AWS 安全事件應變 使用者指南

版本 December 1, 2024

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 安全事件應變 使用者指南:

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS 安全事件應變？ 1
支援的組態 1
功能摘要 2
監控和調查 2
簡化事件回應 2
自助式安全解決方案 3
儀表板提供可見性 3
安全狀態 3
快速協助 3
準備和準備 3
概念和術語 4
開始使用 6
選取成員資格帳戶 6
設定成員資格詳細資訊 7
將帳戶與 建立關聯 AWS Organizations 8
設定主動回應和提醒分類工作流程 8
使用者任務 9
儀表板 9
管理我的事件回應團隊 9
帳戶與 的關聯 AWS Organizations 10
監控和調查 2
準備 11
偵測和分析 11
包含 13
根除 15
復原 15
事件後報告 15
案例 17
建立 AWS 支援的案例 17
建立自我管理的案例 18
回應 AWS 產生的案例 20
管理案例 20
變更案例狀態 20
變更解析程式 21
Action Items (動作項目) 21

編輯案例 22
通訊 22
許可 22
附件 23
標籤 23
案例活動 24
關閉案例 24
使用 AWS CloudFormation 堆疊集 24
取消成員資格 31
標記 AWS 安全事件應變 資源 33
使用 AWS CloudShell 34
取得 的 IAM 許可 AWS CloudShell 34
使用 與安全事件回應互動 AWS CloudShell 35
CloudTrail 日誌 36
CloudTrail 中的安全事件回應資訊 36
了解安全事件回應日誌檔案項目 37
透過 AWS Organizations管理帳戶 40
考量事項和建議 40
受信任的存取權 41
指定委派安全事件回應管理員帳戶所需的許可 42
指定委派管理員 AWS 安全事件應變 43
將成員新增至 AWS 安全事件應變 45
從 移除成員 AWS 安全事件應變 45
..... 46
使用 EventBridge 管理事件 46
傳送安全事件回應事件 47
事件詳細參照 48
案例事件 49
案例評論事件 53
成員事件 56
使用 AWS 安全事件應變 事件 58
教學課程：傳送`Membership Updated`事件的 Amazon Simple Notification Service 提醒 59
先決條件 59
教學課程：建立和訂閱 Amazon SNS 主題 59
教學課程：註冊事件規則 60
教學課程：測試您的規則 62
替代規則：安全事件回應案例更新 62

疑難排解 ... 63
問題 ... 63
錯誤 ... 63
支援 ... 64
安全 ... 65
中的資料保護 AWS 安全事件應變 ... 65
資料加密 ... 66
網際網路流量隱私權 ... 66
服務和內部部署用戶端與應用程式之間的流量。 ... 66
相同區域中 AWS 資源間的流量 ... 67
身分和存取權管理 ... 67
使用身分驗證 ... 68
如何使用 AWS 安全事件應變 IAM ... 70
對 AWS 安全事件應變 身分和存取進行故障診斷 ... 77
使用服務角色 ... 78
使用服務連結角色 ... 78
AWSServiceRoleForSecurityIncidentResponse ... 79
AWSServiceRoleForSecurityIncidentResponse_Triage ... 80
SLRs支援的區域 ... 81
AWS 受管政策 ... 81
受管政策：AWSSecurityIncidentResponseServiceRolePolicy ... 82
受管政策：AWSSecurityIncidentResponseAdmin ... 83
受管政策：AWSSecurityIncidentResponseReadOnlyAccess ... 83
受管政策：AWSSecurityIncidentResponseCaseFullAccess ... 84
受管政策：AWSSecurityIncidentResponseTriageServiceRolePolicy ... 84
SLRs和 受管政策的更新 ... 85
事件回應 ... 87
法規遵循驗證 ... 87
在 AWS 安全事件回應中記錄和監控 ... 88
恢復能力 ... 88
基礎架構安全 ... 89
組態與漏洞分析 ... 89
預防跨服務混淆代理人 ... 89
Service Quotas ... 91
AWS 安全事件應變 ... 91
AWS 安全事件應變 技術指南 ... 93
摘要 ... 93

您是 Well-Architected 嗎？ 93
簡介 94
開始之前 94
AWS 事件回應概觀 95
準備 99
人員 100
流程 103
技術 108
準備項目摘要 113
作業 116
偵測 117
分析 120
遏制 123
根除 127
復原 129
結論 130
事後處理 131
建立從事件中學習的架構 131
建立成功的指標 132
使用入侵指標 135
持續教育和訓練 135
結論 136
貢獻者 136
附錄 A：雲端功能定義 136
記錄和事件 137
可見性和提醒 138
自動化 139
安全儲存 140
未來和自訂安全功能 140
附錄 B： AWS 事件回應資源 141
Playbook 資源 141
鑑識資源 141
注意 141
文件歷史紀錄 142
..... cxlvii

什麼是 AWS 安全事件應變？

AWS 安全事件應變 可協助您快速準備、回應和接收指引，以協助從安全事件中復原。這包括帳戶接管、資料外洩和勒索軟體攻擊等事件。

AWS 安全事件應變 會分類問題清單、呈報安全事件，以及管理需要您立即注意的案例。此外，您還可以存取 AWS 客戶事件回應團隊 (CIRT)，他們將調查受影響的資源。

> **Note**
>
> 無法保證可以復原受影響的資源。我們建議您建立和維護可能影響業務需求的資源備份。

AWS 安全事件應變 可與其他AWS 偵測和回應服務搭配使用，引導您完成從偵測到復原的整個事件生命週期。

目錄

- 支援的組態
- 功能摘要

支援的組態

AWS 安全事件應變 支援下列語言和區域組態：

- Language： AWS 安全事件應變 提供專用英文支援。日文支援僅限於日本標準時間上班時間，並附帶特定限制：
-
  > **Note**
  >
  > 日文語言支援會在上班時間（週一至週五上午 09：00-17：00，假日除外）盡力提供
- 支援 AWS 的區域：

  AWS 安全事件應變 可在 的子集中使用 AWS 區域。在這些支援的區域中，您可以建立成員資格、建立和檢視案例，以及存取儀表板。

  - 美國東部 (俄亥俄)
  - 美國西部 (奧勒岡)
  - 美國東部 (維吉尼亞)

- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (巴黎)
- 歐洲 (斯德哥爾摩)
- 亞太區域 (孟買)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太區域 (雪梨)
- 亞太區域 (東京)
- 加拿大 (中部)
- 南美洲 (聖保羅)

當您啟用監控和調查功能時， 會 AWS 安全事件應變 監控所有作用中廣告的 Amazon GuardDuty 調查結果 AWS 區域。作為安全最佳實務， AWS 建議在所有支援的區域中啟用 GuardDuty AWS 。此組態可讓 GuardDuty 產生有關未經授權或異常活動的調查結果，即使您 AWS 區域 未主動部署資源也一樣。透過這樣做，您可以增強整體安全狀態，並在整個 AWS 環境中維持全面的威脅偵測涵蓋範圍。

> **Note**
>
> Amazon GuardDuty 會報告已設定區域的調查結果。如果您選擇不在特定區域中啟用服務，則警示將無法使用。

功能摘要

監控和調查

AWS 安全事件應變 快速審查來自 Amazon GuardDuty 和與第三方整合的安全提醒 AWS Security Hub，減少您的團隊需要分析的數量。它根據您的環境設定抑制規則，以減少分類和調查所需的低優先順序提醒。

簡化事件回應

使用相關的利益相關者、第三方服務和工具，在幾分鐘內擴展和執行事件回應。

自助式安全解決方案

AWS 安全事件應變 提供 APIs來整合，並可讓您建置自己的自訂安全解決方案。

儀表板提供可見性

監控和測量事件回應準備程度。

安全狀態

存取 AWS 安全性評估和快速事件回應調查的最佳實務和經過審核的工具。

快速協助

聯絡 AWS 客戶事件回應團隊 (CIRT) 以調查、遏制和接收如何從安全事件復原的指引。

準備和準備

透過設定您的事件回應團隊，以使用預先定義的許可政策觸發指定個人或群組的警示，來實作簡化的通知。

概念和術語

下列術語和概念對於了解 AWS 安全事件應變 服務及其運作方式非常重要。

範圍： AWS 安全事件應變 符合國家標準與技術研究所 (NIST) 800-61 電腦安全事件處理指南，提供與產業最佳實務相關的安全事件管理一致方法。

分析：詳細調查和檢查安全事件，以了解其範圍、影響和根本原因。

AWS 安全事件應變 服務入口網站：自助入口網站，可讓您啟動和管理安全事件案例。透過票證系統、自動通知以及直接與服務團隊互動，促進持續的通訊和報告。

通訊： AWS 安全事件回應團隊與客戶在事件回應程序期間持續的對話方塊和資訊共享。

遏制、消除和復原：防止其他未經授權的活動 （遏制），以及移除未經授權的資源和原始漏洞 （消除），並復原資源以如常恢復業務。

持續改進： AWS 安全事件應變 整合從先前參與中學到的意見回饋和經驗，以增強其偵測功能、調查程序和修補動作。 AWS 安全事件應變 也隨時 up-to-date 掌握最新的安全威脅和最佳實務，以因應不斷變化的安全挑戰。

網路安全事件：使用資訊系統或網路來對其包含的系統、網路或資訊產生負面影響的動作。

網路安全事件：違反或即將發生的違反電腦安全政策、可接受的使用政策或標準安全實務的威脅。

事件回應團隊：一組在作用中安全事件期間提供支援的個人。對於 AWS 支援的案例，這是 AWS 客戶事件回應團隊 (CIRT)。

事件回應工作流程：安全事件end-to-end管理中涉及的步驟和活動定義序列，符合 NIST 800-61 標準。

調查工具：用於檢閱帳戶和資源運作狀態 AWS 安全事件應變 的工具和服務連結角色。

經驗教訓：審查和記錄安全事件回應，以識別需要改進的領域，並通知未來的事件回應規劃。

監控和調查： AWS 安全事件應變 快速檢閱來自 Amazon GuardDuty 的安全提醒，將團隊需要分析的最重要提醒帶到最前線。它會根據您環境的特定細節來設定禁止規則，以防止不必要的提醒。

準備：為讓組織準備好有效回應和管理安全事件而進行的活動，例如開發事件回應計劃和測試程序。

報告和通訊：用於在整個事件回應程序中通知您的程序，包括自動通知、呼叫橋接和調查成品的交付。 AWS 安全事件應變 在 中提供單一的集中式儀表板 AWS Management Console ，以管理您的所有 AWS 安全事件應變 工作。

回應者產生的智慧：入侵指標；策略、技術和程序；以及 AWS CIRT 調查觀察到的相關模式。

安全事件專業知識：有效回應和管理安全事件所需的專業知識和技能，特別是在雲端環境中 AWS 。

共同責任模型： AWS 和 客戶之間的安全責任劃分， AWS 負責雲端的安全，而客戶負責雲端的安全。

威脅情報：包含未經授權活動詳細資訊的內部和外部資料饋送，以協助識別和回應不斷變化的安全威脅。

票務系統：專用案例管理平台，可讓您加入和管理安全事件案例、新增附件，以及追蹤事件回應生命週期。

分類：安全事件的初始評估和優先順序，以確定適當的回應和後續步驟。

工作流程：在安全事件的end-to-end管理中涉及的步驟和活動定義序列。

開始使用

目錄

- 選取成員資格帳戶
- 設定成員資格詳細資訊
- 將帳戶與 建立關聯 AWS Organizations
- 設定主動回應和提醒分類工作流程

選取成員資格帳戶

成員帳戶是用來設定帳戶詳細資訊、新增和移除事件回應團隊詳細資訊，以及建立和管理所有作用中和歷史安全事件 AWS 的帳戶。建議您將 AWS 安全事件應變 成員資格帳戶與為 Amazon GuardDuty 和等服務啟用的相同帳戶對齊 AWS Security Hub。

您有兩個選項可以使用 選取您的 AWS 安全事件回應成員帳戶 AWS Organizations。您可以在 Organizations 管理帳戶或 Organizations 委派管理員帳戶中建立成員資格。

使用委派管理員帳戶：AWS 安全性事件回應管理任務和案例管理位於委派管理員帳戶中。我們建議您使用為其他 AWS 安全與合規服務設定的相同委派管理員。提供 12 位數委派管理員帳戶 ID，然後登入該帳戶以繼續。

> **Important**
>
> 當您使用委派管理員帳戶做為設定的一部分時， AWS 安全事件應變 無法在您的 AWS Organizations 管理帳戶中自動建立所需的分類服務連結角色。
> 您可以使用 IAM 在 AWS Organizations 管理帳戶中建立此角色
>
> 建立服務連結角色 (主控台)
>
> 1. 登入您的 AWS Organizations 管理帳戶。
> 2. 在您偏好的方法中，透過 CLI 存取 AWS CloudShell 視窗或存取帳戶。
> 3. 使用 CLI 命令 `aws iam create-service-linked-role --aws-service-name triage.security-ir.amazonaws.com`
> 4. （選用）若要驗證命令是否正常運作，您可以執行命令 `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`

5. 檢閱角色，然後選擇建立角色。

使用目前登入的帳戶：選取此帳戶表示目前的帳戶將指定為 AWS 安全事件應變 成員資格的中央成員資格帳戶。組織中的個人將需要透過此帳戶存取服務，以建立、存取和管理作用中和已解決的案例。

確定您有足夠的管理許可 AWS 安全事件應變。

如需新增許可的特定步驟，請參閱新增和移除 IAM 身分許可。

請參閱 AWS 安全事件應變 受管政策。

若要驗證 IAM 許可，您可以遵循下列步驟：

- 檢查 IAM 政策：檢閱連接至使用者、群組或角色的 IAM 政策，以確保其授予必要的許可。您可以導覽至 https://console.aws.amazon.com/iam/：`Users`//。 `Permissions`
- 測試許可：嘗試執行驗證許可所需的動作。例如，如果您需要存取案例，請嘗試 `ListCases`。如果您沒有必要的許可，您將會收到錯誤訊息。
- 使用 AWS CLI 或 SDK：您可以在偏好的程式設計語言中使用 AWS Command Line Interface 或 AWS 開發套件來測試許可。例如，使用 AWS Command Line Interface，您可以執行 `aws sts get-caller-identity`命令來驗證目前的使用者許可。
- 檢查 AWS CloudTrail 日誌：檢閱 CloudTrail 日誌，以查看您嘗試執行的動作是否正在記錄。這可協助您識別任何許可問題。
- 使用 IAM 政策模擬器：IAM 政策模擬器是一種工具，可讓您測試 IAM 政策並查看它們對您的許可的影響。

> **Note**
>
> 具體步驟可能會因 AWS 服務和您嘗試執行的動作而有所不同。

設定成員資格詳細資訊

- 選取將存放您的成員資格和案例 AWS 區域 的 。

> **Warning**
>
> 您無法在初始成員資格註冊 AWS 區域 後變更預設值。

- 您可以選擇性地選取此成員資格的名稱。
- 主要和次要聯絡人必須在建立成員資格工作流程中提供。這些聯絡人會自動包含在事件回應團隊中。單一成員資格至少必須存在兩個聯絡人，以確保事件回應團隊中至少包含兩個聯絡人。
- 為您的成員資格定義選用標籤。標籤可協助您追蹤 AWS 成本和搜尋資源。

將帳戶與 建立關聯 AWS Organizations

您的成員資格授予 AWS 帳戶 中所有連結的涵蓋範圍 AWS Organizations。 當從您的組織新增或移除帳戶時，關聯帳戶會自動更新。

設定主動回應和提醒分類工作流程

主動回應和提醒分類工作流程是一項選用功能，可讓您在組織內啟用 ，以監控已啟用的安全服務。選取要啟用的功能旁的切換開關。

如果您遇到任何加入問題，請建立 AWS 支援 案例以取得其他協助。請務必包含詳細資訊，包括 AWS 帳戶 ID 和您在設定程序期間可能看到的任何錯誤。

主動回應和警示分類： AWS 安全事件應變 監控並調查從 Amazon GuardDuty 和 Security Hub 整合產生的警示。若要使用此功能，必須啟用 Amazon GuardDuty。 會使用服務自動化來 AWS 安全事件應變 分類低優先順序警示，讓您的團隊可以專注於最關鍵的問題。如需 如何使用 AWS 安全事件應變 Amazon GuardDuty 和 的詳細資訊 AWS Security Hub，請參閱 使用者指南的偵測和分析一節。

此功能可讓 AWS 安全事件應變 監控和調查 AWS 區域 組織中所有帳戶和作用中支援的問題清單。為了促進此功能， 會在您 內的所有成員帳戶中 AWS 安全事件應變 自動建立服務連結角色 AWS Organizations。不過，對於 管理帳戶，您必須手動建立服務連結角色才能啟用監控。

服務無法在 管理帳戶中建立服務連結角色。您必須使用 AWS CloudFormation 堆疊集，在管理帳戶中手動建立此角色。

遏制：發生安全事件時， AWS 安全事件應變 可以執行遏制動作以快速減輕影響，例如隔離遭入侵的主機或輪換登入資料。根據預設，安全事件回應不會啟用遏制功能。若要執行這些遏制動作，您必須先將必要的許可授予服務。這可以透過部署 AWS CloudFormation StackSet 來完成，該 StackSet 會建立所需的角色。

使用者任務

目錄

- 儀表板
- 管理我的事件回應團隊
- 帳戶與 的關聯 AWS Organizations
- 監控和調查
- 案例
- 管理案例
- 使用 AWS CloudFormation 堆疊集
- 取消成員資格

儀表板

在 AWS 安全事件應變 主控台上，儀表板會為您提供事件回應團隊的概觀、主動回應狀態，以及四週的案例滾動計數。

選取 `View incident response team` 以存取事件回應團隊成員的詳細資訊。

選取 `proactive response`以識別是否已啟用警示分類。如果您沒有啟用`alert triaging`工作流程，您可以監控其狀態並選擇`Proactive Response`啟用它。

儀表板的我的案例區段會顯示已開啟和已關閉 AWS 支援案例的數量，以及在定義期間內指派給您的自我管理案例。它也會顯示解決關閉案例所需的平均時間，以小時為單位。

管理我的事件回應團隊

您的事件回應團隊包含事件回應程序的利益相關者。您最多可以設定十位利益相關者做為成員資格的一部分。

內部利益相關者的範例包括事件回應團隊的成員、安全分析師、應用程式擁有者和安全領導團隊。

外部利益相關者的範例包括獨立軟體廠商 (ISV) 和受管服務供應商 (MSP) 的個人，而您想要這些個人包含在事件回應程序中。

> **Note**
>
> 設定您的事件回應團隊不會自動授予團隊成員存取 服務資源的權限，例如成員資格和案例。您可以使用 的 AWS 受管政策 AWS 安全事件應變 來授予 資源的讀取和寫入存取權。 按一下此處以進一步了解。

您在成員層級指定的事件回應團隊成員會自動新增至任何案例。建立案例之後，您可以隨時新增或移除個別團隊成員。

事件回應團隊將收到有關下列事件的電子郵件通知：

- 案例 （建立、刪除、更新）
- 註解 （建立、刪除、更新）
- 附件 （建立、刪除、更新）
- 成員資格 （建立、更新、取消、繼續）

帳戶與 的關聯 AWS Organizations

當您啟用 時 AWS 安全事件應變，將會建立成員資格並與您的 保持一致 AWS Organizations。Organizations 中的所有帳戶都與您的 AWS 安全事件應變 成員資格保持一致。

如需詳細資訊，請參閱使用 管理 AWS 安全事件應變 帳戶 AWS Organizations。

監控和調查

AWS 安全事件應變 會檢閱並分類來自 Amazon GuardDuty 的安全提醒 AWS Security Hub，然後根據您的環境設定禁止規則，以防止不必要的提醒。 AWS CIRT 團隊會調查未分類的問題清單，並快速呈報和引導您的團隊快速包含潛在問題。如果需要，您可以授予代表您實作遏制動作的 AWS 安全事件應變 許可。

AWS 安全事件應變 符合 NIST 800-61r2 電腦安全事件處理指南的安全事件回應。透過符合此業界標準， AWS 安全事件應變 提供一致的安全事件管理方法，並遵循保護和回應 AWS 您環境中安全事件的最佳實務。

當 AWS 安全事件應變 服務識別安全提醒或您請求安全協助時， AWS CIRT 會進行調查。團隊會收集日誌事件和服務資料，例如 GuardDuty 提醒、分類和分析該資料、執行修復和遏制活動，並提供事件後報告。

目錄

- 準備
- 偵測和分析
- 包含
- 根除
- 復原
- 事件後報告

準備

AWS 安全事件應變 團隊會調查並在整個安全事件回應生命週期中與您合作。建議您設定此團隊，並在發生安全事件之前指派必要的許可。

偵測和分析

AWS 安全事件應變 會監控、分類、調查來自 Amazon GuardDuty 的安全調查結果，並透過 整合 AWS Security Hub。可大幅增強 AWS 安全事件應變監控和調查功能範圍和有效性的其他動作包括：

啟用支援的偵測來源

> **Note**
>
> AWS 安全事件應變 服務成本不包括與受支援偵測或使用其他服務來源相關的用量和其他成本和費用 AWS 。如需成本詳細資訊，請參閱個別功能或服務頁面。

Amazon GuardDuty

GuardDuty 是一種威脅偵測服務，可持續監控、分析和處理您 AWS 環境中的資料來源和日誌。不需要啟用 GuardDuty AWS 安全事件應變；不過，若要使用主動回應和提醒分類功能，必須啟用 Amazon GuardDuty。

若要在整個組織中啟用 GuardDuty，請參閱《Amazon GuardDuty 使用者指南》中的`Setting up GuardDuty`一節。

強烈建議您在所有支援的 中啟用 GuardDuty AWS 區域。這可讓 GuardDuty 產生有關未經授權或異常活動的調查結果，即使在您未主動使用的區域中也是如此。如需詳細資訊，請參閱 Amazon GuardDuty 區域和端點

啟用 GuardDuty 可讓您 AWS 安全事件應變 存取關鍵威脅偵測資料，增強其識別和回應 AWS 環境中潛在安全問題的能力。

AWS Security Hub

Security Hub 可以從數個 AWS 服務和支援的第三方安全解決方案中擷取安全調查結果。這些整合可協助 AWS 安全事件應變 監控和調查來自其他偵測工具的問題清單。

若要啟用 Security Hub 與 Organizations 整合，請參閱 AWS Security Hub 使用者指南。

有多種方式可在 Security Hub 上啟用整合。對於第三方產品整合，您可能需要從 購買整合 AWS Marketplace，然後設定整合。整合資訊提供完成這些任務的連結。進一步了解如何啟用 AWS Security Hub 整合。

AWS 安全事件應變 可以在與下列工具整合時監控和調查問題清單 AWS Security Hub：

- CrowdStrike – CrowdStrike Falcon
- 浮水印 – 浮水印
- Trend Micro – Cloud One

透過啟用這些整合，您可以大幅提升 AWS 安全事件應變監控和調查功能的範圍和有效性。

分析問題清單。

AWS 安全事件應變 自動化和 AWS CIRT 服務團隊將分析支援工具的所有調查結果。我們將使用 AWS Support Cases 與您通訊，開始了解您的環境。例如，當我們需要了解問題清單是預期的行為，還是應該呈報至事件時。隨著我們從您的環境進一步了解，我們將自訂服務並減少通訊次數。

報告事件。

您可以透過 AWS 安全事件應變 服務入口網站引發安全事件。在安全事件期間不要等待。 AWS 安全事件應變 會使用自動化和手動技術來調查安全事件、分析日誌，以及尋找異常模式。您的合作夥伴關係和對您環境的了解可加速此分析。

通訊。

AWS 安全事件應變 透過事件案例與您的安全聯絡人互動，在調查期間通知您。多個團隊成員可能支援您的事件，所有 都會使用事件票證來取得客戶提供的內容和 AWS 更新。

通訊可能包括產生安全提醒時的自動通知；事件分析期間的通訊；建立呼叫橋接器；日誌檔案等成品的持續分析；以及在安全事件期間取得調查結果。

此服務將建立 AWS 安全事件應變 案例，以與您的團隊進行通訊。我們會針對您的成員帳戶建立案例。此方法會將所有帳戶的通訊集中到單一位置。「【主動案例】」字首有助於識別由 起始的案例 AWS 安全事件應變。

透過主動參與這些通訊並提供及時的回應，您可以協助 AWS 安全事件應變 服務：

- 更好地了解您的環境和預期的行為。
- 隨著時間的推移減少誤報。
- 改善警示的準確性和相關性。
- 確保快速回應真正的安全事件。
- 請記住， AWS 安全事件應變 服務的有效性會隨著您的協同合作而改善，進而產生更安全且有效率監控 AWS 的環境。

