：

* 程式碼中不一致或冗餘的邏輯
* 發現可存取管理者功能或高權登入漏洞的問題
* 流量發生無法解釋的變化（例如急劇增加或下降）
* 網站內容、版面或設計發生無法解釋的變化
* 影響網站或資源可用性的效能問題

#### **5. 採取事後措施**

繼續監視您的系統是否有任何異常行為，以確保入侵者沒有回來。

https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/