包含

AWS 安全事件應變 會與您合作以包含事件。您可以設定 AWS 安全事件應變 的服務角色，在帳戶中採取自動和手動動作，做為提醒的回應。您也可以使用 SSM 文件，自行執行遏制，或與您的第三方關係合作。

抑制的重要部分是決策；例如是否關閉系統、將資源與網路隔離、關閉存取或結束工作階段。當有預先決定的策略和程序來包含事件時，這些決策會更容易。 AWS 安全事件應變 提供遏制策略、通知您潛在的影響，並只在您已考慮和同意涉及的風險之後，才引導您實施解決方案。

AWS 安全事件應變 代表您執行支援的遏制動作，以加快回應速度，並減少威脅行為者在環境中造成潛在損害的時間。此功能可更快速地緩解已識別的威脅、將潛在影響降至最低，並增強您的整體安全狀態。根據分析的資源，有不同的遏制選項。支援的遏制動作如下：

- EC2 遏制：`AWSSupport-ContainEC2Instance`遏制自動化會執行 EC2 執行個體的可逆網路遏制，讓執行個體保持完整且執行中，但會將其與任何新的網路活動隔離，並防止其與 VPC 內外的資源通訊。

  > **Important**
  >
  > 請務必注意，現有的追蹤連線不會因為變更安全群組而關閉，只有新的安全群組和此 SSM 文件會有效封鎖未來的流量。如需詳細資訊，請參閱 服務技術指南的來源遏制區段。

- IAM 遏制：`AWSSupport-ContainIAMPrincipal`遏制自動化會執行 IAM 使用者或角色的可逆網路遏制，將使用者或角色留在 IAM 中，但將其與帳戶中的資源通訊隔離。

- S3 遏制：`AWSSupport-ContainS3Resource`遏制自動化會執行 S3 儲存貯體的可逆遏制，將物件保留在儲存貯體中，並透過修改其存取政策來隔離 Amazon S3 儲存貯體或物件。

> **Important**
>
> AWS 安全事件應變 根據預設， 不會啟用遏制功能，若要執行這些遏制動作，您必須先使用角色將必要的許可授予服務。您可以個別建立每個帳戶或整個組織的這些角色，方法是使用 AWS CloudFormation 堆疊集來建立所需的角色。

AWS 安全事件應變 鼓勵您針對符合您風險偏好的每個主要事件類型考慮遏制策略。記錄明確的條件，以協助在事件期間做出決策。要考慮的條件包括：

- 資源的潛在損壞
- 保留證據和法規要求
- 服務無法使用 （例如，網路連線、提供給外部各方的服務）
- 實作策略所需的時間和資源
- 策略的有效性 （例如，部分遏制與完全遏制）
- 解決方案的持久性 （例如，可逆與不可逆）
- 解決方案的持續時間 （例如，緊急解決方法、暫時解決方法、永久解決方案） 套用可降低風險的安全控制，並允許時間來定義和實作更有效的遏制策略。

AWS 安全事件應變 建議分階段方法，以根據資源類型實現高效和有效的遏制，涉及短期和長期策略。

- 遏制策略
  - 可以 AWS 安全事件應變 識別安全事件的範圍嗎？
    - 如果是，請識別所有資源 （使用者、系統、資源）。
    - 如果否，請平行調查，並對已識別的資源執行下一個步驟。
  - 資源可以隔離嗎？
    - 如果是，請繼續隔離受影響的資源。
    - 如果否，則與系統擁有者和管理員合作，以決定包含問題所需的進一步動作。
  - 是否將所有受影響的資源與未受影響的資源隔離？
    - 如果是，請繼續下一個步驟。
    - 如果否，則繼續隔離受影響的資源以完成短期遏制，並防止事件進一步升級。

- 系統備份
  - 是否為進一步分析而建立受影響系統的備份副本？
  - 鑑識複本是否加密並存放在安全的位置？
    - 如果是，請繼續下一個步驟。
    - 如果沒有，請加密鑑識影像，然後將它們存放在安全的位置，以防止意外使用、損壞和竄改。

根除

在根除階段，請務必識別和解決所有受影響的帳戶、資源和執行個體，例如刪除惡意軟體、移除遭入侵的使用者帳戶，以及緩解任何發現的漏洞，以在整個環境中套用統一的修補。

最佳實務是使用分階段方法來根除和復原，以及排定修復步驟的優先順序。早期階段的目的是透過高價值的變更快速提高整體安全性（天到週），以防止未來發生事件。後期階段可以專注於長期變更（例如，基礎設施變更），並持續努力讓企業盡可能保持安全。每個案例都是唯一的， AWS CIRT 將與您一起評估必要的動作。

考慮下列各項：

- 您可以重新製作系統映像，並使用修補程式或其他對策來強化系統，以防止或降低攻擊風險嗎？
- 您可以將受感染的系統取代為新的執行個體或資源，在終止受感染的項目時啟用乾淨的基準？
- 您是否已移除未經授權的使用所留下的所有惡意軟體和其他成品，並強化受影響的系統以防止進一步的攻擊？
- 受影響的資源是否需要鑑識？

復原

AWS 安全事件應變 為您提供指引，協助您將系統還原至正常操作、確認系統正常運作，並修復任何漏洞，以防止未來的類似事件。 AWS 安全事件應變 不會直接協助系統復原。主要考量事項包括：

- 受影響的系統是否針對最近的攻擊進行修補和強化？
- 將系統還原至生產的可行時間表為何？
- 您將使用哪些工具來測試、監控和驗證還原的系統？

事件後報告

AWS 安全事件應變 在您的團隊和我們的安全活動結束後， 會提供事件的摘要。

每個月月底，服務 AWS 安全事件應變 會透過電子郵件將每月報告傳送給每位客戶的主要聯絡窗口。報告將使用如下所述的指標，以 PDF 格式交付。客戶每個 會收到一份報告 AWS Organizations。

案例指標

- 已建立的案例
  - 維度名稱：類型
  - 維度值： AWS 支援、自我支援
  - 單位：計數
  - 描述：建立的案例數量。
- 案例已關閉
  - 維度名稱：類型
  - 維度值： AWS 支援、自我管理
  - 單位：計數
  - 描述：關閉案例總數的度量。
- 已開啟的案例
  - 維度名稱：類型
  - 維度值： AWS 支援、自我支援
  - 單位：計數
  - 描述：開啟的案例數量。

分類指標

- 收到的調查結果
  - 單位：計數
  - 描述：傳送至分類的調查結果數量。
- 已封存的問題清單
  - 單位：計數
  - 描述：在未手動調查的情況下處理之後封存的問題清單數目。
- 手動調查的問題清單
  - 單位：計數
  - 描述：執行手動調查的調查結果數量。
- 調查已封存

  - 單位：計數
  - 描述：導致誤報並傳送至封存的手動調查數量
- 調查已呈報
  - 單位：計數
  - 描述：導致安全事件的手動調查數量

案例

AWS 安全事件應變 可讓您建立兩種類型的案例 - AWS 支援或自我管理的案例。

建立 AWS 支援的案例

您可以透過 AWS 安全事件應變 主控台、 API 或 建立 AWS 支援的案例 AWS Command Line Interface。 AWS 支援的案例可讓您從 AWS 客戶事件回應團隊 (CIRT) 取得支援。

> **Note**
>
> AWS CIRT 將在 15 分鐘內回應您的案例。回應時間為來自 AWS CIRT 的第一個回應。我們將盡一切合理努力在此時間範圍內回應您的初始請求。此回應時間不適用於後續回應。

下列範例涵蓋 主控台的使用。

1. 登入 AWS Management Console。在 https：//https://console.aws.amazon.com/security-ir/ 開啟安全事件回應主控台。
2. 選擇建立案例
3. 選擇使用 解決案例 AWS
4. 選取請求的類型
   a. 作用中安全事件：此類型適用於緊急事件回應支援和服務。
   b. 調查：調查可讓您取得對感知安全事件的支援，其中 AWS CIRT 可以支援日誌刪除和事件回應調查的次要確認。
5. 將開始日期預估設定為事件的最早指標日期。例如，當您第一次遇到異常行為，或收到第一個相關的安全提醒時。
6. 定義案例的標題
7. 提供案例的詳細說明。 請考慮下列層面，這些層面可協助事件回應者解決案例：

   a. 發生了什麼？
   b. 誰發現並報告了事件？
   c. 誰會受到案例的影響？
   d. 已知的影響是什麼？
   e. 此案例的緊急程度為何？
   f. 新增案例範圍內的一或多個 AWS 帳戶 IDs。
8. 新增選用案例詳細資訊：
   a. 從下拉式清單中選取受影響的主要服務。
   b. 從下拉式清單中選取受影響的主要區域。
   c. 新增您識別為此案例一部分的一或多個威脅執行者 IP 地址。
9. 將選用的其他事件回應者新增至將接收通知的案例。若要新增個人，請執行下列動作：
   a. 新增電子郵件地址。
   b. 新增選用的名字和姓氏。
   c. 選擇新增以新增另一個個人。
   d. 若要移除個人，請選擇個人的移除選項。
   e. 選擇新增，將所有列出的個人新增至案例。
      i. 您可以選取多個個人，然後選擇移除，從清單中將其刪除。
10. 將選用標籤新增至案例。
   a. 若要新增標籤，請執行以下操作：
   b. 選擇 Add new tag (新增標籤)。
   c. 針對金鑰，輸入標籤的名稱。
   d. 針對值，輸入標籤值。
   e. 若要移除標籤，選擇該標籤的移除選項。

建立 AWS 支援案例後， AWS CIRT 和您的事件回應團隊會立即收到通知。

建立自我管理的案例

您可以透過 AWS 安全事件應變 主控台、API 或 建立 的自我管理 AWS Command Line Interface。這種類型的案例不會與 AWS CIRT 互動。下列範例涵蓋 主控台的使用。

1. 登入 AWS Management Console。在 https：//https://console.aws.amazon.com/security-ir/ 開啟安全事件回應主控台。

2. 選擇 Create Case (建立案例)。
3. ChooseResolve 案例與我自己的事件回應團隊。
4. 將開始日期預估設定為事件的最早指標日期。例如，當您第一次遇到異常行為，或收到第一個相關的安全提醒時。
5. 定義案例的標題。建議在選取產生標題選項時，依建議將資料納入案例標題。
6. 屬於案例的 AWS 帳戶 IDs。若要新增帳戶 ID，請執行下列動作：
   a. 輸入 12 位數的帳戶 ID，然後選擇新增帳戶。
   b. 若要移除帳戶，請選擇您要從案例移除的帳戶旁的移除。
7. 提供案例的詳細說明。
   a. 請考慮下列層面，這些層面可協助事件回應者解決案例：
      i. 發生了什麼？
      ii. 誰發現並報告了事件？
      iii. 誰會受到案例的影響？
      iv. 已知的影響是什麼？
      v. 此案例的緊急程度為何？
8. 新增選用案例詳細資訊：
   a. 從下拉式清單中選取受影響的主要服務。
   b. 從下拉式清單中選取受影響的主要區域。
   c. 新增您識別為此案例一部分的一或多個威脅執行者 IP 地址。
9. 將選用的其他事件回應者新增至將接收通知的案例。若要新增個人，請執行下列動作：
   a. 新增電子郵件地址。
   b. 新增選用的名字和姓氏。
   c. 選擇新增以新增另一個個人。
   d. 若要移除個人，請選擇個人的移除選項。
   e. 選擇新增，將所有列出的個人新增至案例。您可以選取多個個人，然後選擇移除，從清單中將其刪除。
10. 將選用標籤新增至案例。若要新增標籤，請執行以下操作：
   a. 選擇 Add new tag (新增標籤)。
   b. 針對金鑰，輸入標籤的名稱。
   c. 針對值，輸入標籤值。
   d. 若要移除標籤，選擇該標籤的移除選項。

建立案例後，事件回應團隊會收到電子郵件通知。

回應 AWS 產生的案例

AWS 安全事件應變 當您需要採取行動或注意到可能會影響您的帳戶或資源的事項時， 可能會建立傳出通知或案例。只有在您啟用主動回應並提醒將工作流程分類為訂閱的一部分時，才會發生這種情況。

這些通知會在 AWS 安全事件應變 主控台中顯示為字首為「【主動案例】」的安全事件回應案例。若要檢視和管理這些案例：

- 在 https：//https://console.aws.amazon.com/security-ir/ 開啟安全事件回應主控台
- 按一下選單中的「案例」。
- 您應該能夠查看所有案例，包括字首為「【主動案例】」的案例。

這些案例可讓您視需要更新、解析並重新開啟。您可以透過這些案例直接與 AWS 安全事件應變 團隊通訊，確保有效處理潛在的安全問題。

管理案例

目錄

- 變更案例狀態
- 變更解析程式
- Action Items (動作項目)
- 編輯案例
- 通訊
- 許可
- 附件
- 標籤
- 案例活動
- 關閉案例

變更案例狀態

案例將處於下列其中一種狀態：

- 已提交：這是案例的初始狀態。此狀態的案例已由請求提交，但尚未處理。
- 偵測和分析：此狀態表示事件回應者已開始處理案例。此階段包括資料收集、分類事件，以及執行分析以建立資料驅動的結論。
- 遏制、消除和復原：在此狀態中，事件回應者已識別需要額外努力移除的可疑活動。事件回應者將為您提供業務風險分析和其他動作的建議。如果您已啟用服務的選擇加入功能，則 AWS 事件回應者將徵求您的同意，以對受影響帳戶中的 SSM 文件執行遏制動作 (SSM 文件）。
- 事件後活動：在此狀態中，已包含主要安全事件。現在的重點是復原並恢復正常的業務操作。如果案例的解析程式 AWS支援 ，則會提供摘要和根本原因分析。
- 關閉：這是工作流程的最終狀態。關閉狀態的案例表示工作已完成。關閉的案例無法重新開啟，因此請確保所有動作都已完成，然後再轉換為此狀態。

選擇動作/更新狀態，以變更自我管理案例的案例狀態。對於 AWS 支援的案例，狀態由 AWS CIRT 回應者設定。

變更解析程式

對於自我管理的案例，您的事件回應團隊可以向 請求協助 AWS。選擇從 取得說明 AWS，以變更此案例的解析程式 AWS。案例更新為 AWS 支援後，狀態會變更為已提交。現有的案例歷史記錄將可供 AWS CIRT 使用。一旦您向 請求協助 AWS ，您將無法將其變更回自我管理。

Action Items (動作項目)

處理案例的 AWS CIRT 回應者可能會向您的內部團隊請求動作。

在建立案例之後出現的動作項目包括：

- 請求提供許可，讓事件回應者存取案例
- 請求提供有關案例的詳細資訊

客戶動作待定時的動作項目：

- 請求對新評論採取行動以繼續案例

案例準備好關閉時的動作項目：

- 請求檢閱案例報告
- 請求關閉案例

編輯案例

選擇編輯以變更案例的詳細資訊。

對於 AWS 支援和自我管理的案例：

您可以在建立案例之後變更下列案例詳細資訊：

- Title
- 描述

僅適用於 AWS 支援的案例：

您可以變更其他欄位：

- 請求類型：
  - 作用中安全事件：此類型適用於緊急事件回應支援和服務。
  - 調查：調查可讓您取得對感知安全事件的支援，其中 AWS CIRT 可以支援安全事件的日誌刪除和次要確認。
- 開始日期預估：如果您收到此案例的指標早於初始提供的開始日期，請變更此欄位。請考慮在描述欄位中提供有關新偵測到指標的其他詳細資訊，或在通訊索引標籤中新增註解。

通訊

AWS CIRT 可以在處理案例時新增註解以記錄其活動。不同的 AWS CIRT 回應者可以同時處理案例。它們在通訊日誌中表示為AWS 回應者。

許可

許可索引標籤會列出案例的任何變更都會收到通知的所有個人。您可以新增和移除清單中的個人，直到案例關閉為止。

> **Note**
>
> 個別案例可讓您包含最多總共 30 個利益相關者。需要其他許可組態，才能將案例層級存取權授予這些利益相關者。

在 主控台中提供對案例的存取

若要提供 中案例的存取權 AWS Management Console，您可以複製 IAM 許可政策範本，並將此許可新增至使用者或角色。

將 IAM 政策新增至使用者或角色：

1. 複製 IAM 許可政策。
2. 透過 https://console.aws.amazon.com/iam/：// 在 中開啟 IAM。
3. 在導覽窗格中，選擇使用者或角色。
4. 選取使用者或角色以開啟詳細資訊頁面。
5. 在許可索引標籤中，選擇新增許可。
6. 選擇連接政策。
7. 選取適當的 AWS 安全事件應變 受管政策。
8. 選擇 Add Policy (新增政策)。

附件

您的事件回應者可以將附件新增至案例，以協助其他事件回應者調查自我管理的案例。

> **Note**
>
> 如果您選擇 AWS 支援的案例， AWS 則無法檢視附件。 AWS 支援案例的所有詳細資訊都必須透過案例評論或您使用偏好的通訊技術提供螢幕共用來共用。

選擇上傳，從您的電腦選取要新增至案例的檔案。

> **Note**
>
> 任何上傳的附件都會在案例成為 的七天後刪除`Closed`。

標籤

標籤是選用的標籤，您可以指派給您的案例，以保留該資源的中繼資料。每個標籤都是由索引鍵和選用值組成的標籤。您可以使用標籤來搜尋、配置成本，以及驗證資源的許可。

若要新增標籤，請執行以下操作：

1. 選擇 Add new tag (新增標籤)。
2. 針對金鑰，輸入標籤的名稱。
3. 針對值，輸入標籤值。

若要移除標籤，選擇該標籤的移除選項。

案例活動

稽核線索提供所有案例活動的詳細時間記錄。它們在事件後活動中提供重要資訊，並協助識別潛在的改善。任何案例變更的時間、使用者、動作和詳細資訊都會記錄在案例稽核追蹤中。

關閉案例

對於 AWS 支援的案例，請在案例詳細資訊頁面上選擇關閉案例，以在任何狀態永久關閉案例。案例通常會在永久關閉之前達到待關閉狀態。如果您以就緒關閉以外的任何其他狀態過早關閉案例，您請求 AWS CIRT 將停止處理此 AWS 支援案例。

如果您的事件回應團隊是回應者，請在案例詳細資訊頁面上選取動作/關閉案例。

> **Note**
>
> 「準備關閉」狀態表示案例可以永久關閉，而且不需要對案例進行額外的工作。

案例永久關閉後，就無法再次重新開啟。所有資訊都會提供唯讀。為了防止意外關閉，系統會要求您確認是否要關閉案例。

使用 AWS CloudFormation 堆疊集

> **Important**
>
> AWS 安全事件應變 根據預設， 不會啟用遏制功能，若要執行這些遏制動作，您必須先使用 角色將必要的許可授予服務。您可以透過部署StackSets 來個別建立每個帳戶或整個組織的這些角色，而 AWS CloudFormation StackSets 會建立所需的角色。

您可以找到有關如何建立具有服務受管許可的堆疊集的特定指示。

以下是建立 AWSSecurityIncidentResponseContainment 和 AWSSecurityIncidentResponseContainmentExecution 角色的範本堆疊集。

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS ###### containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
```

```
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainEC2Instance:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainS3Resource:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                    'Resource': '*',
                  },
                  {
                    'Effect': 'Allow',
                    'Action': ['iam:PassRole'],
                    'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                  },
                ],
            }
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
 'Action': 'sts:AssumeRole' }],
        }
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
```

```
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'iam:AttachRolePolicy',
                        'iam:AttachUserPolicy',
                        'iam:DeactivateMFADevice',
                        'iam:DeleteLoginProfile',
                        'iam:DeleteRolePolicy',
                        'iam:DeleteUserPolicy',
                        'iam:GetLoginProfile',
                        'iam:GetPolicy',
                        'iam:GetRole',
                        'iam:GetRolePolicy',
                        'iam:GetUser',
                        'iam:GetUserPolicy',
                        'iam:ListAccessKeys',
                        'iam:ListAttachedRolePolicies',
                        'iam:ListAttachedUserPolicies',
                        'iam:ListMfaDevices',
                        'iam:ListPolicies',
                        'iam:ListRolePolicies',
                        'iam:ListUserPolicies',
                        'iam:ListVirtualMFADevices',
                        'iam:PutRolePolicy',
                        'iam:PutUserPolicy',
                        'iam:TagMFADevice',
                        'iam:TagPolicy',
                        'iam:TagRole',
                        'iam:TagUser',
                        'iam:UntagMFADevice',
                        'iam:UntagPolicy',
                        'iam:UntagRole',
                        'iam:UntagUser',
                        'iam:UpdateAccessKey',
                        'identitystore:CreateGroupMembership',
                        'identitystore:DeleteGroupMembership',
                        'identitystore:IsMemberInGroups',
                        'identitystore:ListUsers',
                        'identitystore:ListGroups',
                        'identitystore:ListGroupMemberships',
                      ],
```

```
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowOrgListAccounts',
                      'Effect': 'Allow',
                      'Action': 'organizations:ListAccounts',
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowSSOContainment',
                      'Effect': 'Allow',
                      'Action':
                        [
                          'sso:CreateAccountAssignment',
                          'sso:DeleteAccountAssignment',
                          'sso:DeleteInlinePolicyFromPermissionSet',
                          'sso:GetInlinePolicyForPermissionSet',
                          'sso:ListAccountAssignments',
                          'sso:ListInstances',
                          'sso:ListPermissionSets',
                          'sso:ListPermissionSetsProvisionedToAccount',
                          'sso:PutInlinePolicyToPermissionSet',
                          'sso:TagResource',
                          'sso:UntagResource',
                        ],
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowSSORead',
                      'Effect': 'Allow',
                      'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowS3Read',
                      'Effect': 'Allow',
                      'Action':
                        [
                          's3:GetAccountPublicAccessBlock',
                          's3:GetBucketAcl',
                          's3:GetBucketLocation',
                          's3:GetBucketOwnershipControls',
                          's3:GetBucketPolicy',
```

```
                        's3:GetBucketPolicyStatus',
                        's3:GetBucketPublicAccessBlock',
                        's3:GetBucketTagging',
                        's3:GetEncryptionConfiguration',
                        's3:GetObject',
                        's3:GetObjectAcl',
                        's3:GetObjectTagging',
                        's3:GetReplicationConfiguration',
                        's3:ListBucket',
                        's3express:GetBucketPolicy',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Write',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:CreateBucket',
                        's3:DeleteBucketPolicy',
                        's3:DeleteObjectTagging',
                        's3:PutAccountPublicAccessBlock',
                        's3:PutBucketACL',
                        's3:PutBucketOwnershipControls',
                        's3:PutBucketPolicy',
                        's3:PutBucketPublicAccessBlock',
                        's3:PutBucketTagging',
                        's3:PutBucketVersioning',
                        's3:PutObject',
                        's3:PutObjectAcl',
                        's3express:CreateSession',
                        's3express:DeleteBucketPolicy',
                        's3express:PutBucketPolicy',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowAutoScalingWrite',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'autoscaling:CreateOrUpdateTags',
                        'autoscaling:DeleteTags',
                        'autoscaling:DescribeAutoScalingGroups',
```

```
                'autoscaling:DescribeAutoScalingInstances',
                'autoscaling:DescribeTags',
                'autoscaling:EnterStandby',
                'autoscaling:ExitStandby',
                'autoscaling:UpdateAutoScalingGroup',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowEC2Containment',
            'Effect': 'Allow',
            'Action':
              [
                'ec2:AuthorizeSecurityGroupEgress',
                'ec2:AuthorizeSecurityGroupIngress',
                'ec2:CopyImage',
                'ec2:CreateImage',
                'ec2:CreateSecurityGroup',
                'ec2:CreateSnapshot',
                'ec2:CreateTags',
                'ec2:DeleteSecurityGroup',
                'ec2:DeleteTags',
                'ec2:DescribeImages',
                'ec2:DescribeInstances',
                'ec2:DescribeSecurityGroups',
                'ec2:DescribeSnapshots',
                'ec2:DescribeTags',
                'ec2:ModifyNetworkInterfaceAttribute',
                'ec2:RevokeSecurityGroupEgress',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowKMSActions',
            'Effect': 'Allow',
            'Action':
              [
                'kms:CreateGrant',
                'kms:DescribeKey',
                'kms:GenerateDataKeyWithoutPlaintext',
                'kms:ReEncryptFrom',
                'kms:ReEncryptTo',
              ],
            'Resource': '*',
```

```
                },
                {
                  'Sid': 'AllowSSMActions',
                  'Effect': 'Allow',
                  'Action': ['ssm:DescribeAutomationExecutions'],
                  'Resource': '*',
                },
              ],
          }
```

取消成員資格

具有 的 CancelMembership 許可的角色 AWS 安全事件應變 可以從主控台、API 或 取消成員資格 AWS Command Line Interface。

> **Important**
>
> 一旦取消成員資格，您將無法檢視歷史案例資料。如果您在當月取消，您的會員資格將一直開放到月底。在計費週期結束時，最終成員資格取消時，正在或`ready to close`將會終止的任何資源`Active`或調查。

> **Important**
>
> AWS 安全事件應變 不會遵循每月發生的標準周年計費週期。服務計費會逐月執行。一些範例：
>
> - 12 月 29 日，1 月 29 日
> - 1 月 29 日，2 月 26 日（非閏年）
> - 2 月 26 日、3 月 29 日

> **Important**
>
> 如果您重新訂閱服務，將會建立新的成員資格，而且只有在取消之前下載它們時，才能存取先前成員資格下的案例資源。

取消成員資格後，成員資格事件回應團隊中的每個人都會收到電子郵件通知。

> **Important**
>
> 如果您使用委派管理員帳戶建立成員資格，並使用 AWS Organizations API 從帳戶移除委派管理員指定，成員資格將立即終止。

標記 AWS 安全事件應變 資源

標籤是您指派或 AWS 指派給 AWS 資源的中繼資料標籤。每個標籤皆包含鍵與值。對於您指派的標籤，您可以定義鍵與值。例如，您可以將鍵定義為 `stage`，將資源的值定義為 `test`。

標籤可協助您執行以下操作：

- 識別和組織您的 AWS 資源。許多 AWS 服務 支援標記，因此您可以將相同的標籤指派給來自不同服務的資源，以指出資源相關。
- 追蹤您的 AWS 成本。您可以在儀表板上 AWS Billing 啟用這些標籤。 AWS 會使用標籤來分類您的成本，並傳送每月成本分配報告給您。如需詳細資訊，請參閱 AWS 帳單使用者指南中的使用成本分配標籤。
- 控制對 AWS 資源的存取。如需詳細資訊，請參閱《IAM 使用者指南》中的使用標籤控制存取權限。

請參閱 AWS 安全事件應變 API 參考進行標記。

使用 AWS CloudShell 處理 AWS 安全事件回應

AWS CloudShell 是以瀏覽器為基礎的預先驗證 Shell，您可以直接從 啟動 AWS Management Console。您可以使用您偏好的 shell (Bash、PowerShell 或 Z shell) 對 AWS 服務（包括 AWS 安全事件回應）執行 AWS CLI 命令。另外，您無需下載或安裝命令列工具即可執行此操作。

您AWS CloudShell 從 啟動 AWS Management Console ，而您用來登入 主控台的 AWS 登入資料會自動在新的 shell 工作階段中使用。此預先驗證 AWS CloudShell 使用者可讓您在使用 第 2 AWS CLI 版（預先安裝在 shell 的運算環境）與安全事件回應等 AWS 服務互動時，略過設定登入資料。

目錄

- 取得 的 IAM 許可 AWS CloudShell
- 使用 與安全事件回應互動 AWS CloudShell

取得 的 IAM 許可 AWS CloudShell

AWS Identity and Access Management管理員可以使用 提供的存取管理資源，將許可授予 IAM 使用者，讓他們可以存取 AWS CloudShell 和使用環境的功能。

管理員授予使用者存取權的最快方式是透過 AWS 受管政策。AWS 受管政策是由 AWS建立並管理的獨立政策。下列適用於 CloudShell 的 AWS 受管政策可以連接到 IAM 身分：

- `AWSCloudShellFullAccess`：授予許可，以 AWS CloudShell 完整存取所有功能。

如果您想要限制 IAM 使用者可執行的動作範圍 AWS CloudShell，您可以建立使用 `AWSCloudShellFullAccess`受管政策做為範本的自訂政策。如需限制 CloudShell 中使用者可用的動作的詳細資訊，請參閱AWS CloudShell 《 使用者指南》中的使用 IAM 政策管理 AWS CloudShell 存取和用量。

> **Note**
>
> 您的 IAM 身分也需要政策，授予呼叫安全事件回應的許可。

使用 與安全事件回應互動 AWS CloudShell

AWS CloudShell 從 啟動後 AWS Management Console，您可以立即開始使用命令列界面與安全事件回應互動。

> **Note**
>
> 使用 AWS CLI 時 AWS CloudShell，您不需要下載或安裝任何其他資源。此外，因為您已經在 Shell 中驗證身分，因此無需設定憑證即可呼叫。

使用 AWS CloudShell 和 安全事件回應

- 從 中 AWS Management Console，您可以選擇導覽列上可用的下列選項來啟動 CloudShell：
  - 選擇 CloudShell 圖示。
  - 開始在搜尋方塊中輸入「cloudshell」，然後選擇 CloudShell 選項。

使用 記錄 AWS 安全事件回應 API 呼叫 AWS CloudTrail

AWS 安全事件回應已與 整合 AWS CloudTrail，此服務提供使用者、角色或安全事件回應中的 AWS 服務所採取動作的記錄。CloudTrail 會將安全事件回應的所有 API 呼叫擷取為事件。擷取的呼叫包括來自安全事件回應主控台的呼叫，以及對安全事件回應 API 操作的程式碼呼叫。如果您建立追蹤，則可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括安全事件回應的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對安全事件回應提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的安全事件回應資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在安全事件回應中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立追蹤或 CloudTrail Lake 事件資料存放區。

CloudTrail 追蹤

線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。使用 建立的所有線索 AWS Management Console 都是多區域。您可以使用 AWS CLI建立單一或多區域追蹤。建議您建立多區域追蹤，因為您擷取 AWS 區域 帳戶中所有 的活動。如果您建立單一區域追蹤，您只能檢視追蹤 AWS 區域中記錄的事件。如需追蹤的詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的為您的 AWS 帳戶建立追蹤和為組織建立追蹤。

您可以透過建立追蹤，免費將持續管理事件的一個複本從 CloudTrail 傳遞至您的 Amazon S3 儲存貯體，但這樣做會產生 Amazon S3 儲存費用。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

CloudTrail Lake 事件資料存放區

CloudTrail Lake 讓您能夠對事件執行 SQL 型查詢。CloudTrail Lake 會將分列式 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。如需 CloudTrail Lake 的詳細資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 AWS CloudTrail Lake。

CloudTrail Lake 事件資料存放區和查詢會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

CloudTrail 會記錄所有安全事件回應動作，並記錄在AWS 安全事件回應 API 參考中。例如，對 `CreateMembership`、`CreateCase` 和 `UpdateCase` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是使用根還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解安全事件回應日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示示範 CreateCase 動作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
```

```
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
```

```
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

使用 管理 AWS 安全事件應變 帳戶 AWS Organizations

AWS 安全事件應變 已與 整合 AWS Organizations。組織的 AWS Organizations 管理帳戶可以指定 帳戶做為委派管理員 AWS 安全事件應變。此動作會在 中啟用 AWS 安全事件應變 做為信任的服務 AWS Organizations。如需如何授予這些許可的資訊，請參閱AWS Organizations 搭配使用 與其他 AWS 服務。

以下各節將逐步解說各種任務，您可以執行這些任務做為委派的安全事件回應管理員帳戶。

目錄

- AWS 安全事件應變 搭配 使用的考量和建議 AWS Organizations
- 啟用 的信任存取 AWS 帳戶管理
- 指定委派安全事件回應管理員帳戶所需的許可
- 為 指定委派管理員 AWS 安全事件應變
- 將成員新增至 AWS 安全事件應變
- 從 移除成員 AWS 安全事件應變

AWS 安全事件應變 搭配 使用的考量和建議 AWS Organizations

下列考量事項和建議可協助您了解委派安全事件回應管理員帳戶的運作方式 AWS 安全事件應變：

委派的安全事件回應管理員帳戶是區域性的。

委派的安全事件回應管理員帳戶和成員帳戶必須透過 新增 AWS Organizations。

的委派管理員帳戶 AWS 安全事件應變。

您可以指定一個成員帳戶做為委派的安全事件回應管理員帳戶。例如，如果您### ##### 指定成員帳戶 111122223333，則無法在### #### 指定其他成員帳戶 555555555555。您必須在所有其他區域中使用與委派安全事件回應管理員帳戶相同的帳戶。

不建議將組織的管理設定為委派的安全事件回應管理員帳戶。

您組織的管理可以是委派的安全事件回應管理員帳戶。不過， AWS 安全性最佳實務遵循最低權限原則，不建議使用此組態。

從即時訂閱中移除委派的安全事件回應管理員帳戶會立即取消訂閱。

如果您移除委派的安全事件回應管理員帳戶， 會 AWS 安全事件應變 移除與此委派安全事件回應管理員帳戶相關聯的所有成員帳戶。 AWS 安全事件應變 將不再為所有這些成員帳戶啟用 。

啟用 的信任存取 AWS 帳戶管理

啟用 的受信任存取 AWS 安全事件應變 可讓 管理帳戶的委派管理員修改每個成員帳戶的特定資訊和中繼資料 （例如主要或備用聯絡詳細資訊） AWS Organizations。

使用下列程序，在您的組織中啟用 AWS 安全事件應變 的信任存取。

> **最低許可**
>
> 若要執行這些任務，您必須符合下列要求：
>
> - 您只能從組織的管理帳戶執行此操作。
> - 您的組織必須啟用所有功能。

Console

啟用 的信任存取 AWS 安全事件應變

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在導覽窗格中選擇服務。
3. AWS 安全事件應變 在服務清單中選擇 。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS 安全事件應變對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。

API/CLI

啟用 的信任存取 AWS 帳戶管理

執行下列命令後，您可以使用組織的管理帳戶中的登入資料來呼叫帳戶管理 API 操作，該操作使用 `--accountId` 參數來參考組織中的成員帳戶。

- AWS CLI: enable-aws-service-access

  下列範例 AWS 安全事件應變 會在呼叫帳戶的組織中啟用 的信任存取。

```
$ aws organizations enable-aws-service-access \
```

```
                                        --service-principal security-
ir.amazonaws.com
```

此命令如果成功就不會產生輸出。

指定委派安全事件回應管理員帳戶所需的許可

您可以選擇使用委派管理員來設定您的 AWS 安全事件應變 成員資格 AWS Organizations。如需如何授予這些許可的資訊，請參閱搭配使用 AWS Organizations 與其他 AWS 服務。

> **Note**
>
> AWS 安全事件應變 使用主控台進行設定和管理時， 會自動啟用 AWS Organizations 信任關係。如果您使用 CLI/SDK，則必須使用 EnableAWSServiceAccess API 手動啟用此項目，以信任 `security-ir.amazonaws.com`。

身為 AWS Organizations 管理員，在您為組織指定委派的安全事件回應管理員帳戶之前，請確認您可以執行下列 AWS 安全事件應變 動作： `security-ir:CreateMembership`和 `security-ir:UpdateMembership`。這些動作可讓您使用 為您的組織指定委派的安全事件回應管理員帳戶 AWS 安全事件應變。您還必須確保您可以執行 AWS Organizations 動作，以協助您擷取組織的相關資訊。

若要授予這些許可，請在您帳戶的 AWS Identity and Access Management (IAM) 政策中包含下列陳述式：

```
{
    "Sid": "PermissionsForSIRAdmin",
    "Effect": "Allow",
    "Action": [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

如果您想要將 AWS Organizations 管理帳戶指定為委派的安全事件回應管理員帳戶，您的帳戶也需要 IAM 動作：`CreateServiceLinkedRole`。請先檢閱，AWS 安全事件應變 搭配 使用的考量和建議 AWS Organizations再繼續新增許可。

若要繼續將 AWS Organizations 管理帳戶指定為委派的安全事件回應管理員帳戶，請將下列陳述式新增至 IAM 政策，並以您的 AWS Organizations 管理帳戶的 AWS 帳戶 ID 取代 *111122223333*：

```
{
 "Sid": "PermissionsToEnableSecurityIncidentResponse"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "security-ir.amazonaws.com"
  }
 }
}
```

為 指定委派管理員 AWS 安全事件應變

本節提供在 AWS 安全事件應變 組織中指定委派管理員的步驟。

身為 AWS 組織的管理員，請務必閱讀委派安全事件回應管理員帳戶的運作考量事項和建議方式。在繼續之前，請確定您擁有 指定委派安全事件回應管理員帳戶所需的許可。

選擇偏好的存取方法，為您的組織指定委派的安全事件回應管理員帳戶。只有 管理才能執行此步驟。

Console

1. 在 https：//https://console.aws.amazon.com/security-ir/ 開啟安全事件回應主控台

若要登入，請使用 AWS Organizations 組織的管理憑證。

2. 使用頁面右上角的 AWS 區域 選取器，選取您要為組織指定委派安全事件回應管理員帳戶的區域。
3. 遵循設定精靈來建立您的成員資格，包括委派的管理員帳戶。

API/CLI

- 使用 AWS 帳戶 組織管理的 登入資料執行 CreateMembership。
  - 或者，您可以使用 AWS Command Line Interface 來執行此操作。下列 AWS CLI 命令會指定委派的安全事件回應管理員帳戶。以下是可用於設定成員資格的字串選項：

```
{
  "customerAccountId": "stringstring",
  "membershipName": "stringstring",
  "customerType": "Standalone",
  "organizationMetadata": {
    "organizationId": "string",
    "managementAccountId": "stringstring",
    "delegatedAdministrators": [
      "stringstring"
    ]
  },
  "membershipAccountsConfigurations": {
    "autoEnableAllAccounts": true,
    "organizationalUnits": [
      "string"
    ]
  },
  "incidentResponseTeam": [
    {
      "name": "string",
      "jobTitle": "stringstring",
      "email": "stringstring"
    }
  ],
  "internalIdentifier": "string",
  "membershipId": "stringstring",
  "optInFeatures": [
    {
      "featureName": "RuleForwarding",
```

```
        "isEnabled": true
      }
    ]
  }
```

如果 AWS 安全事件應變 未針對委派的安全事件回應管理員帳戶啟用 ，則無法採取任何動作。如果尚未這樣做，請務必 AWS 安全事件應變 為新指定的安全事件回應管理員帳戶啟用 。

將成員新增至 AWS 安全事件應變

與 AWS Organizations 和您的 AWS 安全事件應變 成員有一對一的關係。從 Organizations 中新增（或移除）帳戶時，這將反映在您的 AWS 安全事件應變 成員資格的涵蓋帳戶中。

若要將 帳戶新增至您的成員資格，請遵循使用 管理 組織中帳戶的 AWS Organizations其中一個選項。

從 移除成員 AWS 安全事件應變

若要從您的成員資格中移除帳戶，請遵循從組織中移除成員帳戶的程序。

Amazon EventBridge

使用 Amazon EventBridge，您可以反應、監控和協調與 AWS 安全事件應變 案例和成員資格相關的事件。您可以透過規則（適用於擴增案例到一或多個目標）或透過管道（適用於具有增強篩選、擴充和轉換功能的point-to-point整合）路由這些事件。

您可以在安全事件回應與第三方工具之間建立整合，或使用生成式 AI 和其他 AWS 工具彙總資料分析。例如，當安全事件回應主動建立案例時，您可以使用 EventBridge 自動化來觸發系統來通知利益相關者。此外，如果您管理多個 AWS 環境，您可以使用 Amazon EventBridge 整合來監控 AWS 安全事件應變 成員資格，以確保所有環境都維持強大的安全狀態。

如需詳細資訊，您可以檢閱什麼是 Amazon EventBridge？

目錄

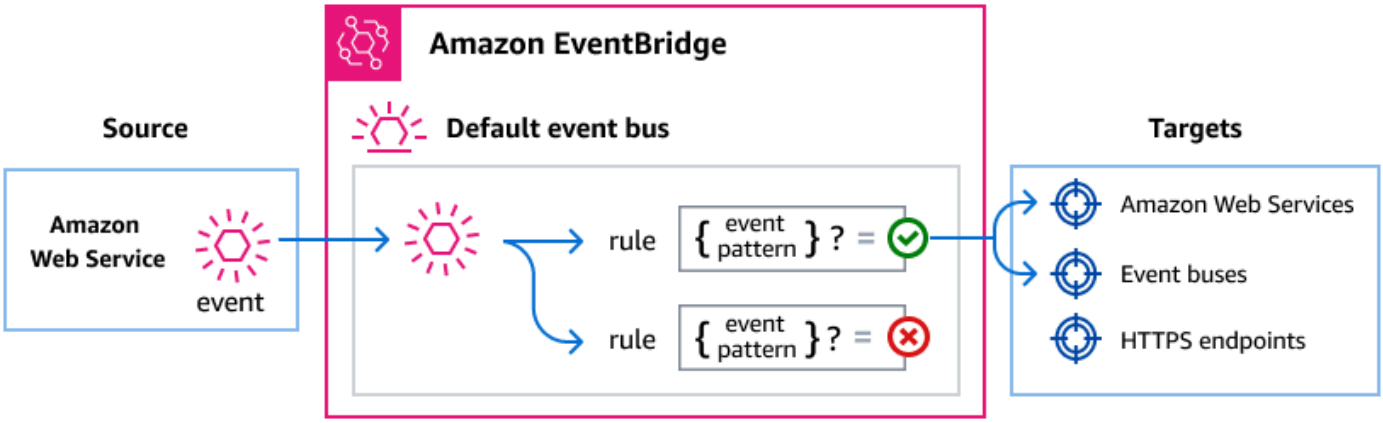
- 使用 Amazon EventBridge 管理安全事件回應事件
- 使用 AWS 安全事件應變 事件
- 教學課程：傳送Membership Updated事件的 Amazon Simple Notification Service 提醒

使用 Amazon EventBridge 管理安全事件回應事件

Amazon EventBridge 是一種無伺服器服務，該服務使用事件將應用程式元件連接在一起，讓您更輕鬆地建置可擴展的事件驅動型應用程式。事件驅動型架構是一種建置鬆耦合軟體系統的方式，透過發出和回應事件來協作。事件代表資源或環境中的變更。

以下是其運作方式：

如同許多 AWS 服務，安全事件回應會產生事件並將其傳送至 EventBridge 預設事件匯流排。（預設事件匯流排會自動在您的 AWS 帳戶中佈建。）事件匯流排是接收事件，並將事件傳遞至零個或多個目的地或目標的路由器。您為事件匯流排指定的規則會在事件到達時評估事件。每個規則會檢查事件是否符合規則的事件模式。如果事件確實相符，事件匯流排會將事件傳送至指定的目標 (s)。



使用 EventBridge 規則傳遞安全事件回應事件

若要讓 EventBridge 預設事件匯流排將安全事件回應事件傳送至目標，您必須建立規則。每個規則都包含事件模式，EventBridge 會比對事件匯流排上收到的每個事件。如果事件資料符合指定的事件模式，EventBridge 會將該事件交付到規則的目標 (s)。

如需建立事件匯流排規則的完整說明，請參閱《Amazon EventBridge 使用者指南》中的建立對事件做出反應的規則。

建立符合安全事件回應事件的事件模式

每個事件模式都是 JSON 物件，其中包含：

- 識別傳送事件之服務的 `source` 屬性。對於安全事件回應事件，來源為 `"aws.security-ir"`。
- (選擇性)：包含要比對之事件類型陣列的 `detail-type` 屬性。
- (選擇性)：包含要比對的任何其他事件資料的 `detail` 屬性。

例如，下列事件模式符合指定 的所有`Case Updated by AWS ###### Service`事件 AWS 帳戶：

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
```

```
                "region": "us-west-2",
                "resources": [
                  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
                ],
                "detail": {
                  "caseId": "1234567890",
                  "updatedBy": "security-ir.amazonaws.com"
                }
              }
```

如需撰寫事件模式的詳細資訊，請參閱《EventBridge 使用者指南》中的事件模式。 EventBridge

安全事件回應事件詳細資訊參考

AWS 服務中的所有事件都有一組通用的欄位，其中包含事件的中繼資料，例如事件來源 AWS 的服務、事件產生的時間、事件發生的帳戶和區域，以及其他。如需這些一般欄位的定義，請參閱《Amazon EventBridge 使用者指南》中的事件結構描述參考。

此外，每個事件都有一個 `detail` 欄位，其中包含該特定事件的特定資料。以下參考定義了各種安全事件回應事件的詳細資訊欄位。

使用 EventBridge 來選取和管理安全事件回應事件時，請謹記下列事項：

- 來自安全事件回應的所有事件的 `source` 欄位設定為 `"aws.security-ir"`。
- `detail-type` 欄位指定事件類型。

  例如 `"Case Updated"`。
- `detail` 欄位包含該特定事件的特定資料。

如需有關建構事件模式以讓規則符合安全事件回應事件的資訊，請參閱《Amazon EventBridge 使用者指南》中的事件模式。

如需事件及其處理方式的詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的 EventBridge 事件。 EventBridge EventBridge

常見欄位：所有 AWS 安全事件應變 事件都包含這些標準 Amazon EventBridge 欄位

- 版本：EventBridge 事件格式版本
- id：事件的唯一識別符

- detail-type：事件類型的人類可讀描述
- 來源：安全事件回應事件一律為 "aws.security-ir"
- 事件發生的帳戶： AWS 帳戶 ID
- 時間：事件發生時的 ISO 8601 時間戳記
- region： AWS 區域 資源的存在位置
- 資源：包含受影響資源 ARN 的陣列

詳細資訊欄位： `detail` 物件包含安全事件回應特定資訊

- caseId：案例的唯一識別符 （僅限案例事件）
- membershipId：成員資格的唯一識別符 （僅限成員事件）
- updatedBy：誰執行更新 （僅限案例和評論更新事件）
- createdBy：建立實體的人員 （僅限案例和評論建立事件）

演員值： `updatedBy`和 `createdBy` 欄位可包含

- AWS 回應者：由 AWS 安全回應者執行的動作
- *`security-ir.amazonaws.com`*：服務自動執行的動作
- 帳戶 ID：客戶執行的動作 （例如 "111122223333")

資源 ARN 值： AWS 安全事件應變 資源使用這些 ARN 格式

- 案例： `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- 成員資格： `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

案例事件

AWS 回應者建立的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
```

```
            "source": "aws.security-ir",
            "account": "111122223333",
            "time": "2023-05-12T00:00:00Z",
            "region": "us-west-2",
            "resources": [
              "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
            ],
            "detail": {
              "caseId": "1234567890",
              "createdBy": "AWS Responder"
            }
          }
```

服務建立的案例

```
          {
            "version": "0",
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "detail-type": "Case Created",
            "source": "aws.security-ir",
            "account": "111122223333",
            "time": "2023-05-12T00:00:00Z",
            "region": "us-west-2",
            "resources": [
              "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
            ],
            "detail": {
              "caseId": "1234567890",
              "createdBy": "security-ir.amazonaws.com"
            }
          }
```

客戶建立的案例

```
          {
            "version": "0",
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "detail-type": "Case Created",
            "source": "aws.security-ir",
```

```
    "account": "111122223333",
    "time": "2023-05-12T00:00:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "111122223333"
    }
  }
```

AWS 回應者更新的案例

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T01:30:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "AWS Responder"
    }
  }
```

AWS 客戶更新的案例

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
```

```
    "time": "2023-05-12T02:15:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "111122223333"
    }
  }
```

AWS 安全事件應變 Service 更新的案例

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T03:45:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "security-ir.amazonaws.com"
    }
  }
```

案例已關閉

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Closed",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-15T14:22:00Z",
```

```
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890"
    }
  }
```

案例評論事件

AWS 回應者建立的案例評論

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Comment Created",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T04:30:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "AWS Responder"
    }
  }
```

客戶建立的案例評論

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Comment Created",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T02:15:00Z",
```

```
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "111122223333"
    }
  }
```

AWS 安全事件應變 服務建立的案例評論

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Comment Created",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T02:15:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "security-ir.amazonaws.com"
    }
  }
```

客戶更新的案例評論

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Comment Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T02:45:00Z",
    "region": "us-west-2",
```

```
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "111122223333"
    }
  }
```

AWS 安全事件應變 服務更新的案例評論

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Comment Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T02:45:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "security-ir.amazonaws.com"
    }
  }
```

AWS 回應者建立的案例評論

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Comment Updated",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T02:45:00Z",
    "region": "us-west-2",
    "resources": [
```

```
                "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
              ],
              "detail": {
                "caseId": "1234567890",
                "updatedBy": "AWS Responder"
              }
            }
```

成員事件

成員資格已建立

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Created",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-01T10:00:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

成員資格已更新

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Updated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-15T16:30:00Z",
              "region": "us-west-2",
```

```
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membership Id": "m-1234567890abcdef0"
              }
            }
```

已取消成員資格

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Closed",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-06-30T23:59:59Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membership Id": "m-1234567890abcdef0"
              }
            }
```

成員資格已終止

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Terminated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-07-01T00:00:00Z",
              "region": "us-west-2",
              "resources": [
```

```
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

使用 AWS 安全事件應變 事件

您可以建立 EventBridge 規則以符合這些事件並觸發自動動作。以下是一些範例使用案例：

比對所有 AWS 安全事件應變 事件：

```
{
  "source": ["aws.security-ir"]
}
```

僅比對案例事件：

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

AWS 回應者更新的相符案例：

```
{
  "source": ["aws.security-ir"],
```

```
            "detail-type": ["Case Updated"],
            "detail": {
              "updatedBy": ["AWS Responder"]
            }
          }
```

符合特定案例的事件：

```
          {
            "source": ["aws.security-ir"],
            "detail": {
              "caseId": ["1234567890"]
            }
          }
```

教學課程：傳送`Membership Updated`事件的 Amazon Simple Notification Service 提醒

在本教學課程中，您會設定 Amazon EventBridge 事件規則，該規則只會擷取訂閱進入 `Membership Updated` 狀態的事件。

先決條件

本教學假設您的成員資格中有有效的訂閱和作用中 AWS 的帳戶。

主題

- 教學課程：建立和訂閱 Amazon SNS 主題
- 教學課程：註冊事件規則
- 教學課程：測試您的規則
- 替代規則：安全事件回應案例更新

教學課程：建立和訂閱 Amazon SNS 主題

在此教學課程中，您會設定 Amazon SNS 主題，做為新事件規則的事件目標。

建立 Amazon SNS 主題

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 選擇 Topics (主題)、Create topic (建立主題)。
3. 針對類型，選擇標準。
4. 針對名稱，輸入 **`MembershipUpdated`** 並選擇建立主題。
5. 在 MembershipUpdated 畫面上，選擇建立訂閱。
6. 對於通訊協定，選擇電子郵件。
7. 對於 Endpoint (端點)，輸入您目前能存取的電子郵件地址，並選擇 Create subscription (建立訂閱)。
8. 檢查您的電子郵件帳戶，並等待收到訂閱確認的電子郵件訊息。您收到訊息時，請選擇 Confirm subscription (確認訂閱)。

教學課程：註冊事件規則

接著，註冊僅擷取事件的事件規則`Membership Updated`。

註冊您的 EventBridge 規則

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
4. 輸入規則的名稱和描述。

> **Note**
>
> 在同一個區域和同一個事件匯流排上，規則不能與另一個規則同名。

5. 針對事件匯流排，選擇要與此規則建立關聯的事件匯流排。如果您想要此規則匯配來自您的帳戶的事件，請選取 AWS 預設事件匯流排。當您帳戶中的 AWS 服務發出事件時，一律會前往您帳戶的預設事件匯流排。

> **Note**
>
> 這應該在您建立 AWS 安全事件應變 成員資格的 AWS Organizations 或委派管理員帳戶中設定。

6. 針對規則類型，選擇具有事件模式的規則。
7. 選擇下一步。
8. 在事件來源中，選擇其他。
9. 針對事件模式，選取自訂模式 (JSON 編輯器）。
10. 將下列的事件模式貼到文字區域。

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

此程式碼會定義 EventBridge 規則，以符合更新或修改服務成員資格的任何事件。如需事件模式的詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的事件和事件模式。

11. 選擇下一步。
12. 在目標類型欄位中，選擇 AWS 服務。
13. 針對選取目標，選擇 SNS 主題，針對主題，選擇 MembershipUpdated。
14. (選用) 針對其他設定，請執行下列動作：
    a. 針對 Maximum age of event (事件的最長存留期)，輸入介於一分鐘 (00:01) 到 24 小時 (24:00) 之間的某個值。
    b. 針對重試嘗試，輸入介於 0 到 185 之間的某個數。
    c. 針對無效字母佇列，選擇是否使用標準 Amazon SQS 佇列做為無效字母佇列。若與此規則匹配的事件未成功傳送到目標，則 EventBridge 會將其傳送至無效字母佇列。執行以下任意一項：
       - 選擇無，即不使用無效字母佇列。
       - 選擇目前 AWS 帳戶中的選取 Amazon SQS 佇列以用作無效字母佇列，然後從下拉式清單中選取要使用的佇列。
       - 選擇在其他 AWS 帳戶中選取 Amazon SQS 佇列做為無效字母佇列，然後輸入要使用的佇列 ARN。您必須將以資源為基礎政策連接到佇列，而且該佇列授與 EventBridge 向其傳送簡訊的許可。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的授與無效字母佇列的許可。
15. 選擇下一步。

16. (選用) 為規則輸入一或多個標籤。如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的 Amazon EventBridge 標籤。
17. 選擇下一步。
18. 檢閱規則的詳細資訊，然後選擇建立規則。

教學課程：測試您的規則

若要測試您的規則，請提交您的 AWS 安全事件應變 成員資格更新。如果您的規則設定正確，您應該會在幾分鐘內收到包含事件文字的電子郵件訊息。

替代規則：安全事件回應案例更新

若要建立監控所有案例更新的事件規則，請使用下列變更重複這些教學課程：

1. 在 教學課程：建立和訂閱 Amazon SNS 主題 中，使用 *CaseUpdates* 做為主題名稱。
2. 在 教學課程：註冊事件規則 中，在 JSON 編輯器中使用下列模式：

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

疑難排解

當您遇到與執行特定動作相關的問題時 AWS 安全事件應變，請參閱本節中的主題。

ERROR 是表示部分或全部操作中故障的操作狀態。或者，當發生問題但任務仍然完成時，您會收到警告。

目錄

- 問題
- 錯誤
- 支援

問題

未傳送來自正確內容的請求。

所有對 AWS 安全事件應變 APIs呼叫都必須來自服務委派管理員或成員資格帳戶中的 IAM 主體。請確定您在 中從正確的 IAM 主體操作 AWS 帳戶 ，而該主體是您組織的 AWS 安全事件應變 委派管理員或成員資格帳戶。

錯誤

AccessDeniedException

您沒有足夠存取權可執行此動作。

請與您的 AWS 管理員合作，以確保您具有在 AWS 安全事件應變 委派管理員或成員資格帳戶中擔任 IAM 角色的許可。同時檢查角色是否具有允許所請求動作的 IAM 政策。如需詳細資訊，請參閱 AWS 安全事件應變 IAM。

ConflictException

請求會導致不一致的狀態。

請檢查您指定的任何案例附件檔案名稱或預設回應團隊成員是否是唯一的。同時檢查您的AWS 安全事件應變 服務成員資格是否尚未設定。在 https：//https://console.aws.amazon.com/security-ir/ 開啟安全事件回應主控台，然後導覽至 `Membership Details`。

InternalServerException

處理請求期間發生非預期的錯誤。請在幾分鐘後再試一次。如果問題仍然存在，請使用 提出案例 支援。

ResourceNotFoundException

請求參考不存在的資源。

請求中指定的一或多個資源不存在。請檢查所有指定的資源 ARNs或 IDs是否正確。這適用於 AWS Organizations IDs、帳戶 IDs、IAM 角色、成員資格、案例、回應團隊成員、案例、案例回應者、案例附件和案例評論。

ThrottlingException

由於請求調節，因此請求遭到拒絕。

您的 IAM 主體在指定期間內向該 API 函數提出了太多請求。請稍候，然後再試一次。如果問題仍然存在，請考慮實作指數退避和重試演算法。

ValidationException

輸入無法滿足 指定的限制條件 AWS 服務。

請求中的一或多個資料欄位不符合驗證和/或邏輯組合要求。請檢查所有資源 ARNs是否已完成，以及文字值是否符合 AWS 安全事件應變 API 參考指南中的大小和格式限制。同時檢查是否允許任何值更新。例如，無法將案例從 AWS 支援變更為自我管理。

支援

如果您需要其他協助，請聯絡 支援 中心進行故障診斷。請備妥下列資訊：

- 您使用 AWS 區域 的
- 成員資格的 AWS 帳戶 ID
- 您的來源內容，如果適用且可用
- 可能有助於故障診斷的問題的任何其他詳細資訊

安全

目錄

- 中的資料保護 AWS 安全事件應變
- 網際網路流量隱私權
- 身分和存取權管理
- 對 AWS 安全事件應變 身分和存取進行故障診斷
- 使用服務角色
- 使用服務連結角色
- AWS 受管政策
- 事件回應
- 法規遵循驗證
- 在 AWS 安全事件回應中記錄和監控
- 恢復能力
- 基礎架構安全
- 組態與漏洞分析
- 預防跨服務混淆代理人

中的資料保護 AWS 安全事件應變

目錄

- 資料加密

AWS 共同責任模型適用於安全事件回應服務的資料保護 AWS 。如此模型所述， AWS 負責保護執行 AWS 雲端中所提供服務的基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責所使用 AWS 服務的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全部落格上的 AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的， AWS 安全最佳實務狀態為您應該保護 AWS 帳戶登入資料，並使用 IAM Identity Center AWS 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者只會獲得完成其工作職責所需的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務中的所有預設安全控制。
- 服務目前不支援 FIPS 140-3。

您絕不應將機密或敏感資訊，例如您的電子郵件地址，放入標籤或任意格式的文字欄位中，例如名稱欄位。這包括當您使用 AWS 支援或使用主控台、API、 AWS CLI 或 AWS SDKs的其他 AWS 服務時。您輸入用於名稱的標籤或任意格式文字欄位的任何資料都可用於帳單或診斷日誌。如果您提供 URL 給外部伺服器，我們強烈建議您不要在 URL 中包含登入資料資訊，以驗證您對該伺服器的請求。

資料加密

目錄

- 靜態加密
- 傳輸中加密
- 金鑰管理

靜態加密

靜態資料使用透明的伺服器端加密功能加密。這可協助降低保護敏感資料所涉及的操作負擔和複雜性。您可以透過靜態加密，建立符合加密合規和法規要求，而且對安全性要求甚高的應用程式。

傳輸中加密

收集和存取的資料 AWS 安全事件應變 僅透過 Transport Layer Security (TLS) 保護的頻道。

金鑰管理

AWS 安全事件應變 實作與 的整合 AWS KMS ，為案例和連接資料提供靜態加密。

AWS 安全事件應變 不支援客戶受管金鑰。

網際網路流量隱私權

服務和內部部署用戶端與應用程式之間的流量。

您的私有網路與 之間有兩個連線選項 AWS：

- AWS Site-to-Site VPN 連線。如需詳細資訊，請參閱《 AWS Site-to-Site VPN使用者指南》中的什麼是AWS Site-to-Site VPN ？。
- AWS Direct Connect 連線。如需詳細資訊，請參閱《 AWS Direct Connect使用者指南》中的什麼是AWS Direct Connect ？。

AWS 安全事件應變 透過網路存取 是透過 AWS 發佈APIs。用戶端必須支援 Transport Layer Security (TLS) 1.2。我們建議使用 TLS 1.3。用戶端也必須支援具備完整轉寄密碼 (PFS) 的密碼套件，例如暫時性 Diffie-Hellman (DHE) 或橢圓曲線 Diffie-Hellman Ephemeral (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。此外，您必須使用存取金鑰 ID，以及與 IAM 委託人相關聯的私密存取金鑰來簽署請求，或者您可以使用 AWS Security Token Service (STS) 來產生臨時安全憑證來簽署請求。

相同區域中 AWS 資源間的流量

的 Amazon Virtual Private Cloud (Amazon VPC) 端點 AWS 安全事件應變 是 VPC 內的邏輯實體，僅允許連線 AWS 安全事件應變。Amazon VPC 會將請求路由至 ， AWS 安全事件應變 並將回應路由回 VPC。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 端點。如需可從 VPC 端點控制存取權限的政策範例，請參閱使用 IAM 政策控制對 DynamoDB 的存取。

> **Note**
>
> Amazon VPC 端點無法透過 AWS Site-to-Site VPN 或 存取 AWS Direct Connect。

身分和存取權管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員控制對 AWS 資源的存取。IAM 管理員控制已驗證 （已登入） 和已授權 （具有許可） 主體來使用 AWS 安全事件應變 資源。IAM 是一項服務 AWS ，您可以免費使用。

目錄

- 使用身分驗證
- 如何使用 AWS 安全事件應變 IAM

對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，具體取決於您在其中執行的工作 AWS 安全事件應變。

安全管理員

建議這些使用者使用 AWSSecurityIncidentResponseFullAccess 受管政策，以確保他們具有成員資格和案例資源的讀取和寫入存取權。

案例監看器

這些人員無權存取所有案例，但您授予明確許可的個別案例除外。

事件回應團隊成員

團隊成員可以同時獲得完整的成員資格和案例存取權。建議並非所有個人都對服務成員資格採取授權動作，但應該能夠存取透過服務建立和管理的任何和所有案例。如需詳細資訊，請參閱 AWS 安全事件應變 受管政策。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （登入 AWS)。

您可以使用透過身分來源提供的登入資料，以聯合身分 AWS 的形式登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS 管理主控台或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入使用者指南中的如何登入 AWS 您的帳戶。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用哪種身分驗證方法，都可能需要提供額外的安全性資訊。例如， AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。若要進一步了解，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的使用多重要素驗證 (MFA) AWS。

AWS 帳戶根使用者

當您建立 AWS 帳戶時，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶群組使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。切勿將根使用者用於您的日常任務，並採取步驟來保護根使用者憑證。只用來執行只有根使用者可以執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者，包括需要管理員存取權的使用者，使用 聯合身分提供者來使用臨時憑證來存取 AWS 服務。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、Identity Center 目錄或任何使用透過身分來源提供的登入資料存取 AWS 服務的使用者。當聯合身分存取 AWS 帳戶時，它們會擔任 角色，而角色會提供臨時登入資料。

對於集中式存取管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接並同步到您自己的身分來源中的一組使用者和群組，以便在所有 AWS 帳戶和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱《IAM Identity Center 使用者指南》中的什麼是 IAM Identity Center？。AWS

IAM 使用者和群組

IAM 使用者是您 AWS 帳戶中的身分，具有單一人員或應用程式的特定許可。我們建議依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證的 IAM 使用者。如果您有需要 IAM 使用者長期登入資料的特定使用案例，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

AnIAM 群組是指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要進一步了解，請參閱《IAM 使用者指南》中的何時建立 IAM 使用者（而非角色）。

IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，暫時在 AWS 管理主控台中擔任 IAM 角色。您可以透過呼叫 CLI AWS 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要將許可指派給聯合身分，您可以建立角色並定義角色的許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，您可以設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與

IAM 中的角色相關聯。如需許可集的詳細資訊，請參閱《AWS IAM Identity Center 使用者指南》中的許可集。

- 臨時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM 角色，允許不同帳戶中的某人（信任的委託人）存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以將政策直接連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務使用其他服務中的功能 AWS 。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 服務角色 – 服務角色是服務擔任以代表您執行動作的 IAM 角色。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 – 服務連結角色是連結至 服務的一種 AWS 服務角色。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的帳戶中 AWS ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並將其提供給其應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解如何使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的何時建立 IAM 角色（而非使用者）。

如何使用 AWS 安全事件應變 IAM

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可），以使用 AWS 安全事件回應資源。IAM 是一項服務 AWS ，您可以免費使用。

可與 AWS 安全事件回應搭配使用的 IAM 功能	
IAM 功能	服務對齊

可與 AWS 安全事件回應搭配使用的 IAM 功能	
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是（全球）
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	否
服務連結角色	是

目錄

- 的身分型政策 AWS 安全事件應變
- 安全 AWS 事件回應的政策條件索引鍵
- AWS 安全事件應變中的存取控制清單 (ACL)

的身分型政策 AWS 安全事件應變

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

目錄

- 身分型政策範例
- 政策最佳實務
- 使用 AWS 安全事件應變 主控台
- 允許使用者檢視他們自己的許可
- 資源型政策
- 政策動作

身分型政策範例

根據預設，使用者和角色沒有建立或修改 AWS 安全事件應變 資源的許可。他們也無法使用 AWS 管理主控台、 AWS 命令列界面 (AWS CLI) 或 AWS API 來執行任務。IAM 管理員可以建立 IAM 政策，授予使用者對所需資源執行動作的許可。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需安全事件回應所定義 AWS 之動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS 安全事件應變。

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 AWS 安全事件應變 資源。這些動作可能會對您的帳戶產生成本 AWS 。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的帳戶中使用 AWS 。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。

套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。

使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過 AWS CloudFormation 等特定

服務使用 AWS 服務動作，您也可以使用條件來授予服務動作的存取權。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。

使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 AWS 帳戶中的根使用者，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 AWS 安全事件應變 主控台

若要存取 https://console.aws.amazon.com/security-ir/，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 AWS 帳戶中資源的詳細資訊 AWS 安全事件應變 。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 CLI 或 AWS API AWS 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

連接 AWS 安全事件應變 Access 或 ReadOnly AWS 受管政策，以確保使用者和角色可以使用 服務主控台。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台上完成此動作的許可，或使用 CLI 或 AWS API AWS 以程式設計方式完成此動作的許可。

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "ViewOwnUserInfo",
"Effect": "Allow",
"Action": [
"iam:GetUserPolicy",
"iam:ListGroupsForUser",
"iam:ListAttachedUserPolicies",
"iam:ListUserPolicies",
```

```
"iam:GetUser"
],
"Resource": ["arn:AWS:iam::*:user/${AWS:username}"]
},
{
"Sid": "NavigateInConsole",
"Effect": "Allow",
"Action": [
"iam:GetGroupPolicy",
"iam:GetPolicyVersion",
"iam:GetPolicy",
"iam:ListAttachedGroupPolicies",
"iam:ListGroupPolicies",
"iam:ListPolicyVersions",
"iam:ListPolicies",
"iam:ListUusers"
],
"Resource": "*"
}
]
}
```

資源型政策

AWS 安全事件回應中的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定委託人。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

政策動作

的政策動作 AWS 安全事件應變

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的動作元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS 安全事件應變 動作清單，請參閱《服務授權參考 AWS 安全事件應變 》中的 定義的動作。

中的政策動作在動作之前 AWS 安全事件應變 使用以下字首：

AWS 安全事件應變 -身分

若要在單一陳述式中指定多個動作，請用逗號分隔。

"動作"： 【 "AWS 安全事件應變 -identity：action1"， "AWS 安全事件應變 -identity：action2" 】

Amazon AWS 安全事件回應的政策資源

支援政策資源：是 管理員可以使用 AWS JSON 政策來指定可存取內容的人員。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

資源 JSON 政策元素會指定套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

"Resource": "*"

安全 AWS 事件回應的政策條件索引鍵

支援服務特定的政策條件索引鍵：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 （或 Condition 區塊) 可讓您指定陳述式生效的條件。Condition 元素是可選用的。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

如果您在陳述式中指定多個條件元素，或在單一條件元素中指定多個索引鍵， 會使用邏輯 AND 操作 AWS 來評估它們。如果您為單一條件索引鍵指定多個值， 會使用邏輯 OR 操作 AWS 來評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

AWS 安全事件應變中的存取控制清單 (ACL)

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

具有 AWS 安全事件回應的屬性型存取控制 (ABAC)

支援 ABAC （政策中的標籤）：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色)，以及許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。然後，您可以設計 ABAC 政策，以便在委託人的標籤與其嘗試存取的資源上的標籤相符時允許操作。ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

若要根據標籤控制存取，您可以使用 AWS：ResourceTag/key-name、 AWS：RequestTag/key-name 或 AWS：TagKeys 條件金鑰，在政策的條件元素中提供標籤資訊。如果服務支援每個資源類型的所有三個條件金鑰，則服務的值為是。如果服務僅支援某些資源類型的全部三個條件索引鍵，則值為部分。如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC？。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的使用屬性型存取控制 (ABAC)。

具有 Amazon AWS 安全事件回應的臨時登入資料

支援臨時憑證：是

AWS 當您使用暫時登入資料登入時， 服務無法運作。如需詳細資訊，包括哪些 AWS 服務使用臨時登入資料，請參閱《AWS IAM 使用者指南》中的使用 IAM 的服務。如果您使用使用者名稱和密碼以外的任何方法登入 AWS 管理主控台，則使用臨時登入資料。 例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的切換至角色 (主控台)。

您可以使用 CLI 或 AWS API 手動建立臨時登入資料 AWS 。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

轉送 AWS 安全事件回應的存取工作階段

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 AWS 服務的委託人許可，結合請求 AWS 服務，向下游服務提出請求。只有在服務收到需要與其他 AWS 服務或資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

對 AWS 安全事件應變 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AWS 安全事件回應和 IAM 時可能遇到的常見問題。

主題

- 我未獲得執行動作的授權
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 AWS 安全事件應變 資源

我未獲授權執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當 mateojackson IAM 使用者嘗試使用主控台檢視虛構 my-example-widget 資源的詳細資訊，但沒有虛構 AWS 安全事件回應 ：GetWidget 許可時，會發生下列範例錯誤。

使用者：arn：AWS：iam： ：123456789012：user/mateojackson 未獲授權執行：AWS 安全事件應變 ：GetWidgeton 資源：my-example-widget

在此情況下，必須更新 mateojackson 使用者的政策，以允許使用 AWS 安全事件應變 ：GetWidget 動作存取 my-example-widget 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我無權執行 iam：PassRole 如果您收到錯誤，告知您無權執行 iam：PassRole 動作，您的政策必須更新，以允許您傳遞角色 AWS 安全事件應變 。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在安全事件回應 中 AWS 執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

使用者：arn：AWS：iam：：123456789012：user/marymajor 未獲授權執行：iam：PassRole

在這種情況下，Mary 的政策必須更新，以允許她執行 iam：PassRole 動作。如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人員存取我的 AWS 安全事件回應資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon AWS 安全事件應變 是否支援這些功能，請參閱 AWS 安全事件回應如何與 IAM 搭配使用。
- 若要了解如何在您擁有的帳戶中 AWS 提供資源的存取權，請參閱《IAM 使用者指南》中的為您擁有的另一個 AWS 帳戶中的 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方擁有 AWS 的帳戶。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

使用服務角色

支援服務角色：否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以將許可委派給 AWS 服務。

使用服務連結角色

的服務連結角色 AWS 安全事件應變

目錄

- AWS SLR：AWSServiceRoleForSecurityIncidentResponse

- AWS SLR：AWSServiceRoleForSecurityIncidentResponse_Triage
- AWS 安全事件應變 服務連結角色支援的區域

支援服務連結角色：是

服務連結角色是連結至 服務的一種 AWS 服務角色。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 AWS 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

服務連結角色可讓您更 AWS 安全事件應變 輕鬆地設定，因為您不必手動新增必要的許可。 AWS 安全事件應變 會定義其服務連結角色的許可，除非另有定義，否則 AWS 安全事件應變 只能擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

如需有關支援服務連結角色的其他 服務的資訊，請參閱AWS 使用 IAM 的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AWS SLR：AWSServiceRoleForSecurityIncidentResponse

AWS 安全事件應變 使用名為 AWSServiceRoleForSecurityIncidentResponse – AWS 安全事件應變 policy 的服務連結角色 (SLR) 來識別訂閱的帳戶、建立案例和標記相關資源。

許可

AWSServiceRoleForSecurityIncidentResponse 服務連結角色信任下列服務擔任該角色：

- `triage.security-ir.amazonaws.com`

連接至此角色是名為 AWSSecurityIncidentResponseServiceRolePolicy 的 AWS 受管政策。服務會使用 角色對下列資源執行動作：

- AWS Organizations：允許服務查詢成員資格帳戶以搭配服務使用。
- CreateCase：允許服務代表成員資格帳戶建立服務案例。
- TagResource：允許將 服務標籤資源設定為服務的一部分。

管理角色

您不需要手動建立一個服務連結角色。當您在 AWS CLI、 或 AWS API AWS Management Console AWS 安全事件應變 中加入至 時，服務會為您建立服務連結角色。

> **Note**
>
> 如果您使用委派管理員帳戶建立成員資格，則需要在 AWS Organizations 管理帳戶中手動建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您加入服務時，它會再次為您建立服務連結角色。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

AWS SLR：AWSServiceRoleForSecurityIncidentResponse_Triage

AWS 安全事件應變 使用名為 AWSServiceRoleForSecurityIncidentResponse_Triage – AWS 安全事件應變 政策的服務連結角色 (SLR)，持續監控您的環境是否有安全威脅、調校安全服務以減少警示雜訊，以及收集資訊以調查潛在事件。

許可

AWSServiceRoleForSecurityIncidentResponse_Triage 服務連結角色信任下列服務擔任該角色：

- `triage.security-ir.amazonaws.com`

連接到此角色是 AWS 受管政策 AWSSecurityIncidentResponseTriageServiceRolePolicy。服務會使用角色對下列資源執行動作：

- 事件：允許服務建立 Amazon EventBridge 受管規則。此規則是您 AWS 帳戶中將事件從您的帳戶交付至 服務所需的基礎設施。此動作會在 管理的任何 AWS 資源上執行`triage.security-ir.amazonaws.com`。
- Amazon GuardDuty：允許服務調校安全服務，以減少警示雜訊並收集資訊以調查潛在事件。此動作會在任何 AWS 資源上執行。
- AWS Security Hub：允許 服務調整安全服務以減少警示雜訊，並收集資訊以調查潛在事件。此動作會在任何 AWS 資源上執行。

管理角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console AWS CLI、 或 AWS API AWS 安全事件應變 中加入至 時，服務會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您加入服務時，它會再次為您建立服務連結角色。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

AWS 安全事件應變 服務連結角色支援的區域

AWS 安全事件應變 支援在提供服務的所有區域中使用服務連結角色。

- 美國東部 (俄亥俄)
- 美國西部 (奧勒岡)
- 美國東部 (維吉尼亞)
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (巴黎)
- 歐洲 (斯德哥爾摩)
- 亞太區域 (孟買)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太區域 (雪梨)
- 亞太區域 (東京)
- 加拿大 (中部)
- 南美洲 (聖保羅)

AWS 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可

以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並且可在您的帳戶中使用 AWS 。如需 AWS 受管政策的詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 服務會維護和更新其相關聯的 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外， AWS 支援跨多個 服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時， 會為新操作和資源 AWS 新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

目錄

- AWS 受管政策：AWSSecurityIncidentResponseServiceRolePolicy
- AWS 受管政策：AWSSecurityIncidentResponseFullAccess
- AWS 受管政策：AWSSecurityIncidentResponseReadOnlyAccess
- AWS 受管政策：AWSSecurityIncidentResponseCaseFullAccess
- AWS 受管政策：AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWS 安全事件應變 SLRs和 受管政策的更新

AWS 受管政策：AWSSecurityIncidentResponseServiceRolePolicy

AWS 安全事件應變 使用 AWSSecurityIncidentResponseServiceRolePolicy AWS 受管政策。此 AWS 受管政策會連接至 AWSServiceRoleForSecurityIncidentResponse 服務連結角色。此政策提供 的存取權， AWS 安全事件應變 以識別訂閱的帳戶、建立案例和標記相關資源。

> **Important**
>
> 請勿在標籤中存放個人身分識別資訊 (PII) 或其他機密或敏感資訊。 AWS 安全事件應變 會使用標籤來為您提供管理服務。標籤不適用於私有或敏感資料

許可詳細資訊

服務使用此政策對下列資源執行動作：

- AWS Organizations：允許服務查詢成員資格帳戶以搭配服務使用。

- CreateCase：允許服務代表成員資格帳戶建立服務案例。
- TagResource：允許將 服務標籤資源設定為服務的一部分。

您可以在 AWSSecurityIncidentResponseServiceRolePolicy 的 AWS 受管政策中檢視與此政策相關聯的許可。

AWS 受管政策：AWSSecurityIncidentResponseFullAccess

AWS 安全事件應變 使用 AWSSecurityIncidentResponseAdmin AWS 受管政策。此政策會授予服務資源的完整存取權，以及相關 的存取權 AWS 服務。您可以將此政策與 IAM 主體搭配使用，以快速新增的許可 AWS 安全事件應變。

> **Important**
>
> 請勿在標籤中存放個人身分識別資訊 (PII) 或其他機密或敏感資訊。 AWS 安全事件應變 會使用標籤來為您提供管理服務。標籤不適用於私有或敏感資料

許可詳細資訊

服務使用此政策對下列資源執行動作：

- IAM 主體唯讀存取：授予服務使用者對現有 AWS 安全事件應變 資源執行唯讀動作的能力。
- IAM 主體寫入存取：授予服務使用者更新、修改、刪除和建立 AWS 安全事件應變 資源的能力。

您可以在 AWSSecurityIncidentResponseFullAccess 的 AWS 受管政策中檢視與此政策相關聯的許可。

AWS 受管政策：AWSSecurityIncidentResponseReadOnlyAccess

AWS 安全事件應變 使用 AWSSecurityIncidentResponseReadOnlyAccess AWS 受管政策。政策會授予服務案例資源的唯讀存取權。您可以將此政策與 IAM 主體搭配使用，以快速新增 的許可 AWS 安全事件應變。

> **Important**
>
> 請勿在標籤中存放個人身分識別資訊 (PII) 或其他機密或敏感資訊。 AWS 安全事件應變 會使用標籤來為您提供管理服務。標籤不適用於私有或敏感資料

許可詳細資訊

服務使用此政策對下列資源執行動作：

- IAM 主體唯讀存取：授予服務使用者對現有 AWS 安全事件應變 資源執行唯讀動作的能力。

您可以在 AWSSecurityIncidentResponseReadOnlyAccess 的 AWS 受管政策中檢視與此政策相關聯的許可。

AWS 受管政策：AWSSecurityIncidentResponseCaseFullAccess

AWS 安全事件應變 使用 AWSSecurityIncidentResponseCaseFullAccess AWS 受管政策。政策會授予服務案例資源的完整存取權。您可以將此政策與 IAM 主體搭配使用，以快速新增 的許可 AWS 安全事件應變。

> **Important**
>
> 請勿在標籤中存放個人身分識別資訊 (PII) 或其他機密或敏感資訊。 AWS 安全事件應變 會使用標籤來為您提供管理服務。標籤不適用於私有或敏感資料

許可詳細資訊

服務使用此政策對下列資源執行動作：

- IAM 主體案例唯讀存取：授予服務使用者對現有 AWS 安全事件應變 案例執行唯讀動作的能力。
- IAM 主體案例寫入存取：授予服務使用者更新、修改、刪除和建立 AWS 安全事件應變 案例的能力。

您可以在 AWSSecurityIncidentResponseCaseFullAccess 的 AWS 受管政策中檢視與此政策相關聯的許可。

AWS 受管政策：AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS 安全事件應變 使用 AWSSecurityIncidentResponseTriageServiceRolePolicy AWS 受管政策。此 AWS 受管政策會連接至 AWSServiceRoleForSecurityIncidentResponse_Triage 服務連結角色。

此政策提供 的存取權 AWS 安全事件應變 ，以持續監控您的環境是否有安全威脅、調校安全服務以減少警示雜訊，以及收集資訊以調查潛在事件。您無法將此政策連接至 IAM 實體。

> **Important**
>
> 請勿在標籤中存放個人身分識別資訊 (PII) 或其他機密或敏感資訊。 AWS 安全事件應變 會使用標籤來為您提供管理服務。標籤不適用於私有或敏感資料

許可詳細資訊

服務使用此政策對下列資源執行動作：

- 事件：允許服務建立 Amazon EventBridge 受管規則。此規則是您 AWS 帳戶中將事件從您的帳戶交付至 服務所需的基礎設施。此動作會在 管理的任何 AWS 資源上執行`triage.security-ir.amazonaws.com`。
- Amazon GuardDuty：允許服務調校安全服務，以減少警示雜訊並收集資訊以調查潛在事件。此動作會在任何 AWS 資源上執行。
- AWS Security Hub：允許 服務調整安全服務以減少警示雜訊，並收集資訊以調查潛在事件。此動作會在任何 AWS 資源上執行。

您可以在 AWSSecurityIncidentResponseTriageServiceRolePolicy 的 AWS 受管政策中檢視與此政策相關聯的許可。

AWS 安全事件應變 SLRs和 受管政策的更新

檢視自此服務開始追蹤這些變更以來 AWS 安全事件應變 SLRs和 受管政策角色更新的詳細資訊。

變更	描述	日期
更新 SLR 新增許可以支援服務權利。	AWSSecurityIncidentResponseTriageServiceRolePolicy 已更新，以新增 security-ir：GetMembership、 security-ir：ListMemberships、 security-ir：UpdateCase、guarddutyy：ListFilters、guarduty：UpdateFilter、guardduty：DeleteFilter 和 guardduty：GetAdministratorAccount 許可。已新增 guardduty：GetAdministratorAccount，以協助管理委派帳戶中的 GuardDuty Auto-Archival 篩選條件。	2025 年 6 月 2 日
新 SLR – AWSServiceRoleForS	新的服務連結角色和連接政策，允許服務存取您的帳戶 AWS Organizations 以識別成員資格。	2024 年 12 月 1 日

變更	描述	日期
ecurityIncidentResponse 新的受管政策 – AWSSecurityIncidentResponseServiceRolePolicy。		
新 SLR – AWSServiceRoleForSecurityIncidentResponse_Triage 新的受管政策 – AWSSecurityIncidentResponseTriageServiceRolePolicy	新的服務連結角色和連接政策，允許服務存取 AWS Organizations 您的帳戶，以執行安全事件的分類。	2024 年 12 月 1 日
新的受管政策 – AWSSecurityIncidentResponseFullAccess	AWS 安全事件應變 新增 SLR 以連接至 IAM 主體，以執行服務的讀取和寫入動作。	2024 年 12 月 1 日
新的受管政策角色 – AWSSecurityIncidentResponseReadOnlyAccess	AWS 安全事件應變 新增 SLR 以連接至 IAM 主體以進行讀取動作	2024 年 12 月 1 日

變更	描述	日期
新的受管政策角色 – AWSSecurityIncidentResponseCaseFullAccess	AWS 安全事件應變 新增 SLR 以連接至 IAM 主體，以針對服務案例執行讀取和寫入動作。	2024 年 12 月 1 日
已開始追蹤變更。	開始追蹤 AWS 安全事件應變 SLRs和 受管政策的變更	2024 年 12 月 1 日

事件回應

安全與合規是 AWS 和 客戶之間的共同責任。此共用模型有助於減輕客戶的操作負擔，因為 會 AWS 操作、管理和控制從主機作業系統和虛擬化層到服務操作所在設施實體安全性的元件。客戶承擔訪客作業系統（包括更新和安全修補程式）的責任和管理、其他相關聯的應用程式軟體，以及 AWS 所提供安全群組防火牆的組態。如需其他資訊，請參閱 AWS 共同責任模型。

透過建立符合雲端中執行之應用程式目標的安全基準，您可以偵測可回應的偏差。由於安全事件回應可能是一個複雜的主題，因此建議您檢閱下列資源，以便更了解事件回應和您的選擇對您公司目標的影響：AWS 安全最佳實務白皮書，以及AWS 雲端採用架構 (CAF) 的安全觀點白皮書。

法規遵循驗證

在多個合規 AWS 計畫中，第三方稽核人員會評估 服務的安全性和 AWS 合規性。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

AWS 安全事件應變 尚未評估是否符合上述計劃。

如需特定合規計劃範圍內 AWS 的服務清單，請參閱AWS 合規計劃範圍內的服務。如需一般資訊，請參閱 AWS 合規計劃。

您可以使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱在 AWS Artifact 中下載報告。

您使用 AWS 服務的合規責任取決於資料的敏感度、您公司的合規目標，以及適用的 I AWS 和 法規。AWS 提供下列資源來協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供在其中部署以安全與合規為重心的基準環境的步驟 AWS。

- HIPAA 安全與合規架構白皮書 – 此白皮書說明公司如何使用 AWS 來建立符合 HIPAA 規範的應用程式。
- AWS 合規資源 – 適用於產業和/或位置的手冊和指南集合。
- Config AWS 開發人員指南 –Config； 中的使用 Config 規則評估資源，評估資源組態符合內部實務、產業準則和法規的程度。 AWS AWS
- AWS Security Hub – AWS 此服務可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制來評估您的 AWS 資源，並檢查是否符合安全產業標準和最佳實務。如需支援的服務和控制清單，請參閱「Security Hub 控制參考」。
- Amazon GuardDuty – AWS 此服務透過監控您的環境是否有可疑和惡意活動，來偵測對 AWS 您的帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – AWS 此服務可協助您持續稽核 AWS 用量，以簡化您管理風險和符合法規和業界標準的方式。

在 AWS 安全事件回應中記錄和監控

監控是維護 和其他 AWS 解決方案的 AWS 安全事件應變 可靠性、可用性和效能的重要部分。 AWS 安全事件應變 目前支援下列 AWS 服務，以監控您的組織及其內發生的活動。

AWS CloudTrail – 使用 CloudTrail，您可以從 AWS 安全事件回應主控台擷取 API 呼叫。例如，當使用者進行身分驗證時，CloudTrail 可以記錄詳細資訊，例如請求中的 IP 地址、提出請求的人員，以及提出請求的時間。

Amazon CloudWatch 指標 – 使用 CloudWatch 指標，您可以近乎即時地監控、報告，以及在發生事件時採取自動動作。例如，您可以在提供的指標上建立 CloudWatch 儀表板來監控您的 AWS 安全事件應變 用量，或在提供的指標上建立 CloudWatch 警示，以便在違反設定的閾值時通知您。

服務的命名空間是 AWS/Usage/ServiceName。可用的指標名稱為 ActiveManagedCases 和 SelfManagedCases。

根據AWS 服務條款，回應者團隊將有權存取您的 CloudTrail、VPC、DNS AWS 安全事件應變 和 S3 日誌資料歷史記錄。當案例在安全事件回應服務入口網站中開啟時， AWS 可能會在作用中安全事件期間使用此資料。

恢復能力

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用

程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

基礎架構安全

AWS 安全事件應變 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫， AWS 安全事件應變 透過網路存取 。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 產生臨時安全登入資料來簽署請求。

組態與漏洞分析

您負責管理服務遏制角色和相關聯的 AWS CloudFormation 堆疊集。

AWS 處理基本安全任務，例如訪客作業系統 (OS) 和資料庫修補、防火牆組態和災難復原。這些程序已由適當的第三方進行檢閱並認證。如需詳細資訊，請參閱以下 AWS 資源：

- 共同的責任模型
- 安全性、身分與合規的最佳實務

預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在 中 AWS，跨服務模擬可能會導致混淆代理人問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了防止這種情況， AWS 提供工具，協助您保護所有 服務的資料，讓服務主體有權存取您帳戶中的資源。

我們建議在資源政策中使用 AWS：SourceArn 和 AWS：SourceAccount 全域條件內容索引鍵，以限制 Amazon Connect 為資源提供其他服務的許可。如果您同時使用兩個全域條件內容索引鍵， AWS：SourceAccount 值和 AWS：SourceArn 值中的帳戶在相同政策陳述式中使用時，必須使用相同的帳戶 ID。

防範混淆代理人問題的最有效方法是精確使用您允許的資源 Amazon Resource Name (ARN) 資源。如果您不知道資源的完整 ARN 或指定多個資源，請針對 ARN 的未知部分使用 AWS：SourceArn 全域內容條件索引鍵搭配萬用字元 (*)。例如，arn：AWS：servicename：：region-name：：您的 AWS 帳戶 ID：*。

如需示範如何預防混淆代理人問題之擔任角色政策的範例，請參閱混淆代理人預防政策。

Service Quotas

AWS 安全事件應變

下表列出AWS 安全事件應變 的資源配額 AWS 帳戶。在獲得服務管理員核准的情況下，某些配額可能會高於以下所述的配額。除非另有指示，否則以每一區域指定這些配額。

	名稱	預設	可調整	說明
1	作用中 AWS 支援的案例	10	是（最多 50 個）	向 AWS CIRT 請求協助的作用中案例數量。
2	作用中的自我管理案例	50	是（最多 100 個）	在沒有 AWS CIRT 協助的情況下，使用平台的作用中案例數量。
3	在 24 小時內建立的服務支援案例	10	否	從 24 小時滾動時段中建立的 AWS CIRT 請求協助的建立案例數量。
4	預設事件回應團隊中的實體數量上限	10	否	預設事件回應團隊中的實體數量上限。
5	案例上的額外成員數量上限	30	否	與案例相關聯的實體數量上限。這最初會填入來自您預設事件回應團隊的實體。
6	案例附件數量上限	50	是（最多 100 個）	可連接到案例的檔案數量上限。

	名稱	預設	可調整	說明
7	最大案例註解大小	1000	否	案例註解中的字元數上限。
8	Case Attachment 檔案名稱大小上限	255	否	檔案名稱中的字元數上限。

AWS 安全事件應變 技術指南

目錄

- 摘要
- 您是 Well-Architected 嗎？
- 簡介
- 準備
- 作業
- 事後處理
- 結論
- 貢獻者
- 附錄 A：雲端功能定義
- 附錄 B： AWS 事件回應資源
- 注意

摘要

本指南概述在客戶 Amazon Web Services (AWS) 雲端環境中回應安全事件的基本原則。它概述了雲端安全性和事件回應的概念，以及識別要回應安全問題的客戶可使用的雲端功能、服務和機制。

本指南適用於擔任技術角色的人員，並假設您熟悉資訊安全的一般原則、對目前現場部署環境中的安全事件回應有基本的了解，並熟悉雲端服務。

您是 Well-Architected 嗎？

AWS Well-Architected Framework 可協助您了解在雲端建置系統時所做決策的優缺點。架構的六大支柱可讓您學習架構最佳實務，以設計和操作可靠、安全、有效率、經濟實惠且永續的系統。使用AWS Well-Architected Tool在 AWS Well-Architected Tool 主控台中免費提供的 ，您可以透過回答每個支柱的一組問題，根據這些最佳實務來檢閱工作負載。

如需雲端架構的更多專家指引和最佳實務，例如參考架構部署、圖表和白皮書，請參閱AWS 架構中心。

簡介

安全是 AWS .customers 的首要任務 AWS。 客戶受益於建置的資料中心和網路架構，以協助支援最安全敏感組織的需求。 AWS 具有共同的責任模型： AWS 管理雲端的安全性，客戶負責雲端的安全。這表示您可以完全控制安全實作，包括存取數種工具和服務，以協助達成您的安全目標。這些功能可協助您為在 中執行的應用程式建立安全基準 AWS 雲端。

發生與基準的偏差時，例如組態錯誤或外部因素變更，您將需要回應和調查。若要成功執行此作業，您需要了解環境中 AWS 安全事件回應的基本概念，以及在發生安全問題之前準備、教育和訓練雲端團隊的需求。請務必了解您可以使用哪些控制項和功能、檢閱解決潛在問題的主題範例，以及識別使用自動化來改善回應速度和一致性的修補方法。此外，您應該了解您的合規和法規要求，因為它們與建置安全事件回應計劃以滿足這些要求相關。

安全事件回應可能很複雜，因此建議您實作反覆方法：從核心安全服務開始，建置基礎偵測和回應功能，然後開發程序手冊來建立事件回應機制的初始程式庫，以供反覆執行和改善。

開始之前

開始了解 中安全事件的事件回應之前 AWS，請先熟悉 AWS 安全與事件回應的相關標準和架構。這些基礎將協助您了解本指南中介紹的概念和最佳實務。

AWS 安全標準和架構

首先，我們建議您檢閱安全性、身分識別與合規、安全支柱 AWS 架構和雲端採用架構 (CAF) 概觀的安全性觀點白皮書的最佳實務。 AWSAWS

AWS CAF 提供指引，支援將組織的不同部分移至雲端之間的協調。 AWS CAF 指引分為數個重點領域，稱為與建置雲端 IT 系統相關的觀點。安全觀點說明如何跨工作流程實作安全計劃，其中一個是事件回應。本文件是我們與客戶合作的經驗產品，協助他們建置有效且高效率的安全事件回應計劃和功能。

產業事件回應標準和架構

本白皮書遵循美國國家標準技術研究所 (NIST) 所建立的電腦安全事件處理指南 SP 800-61 r2 的事件回應標準和最佳實務。閱讀和了解 NIST 引進的概念是有用的先決條件。此 NIST 指南中的概念和最佳實務將套用至本文 AWS 的技術。不過，現場部署事件案例超出本指南的範圍。

AWS 事件回應概觀

首先，請務必了解雲端中的安全操作和事件回應有何不同。若要建置有效的回應功能 AWS，您需要了解與傳統現場部署回應的偏差，及其對事件回應計畫的影響。本節會詳細說明這些差異，以及核心 AWS 事件回應設計原則。

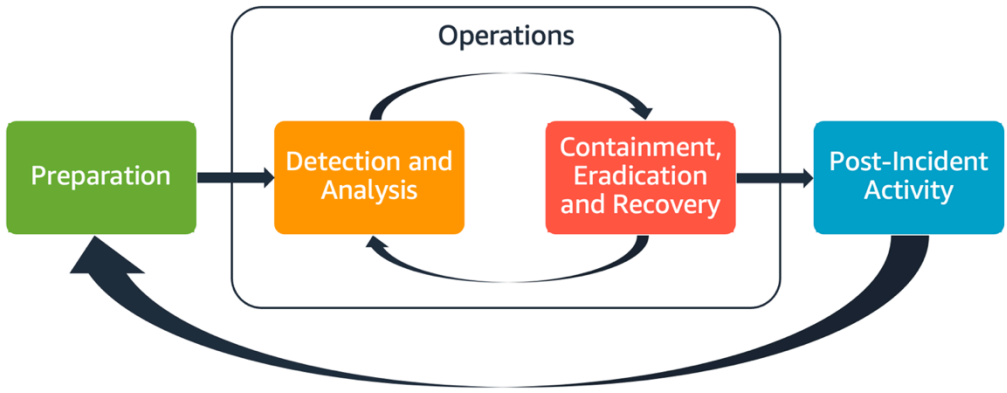
AWS 事件回應的層面

組織內的 AWS 所有使用者都應該對安全事件回應程序有基本的了解，而安全人員應該了解如何回應安全問題。教育、培訓和體驗是成功的雲端事件回應計畫必不可缺的一環，最好能預先實施，以因應發生安全事件的情況。雲端中成功事件回應計畫的基礎是準備、操作和事件後活動。

若要分別了解這三個層面，請參考下列說明：

- 準備 – 讓您的事件回應團隊 AWS 透過啟用偵測控制並驗證對必要工具和雲端服務的適當存取，來偵測和回應 內的事件。此外，備妥必要的程序手冊 (包括手動和自動)，以確認能夠做出可靠且一致的回應。
- 操作 – 在 NIST 事件回應階段之後對安全事件和潛在事件進行操作：偵測、分析、遏制、消除和復原。
- 事件後活動 – 反覆查看安全事件和模擬的結果，以改善回應的有效性、提高從回應和調查衍生的值，並進一步降低風險。您必須從事件中學習，並能夠確實實施後續改進。

本指南會探索並詳細說明這些層面。下圖顯示這些層面的流程，與先前提及的 NIST 事件回應生命週期保持一致，但與包含包含包含控制、根除和復原的偵測和分析的操作一致。



AWS 事件回應的層面

AWS 事件回應原則和設計目標

雖然 NIST SP 800-61 電腦安全事件處理指南所定義的事件回應的一般程序和機制是健全的，但我們也建議您考慮這些與回應雲端環境中的安全事件相關的特定設計目標：

- 建立回應目標 – 與利益相關者、法律顧問和組織領導層合作，以確定回應事件的目標。一些常見的目標包括包含和緩解問題、復原受影響的資源、保留資料以進行鑑識、返回已知的安全操作，以及最終從事件中學習。
- 使用雲端回應 – 在雲端中實作回應模式，即事件發生和資料的位置。
- 了解您擁有的內容和需求 – 將日誌、資源、快照和其他證據複製並儲存在專用於回應的集中式雲端帳戶中，以保留這些記錄、資源、快照和其他證據。運用標籤、中繼資料和機制，強制執行保留政策。您需要了解您使用的服務，然後識別調查這些服務的需求。為了協助您了解您的環境，您也可以使用標記，本文件稍後會在 the section called “制定和實作標記策略”章節中說明。
- 使用重新部署機制 – 如果安全異常可歸因於組態錯誤，則修復方法可能很簡單，例如透過使用適當的組態重新部署資源來移除差異。如果發現可能的入侵，請確認重新部署包含成功且經過驗證的根本原因緩解。
- 盡可能自動化 – 當問題發生或事件重複時，建立以程式設計方式分類和回應常見事件的機制。將人工回應用於自動化不足的唯一、複雜或敏感事件。
- 選擇可擴展的解決方案 – 努力符合組織雲端運算方法的可擴展性。實作可跨環境擴展的偵測和回應機制，以有效縮短偵測和回應之間的時間。
- 了解和改善您的程序 – 主動識別程序、工具或人員中的差距，並實作計畫來修正差距。模擬是尋找差距並改善程序的安全方法。如需如何在程序上反覆運算的詳細資訊，請參閱本文件的 the section called “事後處理”一節。

這些設計目標可提醒您審核架構實作，以確認能夠進行事件回應和威脅偵測。當您規劃雲端實作時，請考慮回應事件，最好使用鑑識健全的回應方法。在某些情況下，這表示您可能有多個專門為這些回應任務設定的組織、帳戶和工具。這些工具和功能應透過部署管道提供給事件回應人員使用。它們不應處於靜態，否則可能造成更大的風險。

雲端安全事件網域

若要有效準備和回應 AWS 環境中的安全事件，您需要了解雲端安全事件的常見類型。客戶的責任中有三個網域可能發生安全事件：服務、基礎設施和應用程式。不同的網域需要不同的知識、工具和回應程序。請考慮這些網域：

- 服務網域 – 服務網域中的事件可能會影響您的 AWS 帳戶、 AWS Identity and Access Management(IAM) 許可、資源中繼資料、帳單或其他區域。服務網域事件是您專門使用 AWS API 機制回應的事件，或者您有與組態或資源許可相關聯的根本原因，並且可能有相關的服務導向記錄。
- 基礎設施網域 – 基礎設施網域中的事件包括資料或網路相關活動，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上的程序和資料、虛擬私有雲端 (VPC) 內 Amazon EC2 執行個體的流量，以及其他區域，例如容器或其他未來服務。您對基礎設施網域事件的回應通常涉及取得事件相關資料以進行鑑識分析。它可能包括與執行個體作業系統的互動，而且在各種情況下，也可能涉及 AWS API 機制。在基礎設施網域中，您可以在訪客作業系統中使用 AWS APIs和數位鑑識/事件回應 (DFIR) 工具的組合，例如專用於執行鑑識分析和調查的 Amazon EC2 執行個體。基礎設施網域事件可能涉及分析網路封包擷取、Amazon Elastic Block Store (Amazon EBS) 磁碟區上的磁碟區塊，或從執行個體取得的揮發性記憶體。
- 應用程式網域 – 應用程式網域中的事件發生在應用程式程式碼中，或部署到服務或基礎設施的軟體中。此網域應包含在雲端威脅偵測和回應手冊中，並可能包含與基礎設施網域類似的回應。透過適當且深思熟慮的應用程式架構，您可以使用自動擷取、復原和部署，使用雲端工具來管理此網域。

在這些網域中，請考慮可能針對 AWS 帳戶、資源或資料採取行動的演員。無論是內部或外部，請使用風險架構來判斷組織的特定風險，並據此做好準備。此外，您應該開發威脅模型，這有助於您的事件回應規劃和深思熟慮的架構建置。

中事件回應的主要差異 AWS

事件回應是內部部署或雲端網路安全策略不可或缺的一部分。最低權限和深度防禦等安全原則旨在保護內部部署和雲端中資料的機密性、完整性和可用性。支援這些安全原則的多種事件回應模式都遵循規範，包括日誌保留、從威脅建模衍生的警示選擇、手冊開發，以及安全資訊和事件管理 (SIEM) 整合。當客戶開始在雲端架構和工程這些模式時，差異就開始了。以下是 中事件回應的主要差異 AWS。

差異 #1：安全即共同的責任

安全與合規的責任由 AWS 與其客戶共同承擔。此共同責任模型可減輕客戶的一些營運負擔，因為 會 AWS 操作、管理和控制從主機作業系統和虛擬化層到服務營運所在設施實體安全性的元件。如需共同責任模型的詳細資訊，請參閱共同責任模型文件。

隨著您在雲端的共同責任變更，事件回應的選項也會變更。規劃和了解這些權衡，並將其與您的控管需求配對，是事件回應中的關鍵步驟。

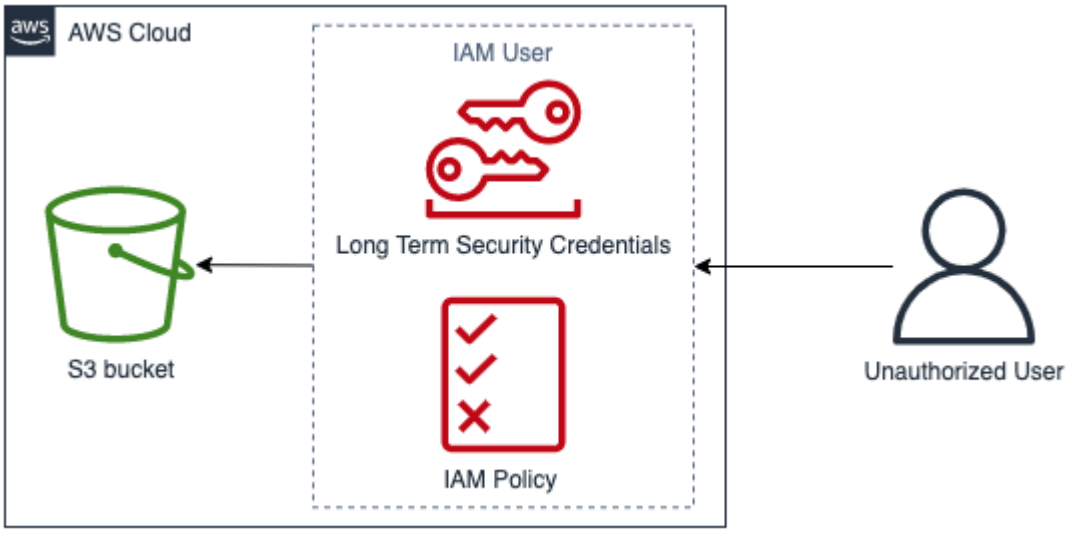
除了與您有直接關係之外 AWS，可能還有其他實體在您的特定責任模型中具有責任。例如，您可能有內部組織單位負責操作的某些層面。您可能也會與其他開發、管理或操作您部分雲端技術的第三方建立關係。

建立和測試符合您操作模型的適當事件回應計畫和適當的手冊非常重要。

差異 #2：雲端服務網域

由於雲端服務中存在安全責任的差異，因此引入了安全事件的新網域：服務網域，先前已在事件網域一節中說明。服務網域包含客戶的 AWS 帳戶、IAM 許可、資源中繼資料、帳單和其他區域。由於您的回應方式，此網域與事件回應不同。服務網域內的回應通常是透過檢閱和發出 API 呼叫，而不是傳統的主機式和網路式回應來完成。在服務網域中，您不會與受影響資源的作業系統互動。

下圖顯示服務網域中以架構反模式為基礎的安全事件範例。在這種情況下，未經授權的使用者會取得 IAM 使用者的長期安全登入資料。IAM 使用者具有 IAM 政策，允許他們從 Amazon Simple Storage Service (Amazon S3) 儲存貯體擷取物件。若要回應此安全事件，您可以使用 AWS APIs來分析 AWS 日誌，例如 AWS CloudTrail和 Amazon S3 存取日誌。您也可以使用 AWS APIs來包含並從事件中復原。



服務網域範例

差異 #3：用於佈建基礎設施APIs

另一個差異來自隨需自助服務的雲端特性。主要設施客戶透過全球許多地理位置提供的公有和私有端點， AWS 雲端 使用 RESTful API 與 互動。客戶可以使用 AWS 登入資料存取這些 APIs。與內部部署存取控制相反，這些登入資料不一定受網路或 Microsoft Active Directory 網域的約束。登入資料會改為與 AWS 帳戶內的 IAM 主體相關聯。這些 API 端點可以在您的公司網路之外存取，這對於了解何時回應在預期網路或地理之外使用登入資料的事件非常重要。

由於以 API 為基礎的本質 AWS，回應安全事件的重要日誌來源是 AWS CloudTrail，它會追蹤您 AWS 帳戶中進行的管理 API 呼叫，以及您可以在其中找到 API 呼叫來源位置的相關資訊。

差異 #4：雲端的動態性質

雲端是動態的，可讓您快速建立和刪除資源。透過自動擴展，資源可以根據流量增加向上和向下旋轉。透過短期基礎設施和快速進度變更，您正在調查的資源可能不再存在或可能已修改。了解 AWS 資源的暫時性性質，以及如何追蹤 AWS 資源的建立和刪除，對於事件分析至關重要。您可以使用 AWS Config 來追蹤 AWS 資源的組態歷史記錄。

差異 #5：資料存取

雲端的資料存取也不同。您無法插入伺服器以收集安全調查所需的資料。資料會透過線路和 API 呼叫收集。您需要練習並了解如何透過 APIs執行資料收集，以便為此輪班做好準備，並驗證適當的儲存體以有效收集和存取。

差異 #6：自動化的重要性

為了讓客戶完全實現雲端採用的優勢，他們的營運策略必須採用自動化。基礎設施即程式碼 (IaC) 是一種高效率的自動化環境模式，其中使用 或第三方AWS CloudFormation解決方案等原生 IaC 服務促進的程式碼來部署、設定、重新設定和銷毀 AWS 服務。這會將事件回應的實作推送為高度自動化，最好能避免人為錯誤，尤其是在處理證據時。在現場部署使用自動化時，在 中至關重要且更簡單 AWS 雲端。

解決這些差異

若要解決這些差異，請遵循下一節中概述的步驟，以驗證您的事件回應計劃是否在人員、程序和技術之間做好萬全準備。

準備

為因應事件做好準備，對於須及時並有效回應的事件來說至關重要。準備工作橫跨三個領域：

- 人員 – 為您的人員做好安全事件的準備，包括識別事件回應的相關利益相關者，並針對事件回應和雲端技術對其進行訓練。
- 程序 – 準備安全事件的程序包括記錄架構、制定完整的事件回應計劃，以及建立手冊以一致地回應安全事件。
- 技術 – 為您的安全事件技術做好準備包括設定存取、彙總和監控必要的日誌、實作有效的提醒機制，以及開發回應和調查功能。

這三個領域對於有效回應事件來說同樣重要。缺少任一個領域，事件回應計畫便不完整或無法發揮效用。您需要讓人員、流程和技術三者緊密整合，才能做好因應事件的準備。

人員

若要回應安全事件，您需要識別支援回應安全事件的利益相關者。此外，對有效回應來說，讓他們接受 AWS 技術和您 AWS 環境的訓練至關重要。

定義角色和責任

處理安全事件時，需要跨組織的紀律和採取行動的傾向。在事件發生期間，您的組織結構中應該有不同的人員在事件期間負責、當責、備詢及保持通訊，例如人力資源部 (HR)、行政團隊和法務部的代表。請考量這些角色和責任，以及是否必須涉及任何第三方。請注意，在許多地理區域中，有當地法律會控管應該和不應該執行的動作。雖然為您的安全回應計劃建立負責任、負責、諮詢和明智的 (RACI) 圖表看起來很愚蠢，但這樣做可以快速直接地溝通，並清楚地概述事件不同階段的領導力。

在事件期間，包括受影響應用程式和資源的擁有者/開發人員是關鍵，因為他們是主題專家 (SMEs)，可以提供資訊和內容以協助衡量影響。在您仰賴開發人員和應用程式擁有者的專業知識進行事件回應之前，請務必先與他們建立關係。應用程式擁有者或 SME (例如您的雲端管理員或工程師) 可能需要在環境不同於前或複雜，或是回應者無法存取的情況下採取行動。

最後，受信任的關係可能會參與調查或回應，因為它們可以提供額外的專業知識和寶貴的審查。若您自己的團隊沒有這些技能，您可能需要對外招聘以尋求協助。

訓練事件回應員工

培訓您的事件回應人員了解其組織使用的技術，對於他們充分回應安全事件至關重要。如果您的員工不了解基礎技術，回應可能會延長。除了傳統的事件回應概念之外，他們也必須了解 AWS 服務及其 AWS 環境。有多種傳統機制可以訓練您的事件人員，例如線上訓練和課堂訓練。您也應考慮執行遊戲日或模擬作為訓練的機制。如需如何執行模擬的詳細資訊，請參閱本文件的 the section called “執行定期模擬”一節。

了解 AWS 雲端 技術

為了減少相依性並縮短回應時間，請確保您的安全團隊和回應者都獲得雲端服務的相關教育，並有機會在組織使用的特定雲端環境中實作實務。若要讓事件回應者有效，請務必了解 AWS 基礎、IAM AWS Organizations、 AWS 記錄和監控服務和 AWS 安全服務。

AWS 提供線上安全研討會 （請參閱AWS 安全研討會)，您可以在其中取得 AWS 安全與監控服務的實作體驗。 AWS 也透過數位訓練、課堂訓練、 AWS 訓練合作夥伴和認證，提供許多訓練選項和學習路徑。若要進一步了解，請參閱AWS 訓練和認證。

AWS 提供以訂閱為基礎的免費培訓，支援多個角色和重點領域。請造訪 AWS Skillbuilder 以進一步了解。

了解您的 AWS 環境

除了了解 AWS 服務、其使用案例，以及它們如何互相整合之外，了解組織 AWS 環境的實際架構方式以及有哪些操作程序也同樣重要。通常，這類內部知識不會被記錄，而且只有少數領域專家可以理解，這可以建立相依性、阻礙創新和緩慢的回應時間。

為了避免這些相依性和加快回應時間，安全分析師應該記錄、存取和了解您 AWS 環境的內部知識。了解您的完整雲端足跡需要相關安全利益相關者和雲端管理員之間的協作。準備事件回應程序的一部分包括記錄和集中架構圖，這在本白皮書the section called “記錄和集中架構圖”稍後會介紹。不過，從人員的角度來看，您的分析師必須能夠存取和了解與您 AWS 環境相關的圖表和操作程序。

了解 AWS 回應團隊和支援

支援

支援 提供各種計劃，可讓您存取支援 AWS 解決方案成功和運作狀態的工具和專業知識。如果您需要技術支援和其他資源來協助規劃、部署和最佳化您的 AWS 環境，您可以選擇最符合您 AWS 使用案例的支援計畫。

將 AWS Management Console （需要登入） 中的支援中心視為聯絡中心，以取得影響 AWS 資源問題的支援。對 支援 的存取由 IAM 控制。如需取得 AWS 支援功能存取權的詳細資訊，請參閱 入門 支援。

此外，如果您需要報告濫用，請聯絡 AWS Tust and Safety 團隊。

AWS 客戶事件回應團隊 (CIRT)

AWS 客戶事件回應團隊 (CIRT) 是專門的全年無休全球 AWS 團隊，可在AWS 共同責任模型客戶端的作用中安全事件期間為客戶提供支援。

當 AWS CIRT 支援您時，您將收到有關作用中安全事件的分類和復原的協助 AWS。他們將使用 AWS 服務日誌協助進行根本原因分析，並為您提供復原建議。他們也會提供安全建議和最佳實務，協助您避免未來的安全事件。

AWS 客戶可以透過AWS 支援案例與 AWS CIRT 互動。

- 所有客戶：
  1. 帳戶和帳單
  2. 服務：帳戶
  3. 類別：安全性

4. 嚴重性：一般問題

- 具有開發人員 支援 計劃的客戶：
  1. 帳戶和帳單
  2. 服務：帳戶
  3. 類別：安全性
  4. 嚴重性：重要問題

- 擁有商業 支援 計劃的客戶：
  1. 帳戶和帳單
  2. 服務：帳戶
  3. 類別：安全性
  4. 嚴重性：緊急業務影響問題

- 擁有企業 支援 計劃的客戶：
  1. 帳戶和帳單
  2. 服務：帳戶
  3. 類別：安全性
  4. 嚴重性：關鍵業務風險問題

- AWS 安全事件應變 訂閱的客戶：在 https：//https://console.aws.amazon.com/security-ir/ 開啟安全事件回應主控台

DDoS 回應支援

AWS 提供 AWS Shield的受管分散式拒絕服務 (DDoS) 保護服務，可保護在 上執行的 Web 應用程式 AWS。 AWS Shield 提供永遠在線偵測和自動內嵌緩解措施，可將應用程式停機時間和延遲降至最低，因此不需要參與 支援 即可受益於 DDoS 保護。有兩種方案 AWS Shield：Shield Standard 和 Shield Advanced。若要了解這兩個層之間的差異，請參閱 Shield 功能文件。

AWS Managed Services (AMS)

AWS Managed Services (AMS) 提供 AWS 基礎設施的持續管理，讓您可以專注於應用程式。透過實作維護基礎設施的最佳實務，AMS 有助於降低營運開銷和風險。AMS 可自動化常見的活動，例如，變

更請求、監控、修補程式管理、安全性和備份服務，而且提供佈建、執行和支援基礎設施的完整生命週期服務。

AMS 負責部署安全偵測控制套件，並提供每天第一行的提醒回應。提醒啟動時，AMS 會依照一組標準的自動化和手動程序手冊來驗證回應的一致性。這些程序手冊會在上線期間與 AMS 客戶共享，讓他們能夠透過 AMS 來制定和協調應變措施。

流程

開發完整且明確定義的事件回應程序，是成功且可擴展事件回應計畫的關鍵。發生安全事件時，明確的步驟和工作流程將協助您及時回應。您可能已經有現有的事件回應程序。無論您目前的狀態為何，都必須定期更新、重複執行和測試事件回應程序。

制定和測試事件回應計劃

要為事件回應開發的第一個文件是事件回應計劃。事件回應計畫應是您事件回應計畫和策略的基礎。事件回應計畫是高階文件，通常包含下列各節：

- 事件回應團隊概觀 – 概述事件回應團隊的目標和職能
- 角色和責任 – 列出事件回應利益相關者，並在事件發生時詳細說明其角色
- 通訊計劃 – 詳細說明聯絡資訊，以及在事件期間如何通訊

  最佳實務是讓out-of-band通訊做為事件通訊的備份。提供安全out-of-band通訊管道的應用程式範例為 AWS Wickr。
- 事件回應的階段和要採取的動作 – 列舉事件回應的階段 – 例如偵測、分析、根除、包含和復原 – 包括在這些階段內要採取的高階動作
- 事件嚴重性和優先順序定義 – 詳細說明如何分類事件嚴重性、如何排定事件優先順序，以及嚴重性定義如何影響呈報程序

儘管不同規模和產業的公司都會有這些章節，但每個組織的事件回應計畫都是獨一無二的。您需要建置最適合您組織的事件回應計劃。

記錄和集中架構圖

若要快速準確地回應安全事件，您需要了解系統和網路的架構方式。根據最佳實務，了解這些內部模式不僅對於事件回應很重要，也對於驗證架構模式之應用程式之間的一致性也很重要。您也應該確認本文件是最新的，並根據新的架構模式定期更新。您應該開發詳細說明下列項目的文件和內部儲存庫：

- AWS 帳戶結構 - 您需要知道：

  - 您有多少 AWS 帳戶？
  - 這些 AWS 帳戶如何組織？
  - 誰是 AWS 帳戶的商業擁有者？
  - 您是否使用服務控制政策 SCPs)？ 若是如此，使用 SCPs 實作了哪些組織護欄？
  - 您是否限制可使用的區域和服務？
  - 業務單位和環境之間有什麼差異 (dev/test/prod)？
- AWS 服務模式
  - 您使用哪些 AWS 服務？
  - 什麼是最廣泛使用的 AWS 服務？
- 架構模式
  - 您使用哪些雲端架構？
- AWS 身分驗證模式
  - 您的開發人員通常如何進行身分驗證 AWS？
  - 您是否使用 IAM 角色或使用者 （或兩者）？ 您的身分驗證是否 AWS 連線至身分提供者 (IdP)？
  - 如何將 IAM 角色或使用者映射至員工或系統？
  - 當有人不再獲得授權時，如何撤銷存取權？
- AWS 授權模式
  - 您的開發人員使用哪些 IAM 政策？
  - 您是否使用資源型政策？
- 記錄和監控
  - 您使用哪些記錄來源，以及它們存放在哪裡？
  - 您是否彙總 AWS CloudTrail 日誌？ 如果是這樣，它們會存放在哪裡？
  - 如何查詢 CloudTrail 日誌？
  - 您是否已啟用 Amazon GuardDuty？
  - 如何存取 GuardDuty 調查結果 （例如主控台、票證系統、SIEM)？
  - 問題清單或事件是否彙總在 SIEM 中？
  - 票證是否會自動建立？
  - 有哪些工具可用來分析調查的日誌？
- 網路拓撲
  - 您網路上的裝置、端點和連線在實體或邏輯上如何排列？
  - 您的網路如何與 連線 AWS？

  - 如何在環境之間篩選網路流量？
- 外部基礎設施
  - 如何部署面向外部的應用程式？
  - 哪些 AWS 資源可公開存取？
  - 哪些 AWS 帳戶包含面向外部的基礎設施？
  - 有哪些 DDoS 或外部篩選？

記錄內部技術圖表和程序可簡化事件回應分析師的任務，協助他們快速取得機構知識來回應安全事件。完整的內部技術程序文件不僅簡化了安全調查，還調整了程序的合理化和評估。

開發事件回應手冊

準備事件回應流程的關鍵部分是制定程序手冊。事件回應程序手冊提供一系列方案指引和安全事件發生時應遵循的步驟。提供清晰的結構和步驟簡化了回應的複雜度並減少人為錯誤的可能性。

要為 建立手冊的內容

應針對事件案例建立程序手冊，例如：

- 預期事件 – 應為您預期的事件建立手冊。這包括拒絕服務 (DoS)、勒索軟體和憑證入侵等威脅。
- 已知的安全性問題清單或提醒 – 應為已知的安全性問題清單和提醒建立手冊，例如 GuardDuty 問題清單。您可能會收到 GuardDuty 調查結果並思考：「現在該怎麼辦？」 若要防止錯誤處理 GuardDuty 調查結果或忽略調查結果，請為每個潛在的 GuardDuty 調查結果建立手冊。如需部分修復詳細資料和指引，請參閱 GuardDuty 文件。值得注意的是，在預設情況下 GuardDuty 是未啟用的狀態，並且會產生費用。如需 GuardDuty 的詳細資訊，請參閱附錄 A：雲端功能定義 - the section called “可見性和提醒”。

手冊中要包含的內容

程序手冊應包含安全分析師應完成的技術步驟，以便充分調查和應對潛在的安全事件。

要納入程序手冊的項目包括：

- 手冊概觀 – 此手冊處理哪些風險或事件案例？ 程序手冊的目標是什麼？
- 先決條件 – 此事件案例需要哪些日誌和偵測機制？ 預期的通知是什麼？
- 利害關係人資訊 – 涉及的人員及其聯絡資訊為何？ 每個利害關係人的責任是什麼？
- 回應步驟 – 在事件回應的各階段中，應採取哪些策略步驟？ 分析師應該執行哪些查詢？ 應該執行哪些程式碼以達到預期的成果？

  - Detect – 如何偵測事件？
  - 分析 – 如何判斷影響範圍？
  - 包含 – 如何隔離事件以限制範圍？
  - 消除 – 如何從環境中移除威脅？
  - 復原 – 如何將受影響的系統或資源帶回生產環境？
- 預期結果 – 執行查詢和程式碼之後，手冊的預期結果是什麼？

若要驗證每個程序手冊中一致的資訊，建立程序手冊範本以在其他安全程序手冊中使用會很有幫助。某些先前列出的項目，例如利益相關者資訊，可以在多個手冊之間共用。如果是這種情況，您可以建立該資訊的集中式文件，並在手冊中參考它，然後列舉手冊中的明確差異。這將讓您不必更新所有個別手冊中的相同資訊。透過建立範本並識別手冊中的常見或共用資訊，您可以簡化和加速手冊開發。最後，您的手冊可能會隨著時間演進；一旦您確認步驟一致，就會形成自動化的需求。

範例手冊

您可以在 的附錄 B 中找到許多範例手冊the section called “Playbook 資源”。此處的範例可用來引導您了解要建立哪些手冊，以及手冊中要包含哪些內容。不過，請務必製作手冊，其中包含與您業務最相關的風險。您需要驗證手冊中的步驟和工作流程是否包含您的技術和程序。

執行定期模擬

組織隨著時間的推移而成長和發展，威脅態勢也是如此。因此，持續檢閱您的事件回應功能非常重要。模擬是一種可用來執行此評估的方法。模擬會使用真實世界的安全事件案例，這些案例旨在模擬威脅參與者的策略、技術和程序 (TTP)，並且讓組織可藉由回應這些可能發生在現實中的模擬網路事件，來運用和評估其事件回應能力。

模擬具有各種優點，包括：

- 驗證網路整備程度和培養事件回應人員的信心。
- 測試工具和工作流程的正確性及效率。
- 根據您的事件回應計畫，精進溝通和呈報方法。
- 提供回應罕見媒介的機會。

模擬的類型

主要的模擬類型有三種：

- 桌上練習 – 模擬的桌上方法嚴格是一種以討論為基礎的工作階段，涉及各種事件回應利益相關者來練習角色和責任，並使用已建立的通訊工具和程序手冊。練習促進通常可以在虛擬場地、實體場地或組合的全天內完成。由於以討論為基礎的本質，桌面練習著重於程序、人員和協同合作。技術是討論不可或缺的一部分；不過，實際使用事件回應工具或指令碼通常不是資料表式練習的一部分。
- 紫色團隊練習 – 紫色團隊練習可提高事件回應者 (藍隊) 與模擬威脅執行者 (紅隊) 之間的協同合作程度。藍色團隊通常由安全營運中心 (SOC) 的成員組成，但也可以包括在實際網路事件期間涉及的其他利益相關者。紅隊通常由滲透測試團隊或關鍵利益相關者組成，他們受過攻擊性安全訓練。紅隊演練在設計案例時與練習主持人合作，讓案例準確且可行。在紫色團隊練習期間，主要重點是偵測機制、工具和支援事件回應工作的標準操作程序 (SOPs)。
- 紅隊演練 – 在紅隊演練期間，違規 (紅隊) 會執行模擬，以從預先確定的範圍實現特定目標或一組目標。防禦者 (藍隊) 不一定知道練習的範圍和持續時間，這可提供更逼真的評估，評估他們會如何回應實際的事件。由於紅隊演練可能是侵入性測試，因此您應該謹慎並實作控制，以確認演練不會對您的環境造成實際傷害。

> **Note**
>
> AWS 要求客戶在進行紫色團隊或紅隊演練之前，檢閱滲透測試網站上提供的滲透測試政策。

表 1 摘要說明這些模擬類型的一些主要差異。請務必注意，定義通常被視為鬆散定義，並且可以自訂以符合組織的需求。

表 1 – 模擬的類型

	桌上練習	紫色團隊練習	紅隊演練
摘要	專注於一個特定安全事件案例的紙張驅動練習。這些可以是高階或技術，並由一系列的紙質注入驅動。	與桌面練習相比，更逼真的產品。在紫色團隊練習期間，主持人與參與者協作，以提高練習參與度，並在必要時提供培訓。	一般而言是更進階的模擬產品。通常隱蔽程度很高，參與者可能不知道練習的所有詳細資訊。
所需的資源	所需的技術資源有限	需要各種利益相關者和所需的高階技術資源	需要各種利益相關者和所需的高階技術資源

	桌上練習	紫色團隊練習	紅隊演練
複雜性	低	中	高

考慮定期推行網路模擬。每個練習類型都可以為參與者和整個組織提供獨特的好處，因此您可以選擇從較不複雜的模擬類型（例如桌面練習）開始，並進入較複雜的模擬類型（紅隊演練）。您應根據自身的安全成熟度、資源和所需的結果來選取模擬類型。由於複雜性和成本，某些客戶可能不會選擇執行紅隊演練。

練習生命週期

無論您選擇的模擬類型為何，模擬通常遵循下列步驟：

1. 定義核心練習元素 – 定義模擬案例和模擬的目標。這兩者都應獲得領導階層的允許。
2. 識別關鍵利益相關者 – 至少，一項練習需要練習主持人和參與者。根據情境，可能會涉及法律、通訊或主管領導階層等其他利害關係人。
3. 建置和測試案例 – 如果特定元素不可行，可能需要重新定義案例，因為它正在建置中。預計最終的情境會成為此階段的輸出。
4. 促進模擬 – 模擬的類型決定了所使用的促進方式（與高度技術、模擬案例相比，以紙張為基礎的情況）。協調員應使其促進策略與模擬演練目標相對應，他們應盡可能吸引所有模擬演練參與者，以提供最大的效益。
5. 制定行動後報告 (AAR) – 識別表現良好的領域、可以使用改善的領域，以及潛在的差距。AAR 應衡量模擬的有效性以及團隊對於模擬事件的應變能力，以便在未來的模擬追蹤進展幅度。

技術

如果您在安全事件之前開發並實作適當的技術，您的事件回應人員將能夠調查、了解範圍，並及時採取行動。

開發 AWS 帳戶結構

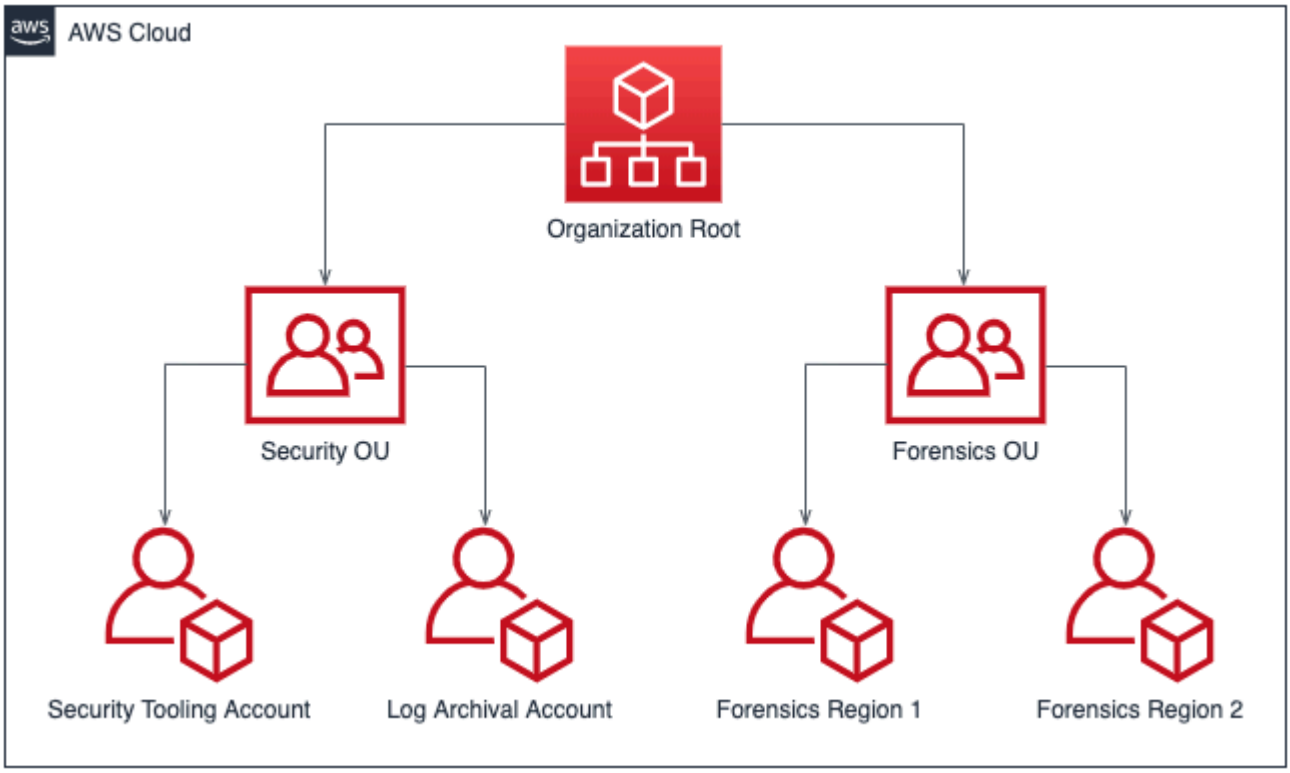
AWS Organizations 當您成長和擴展 AWS 資源時， 會協助集中管理 AWS 環境。 AWS 組織會合併 AWS 您的帳戶，以便您以單一單位管理它們。您可以使用組織單位 (OU) 將帳戶群組在一起，以單一單位的形式進行管理。

對於事件回應，擁有支援事件回應功能 AWS 的帳戶結構很有幫助，其中包括安全 OU 和鑑識 OU。在安全性 OU 中，您應該擁有下列項目的帳戶：

- 日誌封存 – 彙總日誌封存 AWS 帳戶中的日誌。
- 安全工具 – 將安全服務集中在安全工具 AWS 帳戶中。此帳戶會以安全性服務的委派系統管理員身分運作。

在鑑識 OU 中，您可以選擇為營運所在的每個區域實作一或多個鑑識帳戶，具體視哪個區域最適合您業務和營運模式而定。對於每個區域帳戶方法的範例，如果您僅在美國東部（維吉尼亞北部）(us-east-1) 和美國西部（奧勒岡）(us-west-2) 中操作，則您會在鑑識 OU 中有兩個帳戶：一個用於 us-east-1，另一個用於 us-west-2。佈建新帳戶需要一些時間，因此必須在事件之前建立和檢測鑑識帳戶，以便回應者能夠有效地使用這些帳戶進行回應。

下圖顯示範例帳戶結構，包括具有每個區域鑑識帳戶的鑑識 OU：



事件回應的每個區域帳戶結構

制定和實作標記策略

取得有關業務使用案例的內容資訊以及與 AWS 資源相關的內部利益相關者可能很困難。其中一種方法是標籤形式，將中繼資料指派給您的 AWS 資源，並包含使用者定義的金鑰和值。您可以建立標籤，依目的、擁有者、環境、處理的資料類型以及您選擇的其他條件來分類資源。

擁有一致的標記策略可讓您快速識別和辨別 AWS 資源的相關內容資訊，以加快回應時間。標籤也可以作為啟動回應自動化的機制。如需如何標記的詳細資訊，請參閱標記 AWS 資源的文件。您需要先定義要在整個組織中實作的標籤。之後，您將實作並強制執行此標記策略。您可以在 AWS 部落格中找到實作和強制執行的詳細資訊 使用標籤政策和服務控制政策 (SCPs) AWS 實作 AWS 資源標記策略。

更新 AWS 帳戶聯絡資訊

對於您的每個 AWS 帳戶，請務必擁有準確且up-to-date聯絡資訊，以便正確的利益相關者收到 AWS 來自 安全性、帳單和操作等主題的重要通知。對於每個 AWS 帳戶，您都有主要聯絡人和用於安全性、帳單和操作的替代聯絡人。您可以在AWS 帳戶管理參考指南中找到這些聯絡人之間的差異。

如需管理替代聯絡人的詳細資訊，請參閱AWS 新增、變更或移除替代聯絡人的文件。如果您的團隊管理帳單、操作和安全相關問題，最佳實務是使用電子郵件分發清單。電子郵件分發清單會移除一個人的相依性，如果他們不在辦公室或離開公司，可能會導致封鎖。您也應該驗證電子郵件和帳戶聯絡資訊，包括電話號碼，是否受到保護，以防止根帳戶密碼重設和多重驗證 (MFA) 重設。

對於使用 的客戶 AWS Organizations，組織管理員可以使用管理帳戶或委派管理員帳戶集中管理成員帳戶的替代聯絡人，而不需要每個 AWS 帳戶的登入資料。您也需要驗證新建立的帳戶具有準確的聯絡資訊。請參閱自動更新新建立 AWS 帳戶 部落格文章的替代聯絡人。

準備對 的存取 AWS 帳戶

在事件期間，您的事件回應團隊必須能夠存取事件涉及的環境和資源。確保您的團隊在事件發生之前擁有適當的存取權來執行其職責。若要這樣做，您應該知道團隊成員需要的存取層級 （例如，他們可能採取的動作類型），並應事先佈建最低權限存取。

若要實作和佈建此存取權，您應該識別帳戶策略和雲端身分策略，並與組織的雲端架構師討論 AWS ，以了解已設定哪些身分驗證和授權方法。由於這些登入資料具有特殊權限，因此在實作過程中，您應該考慮使用核准流程或從保存庫或安全處擷取登入資料。實作之後，您應該在事件發生之前妥善記錄和測試團隊成員的存取權，以確保他們可以毫無延遲地回應。

最後，專為回應安全事件而建立的使用者通常具有特殊權限，以提供足夠的存取權。因此，應限制、監控這些登入資料，且不用於日常活動。

了解威脅環境

開發威脅模型

透過開發威脅模型，組織可以在未經授權的使用者可以識別威脅和緩解措施。威脅建模有多種策略和方法；請參閱如何處理威脅建模部落格文章。對於事件回應，威脅模型可協助識別威脅行為者在事件期間可能使用的攻擊媒介。了解您要防禦的內容至關重要，以便及時回應。您也可以使用 AWS Partner 進行威脅建模。若要搜尋 AWS 合作夥伴，請使用 AWS Partner Network。

整合和使用網路威脅情報

網路威脅情報是威脅行為者意圖、機會和能力的資料和分析。取得和使用威脅情報有助於及早偵測事件，並更好地了解威脅行為者的行為。網路威脅情報包括靜態指標，例如 IP 地址或惡意軟體的檔案雜湊。它還包含高階資訊，例如行為模式和意圖。您可以從許多網路安全供應商和開放原始碼儲存庫收集威脅情報。

若要為您的 AWS 環境整合和最大化威脅情報，您可以使用一些out-of-the-box功能，並整合您自己的威脅情報清單。Amazon GuardDuty 使用 AWS 內部和第三方威脅情報來源。其他服務 AWS ，例如 DNS 防火牆和 AWS WAF 規則，也會接受來自進階威脅情報群組 AWS的輸入。有些 GuardDuty 調查結果會映射到 MITRE ATT&CK 架構，該架構提供有關對手策略和技術的真實世界觀察資訊。

選取並設定日誌以進行分析和提醒

在安全調查期間，您需要能夠審核相關日誌以記錄和了解該事件的完整範圍和時間表。產生提醒也需要日誌，以指出特定關注的動作已發生。選擇、啟用、儲存和設定查詢與擷取機制和設定提醒至關重要。本節會檢閱每個動作。如需詳細資訊，請參閱安全事件回應的記錄策略 AWS 部落格文章。

選取並啟用日誌來源

在安全調查之前，您需要擷取相關日誌，以追溯重建 AWS 帳戶中的活動。選取並啟用與其 AWS 帳戶工作負載相關的日誌來源。

AWS CloudTrail 是一種記錄服務，可追蹤針對擷取 AWS 服務活動 AWS 的帳戶發出的 API 呼叫。它預設為啟用，並保留 90 天的管理事件，這些事件可透過 CloudTrail 的事件歷史記錄設施 AWS Management Console使用 AWS CLI、 或 AWS SDK 擷取。若要延長資料事件的保留和可見性，您需要建立 CloudTrail Trail 並與 Amazon S3 儲存貯體建立關聯，以及選擇性地與 CloudWatch 日誌群組建立關聯。或者，您可以建立 CloudTrail Lake，這會保留 CloudTrail 日誌長達七年，並提供以 SQL 為基礎的查詢設施。

AWS 建議使用 VPC 的客戶分別使用 VPC 流程日誌和 Amazon Route 53 解析程式查詢日誌來啟用網路流量和 DNS 日誌，並將其串流到 Amazon S3 儲存貯體或 CloudWatch 日誌群組。您可以為 VPC、子網路或網路界面建立 VPC 流程日誌。對於 VPC 流程日誌，您可以選擇啟用流程日誌以降低成本的方式和位置。

AWS CloudTrail 日誌、VPC 流程日誌和 Route 53 解析程式查詢日誌是支援 中安全調查的基本日誌三角結構 AWS。

AWS 服務可以產生基本記錄 trifecta 未擷取的日誌，例如 Elastic Load Balancing 日誌、 AWS WAF 日誌、 AWS Config 記錄器日誌、Amazon GuardDuty 調查結果、Amazon Elastic Kubernetes Service

(Amazon EKS) 稽核日誌，以及 Amazon EC2 執行個體作業系統和應用程式日誌。如需記錄和監控選項的完整清單the section called “附錄 A：雲端功能定義”，請參閱 。

選取日誌儲存

日誌儲存的選擇通常與您使用的查詢工具、保留功能、熟悉度和成本有關。當您啟用 AWS 服務日誌時，請提供儲存設施；通常是 Amazon S3 儲存貯體或 CloudWatch 日誌群組。

Amazon S3 儲存貯體透過選用的生命週期政策，提供經濟實惠的耐用儲存體。存放在 Amazon S3 儲存貯體中的日誌可以使用 Amazon Athena 等服務進行原生查詢。CloudWatch 日誌群組透過 CloudWatch Logs Insights 提供耐用的儲存方式和內建查詢設施。

識別適當的日誌保留

當您使用 S3 儲存貯體或 CloudWatch 日誌群組存放日誌時，您必須為每個日誌來源建立足夠的生命週期，以最佳化儲存和擷取成本。客戶通常有 3 到 12 個月的日誌可供查詢，保留期長達七年。可用性和保留時間的選擇應該配合您的安全需求與各種法令、法規和業務規定。

選取並實作日誌的查詢機制

在 中 AWS，您可以用來查詢日誌的主要服務是 CloudWatch Logs Insights 用於儲存在 CloudWatch 日誌群組中的資料，以及 Amazon Athena 和 Amazon OpenSearch Service 用於儲存在 Amazon S3 中的資料。您也可以使用第三方查詢工具，例如安全性資訊和事件管理 (SIEM)。

選取日誌查詢工具的過程中應該考慮安全營運的人員、程序和技術層面。選取可滿足營運、業務和安全需求，且長期可存取和可維護的工具。請記住，將要掃描的日誌數目維持在日誌查詢工具限制之內，以便以最佳狀態運作。由於成本或技術限制，客戶擁有多個查詢工具並不常見。例如，客戶可能會使用第三方 SIEM 來執行過去 90 天的查詢，並使用 Athena 執行超過 90 天的查詢，因為 SIEM 的日誌擷取成本。無論實作為何，請確認您的方法能將最大化營運效率所需的工具數量降至最低，尤其是在安全事件調查期間。

使用日誌來提醒

AWS 原生透過安全服務提供提醒，例如 Amazon GuardDuty、 AWS Security Hub和 AWS Config。您也可以針對這些服務未涵蓋的安全提醒，或與您環境相關的特定提醒，使用自訂提醒產生引擎。the section called “偵測” 本文件中稱為 的章節涵蓋了建立這些提醒和偵測。

開發鑑識功能

在安全事件發生之前，將開發鑑識功能納入考量，以協助安全事件調查。將鑑識技術整合至 NIST 事件回應的指南提供此類指導。

上的鑑識 AWS

適用於傳統內部部署鑑識的概念 AWS。部落格文章中的鑑識調查環境策略 AWS 雲端為您提供重要資訊，以開始將鑑識專業知識遷移至 AWS。

將環境和 AWS 帳戶結構設定為鑑識之後，您會想要定義在四個階段有效執行鑑識健全方法所需的技術：

- 收集 – 收集相關 AWS 日誌，例如 AWS CloudTrail、 AWS Config、VPC 流程日誌和主機層級日誌。收集受影響 AWS 資源的快照、備份和記憶體傾印。
- 檢查 – 透過擷取和評估相關資訊來檢查收集的資料。
- 分析 – 分析收集的資料，以了解事件並從中得出結論。
- 報告 – 呈現分析階段所產生的資訊。

擷取備份和快照

設定重要系統和資料庫的備份，對於從安全事件中復原和鑑識用途非常重要。備份就緒後，您可以將系統還原到先前的安全狀態。在 上 AWS，您可以拍攝各種資源的快照。快照可為您提供那些資源的時間點備份。有許多 AWS 服務，可以在備份和復原方面為您提供支援。如需這些服務和備份和復原方法的詳細資訊，請參閱備份和復原規範指南。如需詳細資訊，請參閱使用備份從安全事件復原部落格文章。

尤其是當涉及勒索軟體等情況時，務必確保備份是否有充足的保護。請參閱部落格文章中保護備份安全的 10 大安全最佳實務 AWS，以取得保護備份的指導方針。除了確保備份的安全之外，您還應該定期測試備份和還原程序，以確認您現有的技術和程序是否如預期般運作。

在 上自動化鑑識 AWS

在安全事件期間，您的事件回應團隊必須能夠快速收集和分析證據，同時在事件周圍的期間內保持準確性。事件回應團隊在雲端環境中手動收集相關證據既具有挑戰性又耗時，尤其是在大量執行個體和帳戶中。此外，手動收集可能容易出現人為錯誤。基於這些原因，客戶應該開發和實作鑑識的自動化。

AWS 為鑑識提供了多種自動化資源，這些資源合併在 下的附錄中the section called “鑑識資源”。這些資源是我們已開發和客戶已實作的鑑識模式範例。雖然這些範例在一開始可能是有用的參考架構，但請根據環境、需求、工具和鑑識程序，考慮是否加以修改或建立新的鑑識自動化模式。

準備項目摘要

徹底準備回應安全事件對於及時且有效的事件回應至關重要。事件回應準備涉及人員、程序和技術。這三個網域對於準備也同樣重要。您應該準備並發展所有三個網域的事件回應計畫。

表 2 摘要說明本節中詳述的準備項目。

表 2 – 事件回應準備項目

網域	準備項目	動作項目
人員	定義角色和責任。	• 識別相關的事件回應利益相關者。 • 制定事件的負責、負責、明智、諮詢 (RACI) 圖表。
人員	訓練事件回應人員 AWS。	• 在 AWS 基礎上訓練事件回應利益相關者。 • 培訓事件回應利益相關者 AWS 的安全和監控服務。 • 訓練您 AWS 環境的事件回應利益相關者及其架構方式。
人員	了解 AWS 支援選項。	• 了解 AWS 支援、客戶事件回應團隊 (CIRT)、DDoS 回應團隊 (DRT) 和 AMS 的差異。 • 如有需要，了解在作用中安全事件期間到達 CIRT 的分類和呈報路徑。
程序	制定事件回應計劃。	• 建立定義事件回應計劃和策略的高階文件。 • 將 RACI、通訊計畫、事件定義和事件回應階段納入事件回應計畫。
程序	記錄和集中架構圖。	• 記錄如何在帳戶結構、服務用量、IAM 模式和其他核心功能之間設定 AWS 環境的詳細資訊 AWS 。

網域	準備項目	動作項目
		• 開發雲端架構的架構圖。
程序	開發事件回應手冊。	• 為手冊的結構建立範本。 • 為預期的安全事件建置程序手冊。 • 為已知的安全提醒建置手冊，例如 GuardDuty 調查結果。
程序	執行定期模擬。	• 開發定期節奏來執行事件模擬。 • 使用輸出和經驗教訓來反覆執行事件回應計畫。
技術	開發 AWS 帳戶結構。	• 規劃 帳戶結構，以了解 AWS 帳戶如何分隔工作負載。 • 使用安全工具和日誌封存帳戶建立安全 OU。 • 針對您操作的每個區域，使用鑑識帳戶建立鑑識 OU。
技術	制定並實作標記策略，以協助回應者識別調查結果的擁有權和內容。	• 規劃標記策略，以及您希望與 AWS 資源建立關聯的標籤。 • 實作和強制執行標記策略。
技術	更新 AWS 帳戶聯絡資訊。	• 確認 AWS 帳戶已列出聯絡資訊。 • 建立聯絡資訊的電子郵件分發清單，以移除單一失敗點。 • 保護與帳戶資訊相關聯的電子郵件 AWS 帳戶。

網域	準備項目	動作項目
技術	準備存取 AWS 帳戶。	• 定義回應事件所需的存取事件回應者。 • 實作、測試和監控存取權。
技術	了解威脅環境。	• 開發環境和應用程式的威脅模型。 • 整合和使用網路威脅情報。
技術	選取並設定日誌。	• 識別並啟用調查日誌。 • 選取日誌儲存。 • 識別和實作日誌保留。 • 開發擷取和查詢日誌和成品的機制。 • 使用日誌進行提醒。
技術	開發鑑識功能。	• 識別鑑識收集所需的成品。 • 擷取並保護金鑰系統的備份。 • 定義分析已識別日誌和成品的機制。 • 實作自動化以進行鑑識分析。

建議採用反覆方法進行事件回應準備。所有這些準備項目都無法整夜完成；您應該建立計畫，以啟動小型的 ，並隨著時間持續改善您的事件回應功能。

作業

操作是進行事件回應的核心。這也是採取行動回應和補救安全事件的所在。操作包括以下五個階段：偵測、分析、遏制、根除和復原。您可以在表 3 中找到這些階段和目標的描述。

表 3 – 操作階段

階段	目標
偵測	識別潛在的安全事件。
分析	判斷安全事件是否為事件，並評估事件的範圍。
遏制	盡量縮小並限制安全事件的範圍。
根除	移除與安全事件相關的未經授權資源或成品。實作造成安全事件的緩和措施。
復原	將系統還原至已知的安全狀態，並監控這些系統以確認威脅未傳回。

這些階段應做為您回應和操作安全事件時的指引，以便採取有效且可靠的方式來回應。您採取的實際行動會因事件而有所不同。舉例來說，對於涉及勒索軟體的事件與涉及公有 Amazon S3 儲存貯體的事件將採取不同的回應步驟。此外，這些階段不一定會依序發生。在遏制和根除之後，您可能需要返回分析，以了解採取的行動是否有效。

偵測

提醒是偵測階段的主要元件。它會產生通知，根據感興趣的 AWS 帳戶活動啟動事件回應程序。

警示準確性具有挑戰性；不一定能夠完全確定是否已發生事件、正在進行中，或未來是否會發生。以下是幾個原因：

- 偵測機制是以基準偏差、已知模式和來自內部或外部實體的通知為基礎。
- 由於技術和人員無法預測的性質，分別是安全事件的方法和執行者，基準會隨著時間而變化。惡意模式會透過新的或修改的威脅行為者策略、技術和程序 (TTPs出現。
- 人員、技術和程序的變更不會立即納入事件回應程序中。有些是在調查過程中發現的。

警示來源

您應該考慮使用下列來源來定義提醒：

- 問題清單 – Amazon GuardDuty、AWS Security Hub、Amazon Macie、Amazon Inspector、AWS Config、IAM Access Analyzer 和 Network Access Analyzer 等 AWS 服務會產生可用來製作警示的問題清單。

- 日誌 – 存放在 Amazon S3 儲存貯體和 CloudWatch 日誌群組中的 AWS 服務、基礎設施和應用程式日誌可以進行剖析和關聯，以產生警示。
- 帳單活動 y – 帳單活動的突然變更可能表示安全事件。請遵循建立帳單警示的文件，以監控您的預估 AWS 費用來監控此項目。
- 網路威脅情報 – 如果您訂閱第三方網路威脅情報摘要，您可以將該資訊與其他記錄和監控工具建立關聯，以識別事件的潛在指標。
- 合作夥伴工具 – (APN) AWS Partner Network 中的合作夥伴提供可協助您實現安全目標的頂層產品。對於事件回應，具有端點偵測和回應 (EDR) 或 SIEM 的合作夥伴產品可協助支援您的事件回應目標。如需詳細資訊，請參閱 中的安全合作夥伴解決方案和安全解決方案。 AWS Marketplace
- AWS 信任和安全性 – 如果我們發現濫用或惡意活動， 支援 可能會聯絡客戶。
- 一次性聯絡 – 由於可能是您的客戶、開發人員或您組織中發現異常的其他員工，因此擁有知名且廣為人知的方法來聯絡安全團隊非常重要。熱門選項包括票務系統、聯絡電子郵件地址和 Web 表單。如果您的組織與一般大眾合作，您可能還需要面向公眾的安全聯絡機制。

如需有關您可以在調查期間使用的雲端功能的詳細資訊，請參閱本文件the section called “附錄 A：雲端功能定義”中的 。

做為安全控制工程一部分的偵測

偵測機制是安全控制開發不可或缺的一部分。定義指示和預防性控制時，應建構相關的偵測性和回應性控制。例如，組織會建立與 AWS 帳戶根使用者相關的指令控制，這應該僅用於特定且定義良好的活動。它們將其與使用 AWS 組織的服務控制政策 (SCP) 實作的預防性控制相關聯。如果發生超出預期基準的根使用者活動，則使用 EventBridge 規則和 SNS 主題實作的偵測性控制會提醒安全操作中心 (SOC)。回應式控制需要 SOC 選取適當的手冊、執行分析和工作，直到事件解決為止。

安全控制的最佳定義方式是對在 中執行的工作負載進行威脅建模 AWS。偵測性控制的關鍵性將透過查看特定工作負載的業務影響分析 (BIA) 來設定。偵測性控制項產生的警示不會在進入時處理，而是根據其初始重要性在分析期間進行調整。初始關鍵性集有助於排定優先順序；發生警示的內容將決定其真正的關鍵性。例如，組織使用 Amazon GuardDuty 做為用於屬於工作負載之 EC2 執行個體的偵測控制元件。`Impact:EC2/SuspiciousDomainRequest.Reputation` 會產生調查結果，通知您工作負載中列出的 Amazon EC2 執行個體正在查詢疑似惡意的網域名稱。此提醒預設為低嚴重性，並且隨著分析階段的進展，已確定未經授權的演員`p4d.24xlarge`已部署數百個 類型的 EC2 執行個體，大幅增加組織的營運成本。此時，事件回應團隊會決定將此提醒的重要性調整為高，增加緊迫感並加速進一步的動作。請注意，GuardDuty 調查結果嚴重性無法變更。

Detective 控制實作

請務必了解 如何實作偵測性控制，因為它們有助於判斷警示將如何用於特定事件。技術偵測性控制有兩種主要實作：

- 行為偵測倚賴通常稱為機器學習 (ML) 或人工智慧 (AI) 的數學模型。偵測是透過推論進行；因此，提醒不一定反映實際的事件。
- 規則型偵測是確定性的；客戶可以設定要提醒哪些活動的確切參數，這是確定的。

偵測系統的現代實作，例如入侵偵測系統 (IDS)，通常都具有這兩種機制。以下是使用 GuardDuty 進行規則型和行為偵測的一些範例。

- `Exfiltration:IAMUser/AnomalousBehavior` 產生問題清單時，它會通知您「在您的帳戶中觀察到異常 API 請求。」 當您進一步查看文件時，它會告訴您「ML 模型會評估您帳戶中的所有 API 請求，並識別與對手使用的技術相關聯的異常事件」，指出此調查結果具有行為本質。
- 對於調查結果 `Impact:S3/MaliciousIPCaller`，GuardDuty 正在 CloudTrail 中分析來自 Amazon S3 服務的 API 呼叫，將`SourceIPAddress`日誌元素與包含威脅情報摘要的公有 IP 地址資料表進行比較。一旦找到與項目的直接相符項目，就會產生問題清單。

我們建議您實作行為和規則型警示的混合，因為不一定可以針對威脅模型中的每個活動實作規則型警示。

以人員為基礎的偵測

到目前為止，我們討論了以技術為基礎的偵測。另一個重要的偵測來源來自客戶組織內外的人員。內部人員可以定義為員工或承包商，而外部人員則是安全研究人員、執法部門、新聞和社交媒體等實體。

雖然技術型偵測可以系統化設定，但以人員為基礎的偵測有各種形式，例如電子郵件、票證、郵件、新聞文章、電話和面對面互動。以技術為基礎的偵測通知可以近乎即時地交付，但對於以人員為基礎的偵測沒有時間軸預期。安全文化必須整合、促進和增強以人員為基礎的偵測機制，以深度防禦安全的方法。

Summary

透過偵測，結合規則型和行為驅動警示非常重要。此外，您應該有適當的機制，讓內部和外部人員提交有關安全問題的票證。人類可以是安全事件最有價值的來源之一，因此請務必制定程序，以便人員呈報疑慮。您應該使用環境的威脅模型來開始使用建置偵測。威脅模型將協助您根據與您的環境最相關的威脅建立提醒。最後，您可以使用 MITRE ATT&CK 等架構來了解威脅行為者策略、技術和程序 (TTPs)。MITRE ATT&CK 架構有助於將 作為各種偵測機制的通用語言使用。

分析

日誌、查詢功能和威脅情報是分析階段所需的一些支援元件。許多用於偵測的相同日誌也用於分析，並且需要加入和設定查詢工具。

驗證、範圍和評估提醒的影響

在分析階段，會以目標執行全面的日誌分析，以驗證警示、定義範圍，並評估潛在入侵的影響。

- 驗證提醒是分析階段的進入點。事件回應者將尋找來自各種來源的日誌項目，並直接與受影響工作負載的擁有者互動。
- 範圍是下一個步驟，當所有涉及的資源都被清查，並在利益相關者同意不太可能是誤報之後調整警示重要性。
- 最後，影響分析會詳細說明實際的業務中斷。

識別受影響的工作負載元件後，範圍結果可以與相關工作負載的復原點目標 (RPO) 和復原時間目標 (RTO) 相關聯，並針對警示重要性進行調整，這會啟動資源分配，以及接下來發生的所有活動。並非所有事件都會直接中斷支援業務流程之工作負載的操作。敏感資料揭露、智慧財產權盜竊或資源劫持（如加密貨幣挖掘）等事件可能不會立即停止或破壞業務流程，但日後可能會導致後果。

豐富安全日誌和調查結果

充實威脅情報和組織內容

在分析過程中，感興趣的觀察項目需要擴充以增強提醒的內容化。如準備一節所述，整合和利用網路威脅情報有助於進一步了解安全調查結果。威脅情報服務用於將評價和屬性擁有權指派給公有 IP 地址、網域名稱和檔案雜湊。這些工具提供付費和免費服務。

採用 Amazon Athena 作為日誌查詢工具的客戶可以利用 AWS Glue 任務將威脅情報資訊載入為資料表。威脅情報資料表可用於 SQL 查詢，以關聯日誌元素，例如 IP 地址和網域名稱，提供要分析資料的豐富檢視。

AWS 不會直接提供威脅情報給客戶，但 Amazon GuardDuty 等服務會使用威脅情報來擴充和產生問題清單。您也可以根據自己的威脅情報，將自訂威脅清單上傳至 GuardDuty。

透過自動化擴充

自動化是 AWS 雲端 控管不可或缺的一部分。它可以在事件回應生命週期的各個階段使用。

對於偵測階段，規則型自動化會比對日誌中威脅模型的感興趣模式，並採取適當的動作，例如傳送通知。分析階段可以利用偵測機制，並將警示內文轉送到能夠查詢日誌和充實可觀察項目的引擎，以進行事件的內容化。

警示內文的基本形式是由資源和身分組成。例如，您可以實作自動化來查詢 CloudTrail，了解警示主體在警示期間身分或資源執行的 AWS API 活動，提供額外的洞見，包括 `eventSource`、`SourceIPAddress`、 `eventName`和 已識別`userAgent`的 API 活動。透過以自動化方式執行這些查詢，回應者可以在分類期間節省時間，並取得其他內容，以協助做出更明智的決策。

如需如何使用自動化來豐富 AWS 安全問題清單並簡化分析的範例，請參閱如何使用帳戶中繼資料強化 Security Hub 問題清單部落格文章。

收集和分析鑑識證據

如本文件the section called “準備”章節所述，鑑識是在事件回應期間收集和分析成品的程序。在 上 AWS，它適用於基礎設施網域資源，例如網路流量封包擷取、作業系統記憶體傾印，以及 AWS CloudTrail 日誌等服務網域資源。

鑑識程序具有下列基本特性：

- 一致 – 它遵循記錄的確切步驟，沒有偏差。
- 可重複 – 在針對相同成品重複時，會產生完全相同的結果。
- 慣例 – 它已公開記錄並廣泛採用。

對於事件回應期間收集的成品，維護監管鏈非常重要。除了將成品存放在唯讀儲存庫之外，使用自動化並產生此集合的自動文件也很有幫助。分析應僅對收集成品的確切複本執行，以維護完整性。

收集相關成品

考慮到這些特性，並根據相關提醒和影響和範圍的評估，您將需要收集與進一步調查和分析相關的資料。可能與調查相關的各種資料類型和資料來源，包括服務/控制平面日誌 (CloudTrail、Amazon S3 資料事件、VPC 流程日誌）、資料 (Amazon S3 中繼資料和物件） 和資源 （資料庫、Amazon EC2 執行個體）。

您可以收集服務/控制平面日誌進行本機分析，或者最好直接使用原生 AWS 服務 （如適用） 進行查詢。您可以直接查詢資料 （包括中繼資料），以取得相關資訊或取得來源物件；例如，使用 AWS CLI 取得 Amazon S3 儲存貯體和物件中繼資料，並直接取得來源物件。需要以符合資源類型和預期分析方法的方式收集資源。例如，可以透過建立執行資料庫之系統的複本/快照、建立整個資料庫本身的複本/快照，或從與調查相關的資料庫查詢和擷取特定資料和日誌，來收集資料庫。

對於 Amazon EC2 執行個體，應該收集一組特定的資料，以及應該執行的特定收集順序，以取得並保留最多的資料量以供分析和調查。

具體而言，回應從 Amazon EC2 執行個體取得並保留最多資料量的順序如下：

1. 取得執行個體中繼資料 – 取得與調查和資料查詢相關的執行個體中繼資料（執行個體 ID、類型、IP 地址、VPC/子網路 ID、區域、Amazon Machine Image (AMI) ID、連接的安全群組、啟動時間）。
2. 啟用執行個體保護和標籤 – 啟用執行個體保護，例如終止保護、將關機行為設定為停止（如果設定為終止）、停用連接 EBS 磁碟區的終止時刪除屬性，以及為視覺表示法套用適當的標籤，並在可能的回應自動化中使用（例如，套用名稱為 `Status`和值為 的標籤時`Quarantine`，執行鑑識資料擷取並隔離執行個體）。
3. 取得磁碟 (EBS 快照）– 取得所連接 EBS 磁碟區的 EBS 快照。每個快照都包含將資料還原至新 EBS 磁碟區所需的資訊（從拍攝快照的那一刻開始）。如果您使用執行個體存放區磁碟區，請參閱執行即時回應/成品收集的步驟。
4. 取得記憶體 – 由於 EBS 快照只會擷取已寫入 Amazon EBS 磁碟區的資料，這可能排除應用程式或作業系統在記憶體中存放或快取的資料，因此必須使用適當的第三方開放原始碼或商業工具取得系統記憶體映像，以便從系統取得可用的資料。
5. （選用）執行即時回應/成品收集 – 只有在磁碟或記憶體無法以其他方式取得，或有有效的業務或操作原因時，才能透過系統的即時回應執行目標資料收集（磁碟/disk/memory/logs)。這樣做會修改寶貴的系統資料和成品。
6. 停用執行個體 – 從 Auto Scaling 群組分離執行個體、從負載平衡器取消註冊執行個體，以及調整或套用預先建置的執行個體描述檔，且具有最小化或無許可。
7. 隔離或包含執行個體 – 結束並防止目前和未來的執行個體連線，以確認執行個體與環境中的其他系統和資源有效隔離。如需詳細資訊，請參閱本文件的 the section called “遏制”一節。
8. 回應者的選擇 – 根據情況和目標，選取下列其中一項：
   - 停用並關閉系統（建議）。

     取得可用證據後關閉系統，以驗證最有效的緩解措施，避免執行個體未來對環境造成潛在影響。
   - 在受檢測進行監控的隔離環境中繼續執行執行個體。

     雖然不建議將其做為標準方法， 如果情況值得持續觀察執行個體（例如需要額外的資料或指標來執行執行個體的完整調查和分析）， 您可以考慮關閉執行個體， 建立執行個體的 AMI， 在預先檢測為完全隔離的沙盒環境中，在您的專用鑑識帳戶中重新啟動執行個體，並使用檢測設定，以促進幾乎持續監控執行個體（例如， VPC 流量日誌或 VPC 流量鏡射）。

> **Note**
>
> 在即時回應活動或系統隔離或關閉之前擷取記憶體至關重要，才能擷取可用的揮發性（和有價值的）資料。

開發敘述

在分析和調查期間，記錄所採取的動作、執行的分析和識別的資訊，以供後續階段使用，最終為最終報告。這些敘述應簡潔且精確，確認包含相關資訊，以驗證對事件的有效了解，並維持準確的時間表。當您與核心事件回應團隊以外的人員互動時，它們也很有幫助。請見此處範例：

> 行銷和銷售部門在 2022 年 3 月 15 日收到要求以加密貨幣付款的勒索軟體通知，以避免公開發佈可能的敏感資料。SOC 判定屬於行銷和銷售的 Amazon RDS 資料庫已於 2022 年 2 月 20 日公開存取。SOC 查詢 RDS 存取日誌，並決定 IP 地址 198.51.100.23 是在 2022 年 2 月 20 日使用，其登入資料*mm03434*屬於其中一個 Web 開發人員 Major Mary。SOC 查詢的 VPC 流程日誌，並確定大約 256MB 的資料在相同日期輸出至相同的 IP 地址（時間戳記 2022-02-20T15：50+00Z)。透過開放原始碼威脅情報判定的 SOC 目前可在公有儲存庫 中以純文字提供登入資料*https[:]//example[.]com/majormary/rds-utils*。

遏制

抑制的一個定義，因為它與事件回應相關，是處理安全事件期間策略的程序或實作，其作用是將安全事件的範圍降至最低，並包含環境中未經授權的使用效果。

遏制策略取決於多種因素，而且在實施遏制策略、時機和目的方面，不同組織可能有所不同。NIST SP 800-61 電腦安全事件處理指南概述了決定適當遏制策略的數個條件，其中包括：

- 資源的潛在損壞和遭竊
- 需要證據保留
- 服務可用性（網路連線、提供給外部各方的服務）
- 實作策略所需的時間和資源
- 策略的有效性（部分或完全遏制）
- 解決方案的持續時間（緊急解決方法在四小時內移除，暫時解決方法在兩週內移除，永久解決方案）

不過 AWS，對於 上的服務，基本的遏制步驟可以細分為三個類別：

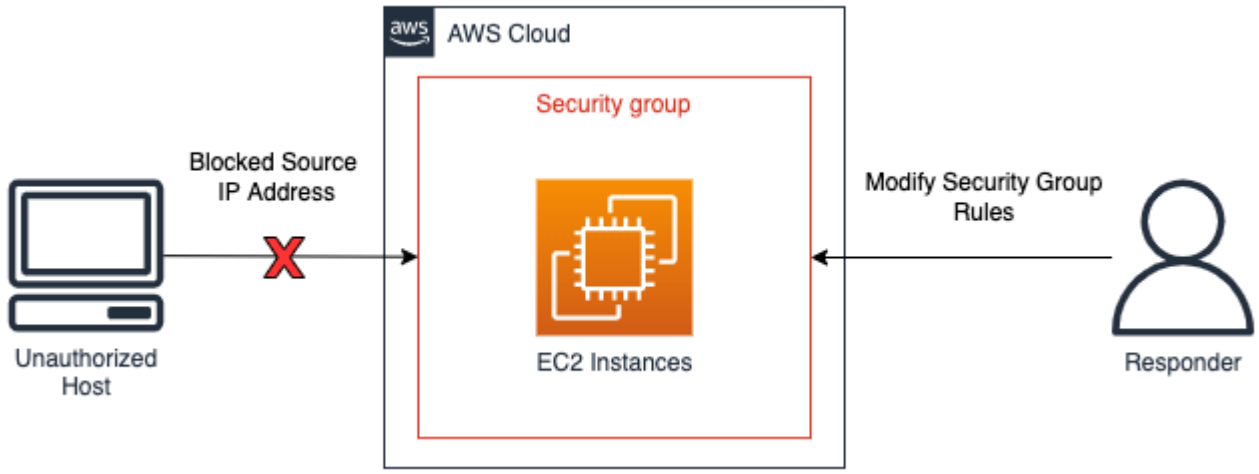
- 來源遏制 – 使用篩選和路由來防止來自特定來源的存取。
- 技術和存取限制 – 移除存取，以防止未經授權存取受影響的資源。
- 目的地遏制 – 使用篩選和路由來防止存取目標資源。

來源遏制

來源遏制是使用和套用環境內的篩選或路由，以防止從特定來源 IP 地址或網路範圍存取資源。使用 AWS 服務的來源遏制範例會反白顯示如下：

- 安全群組 – 建立隔離安全群組並將其套用至 Amazon EC2 執行個體，或從現有安全群組移除規則，有助於包含對 Amazon EC2 執行個體或 AWS 資源的未經授權流量。請務必注意，現有的追蹤連線不會因為變更安全群組而關閉，因為新的安全群組只會有效封鎖未來的流量（如需追蹤和未追蹤連線的其他資訊，請參閱此事件回應手冊和安全群組連線追蹤)。
- 政策 – Amazon S3 儲存貯體政策可設定為封鎖或允許來自 IP 地址、網路範圍或 VPC 端點的流量。政策會建立封鎖可疑地址和存取 Amazon S3 儲存貯體的能力。如需儲存貯體政策的其他資訊，請參閱使用 Amazon S3 主控台新增儲存貯體政策。
- AWS WAF – 可在 上設定 Web 存取控制清單 (Web ACLs) AWS WAF ，以對資源回應的 Web 請求提供精細的控制。您可以將 IP 地址或網路範圍新增至在 上設定的 IP 集 AWS WAF，並將相符條件，例如區塊，套用至 IP 集。如果來自來源流量的 IP 地址或網路範圍符合 IP 集規則中設定的流量，這將封鎖資源的 Web 請求。

下圖顯示來源遏制的範例，其中事件回應分析師修改 Amazon EC2 執行個體的安全群組，以便將新連線限制為僅特定 IP 地址。如安全群組項目符號所述，現有的追蹤連線不會因為變更安全群組而關閉。



來源遏制範例

> **Note**
>
> 安全群組和網路 ACLs 不會篩選 Amazon Route 53 的流量。包含 EC2 執行個體時，如果您想要防止它聯絡外部主機，請確定您也明確封鎖 DNS 通訊。

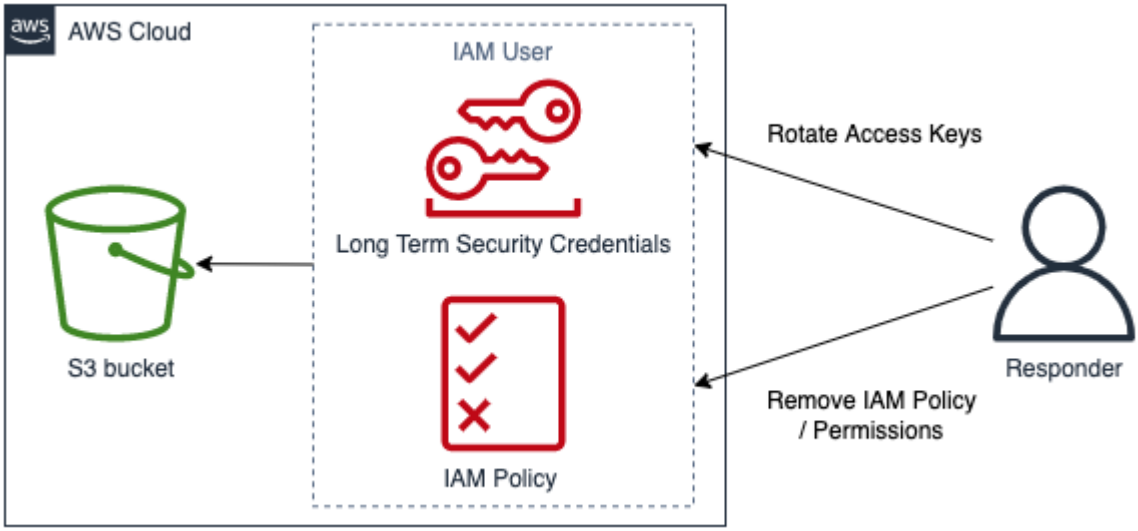
技術和存取限制

限制可存取資源的函數和 IAM 主體，以防止未經授權使用資源。這包括限制有權存取 資源的 IAM 主體的許可；也包括暫時安全登入資料撤銷。使用 AWS 服務的技術和存取限制範例會反白顯示如下：

- 限制許可 – 指派給 IAM 主體的許可應遵循最低權限原則。不過，在作用中的安全事件期間，您可能需要進一步限制從特定 IAM 主體存取目標資源。在這種情況下，可以透過從要包含的 IAM 主體中移除許可來包含對資源的存取。這是使用 IAM 服務完成的，可以使用 AWS CLI、 AWS Management Console或 AWS SDK 套用。
- 撤銷金鑰 – IAM 主體使用 IAM 存取金鑰來存取或管理資源。這些是對 AWS CLI 或 AWS API 簽署程式設計請求的長期靜態登入資料，並以字首 AKIA 開頭（如需詳細資訊，請參閱 IAM 識別符中的了解唯一 ID 字首一節）。若要包含 IAM 存取金鑰遭到入侵的 IAM 主體存取，可以停用或刪除存取金鑰。請務必注意下列事項：
  - 存取金鑰在停用後可以重新啟用。
  - 存取金鑰一旦刪除即無法復原。
  - IAM 主體在任何指定時間最多可以有兩個存取金鑰。
  - 停用或刪除金鑰後，使用存取金鑰的使用者或應用程式將失去存取權。
- 撤銷臨時安全登入資料 – 組織可以使用臨時安全登入資料來控制對 AWS 資源的存取，並以字首 ASIA 開頭（如需詳細資訊，請參閱 IAM 識別符中的了解唯一 ID 字首一節）。臨時登入資料通常由 IAM 角色使用，不需要輪換或明確撤銷，因為它們的生命週期有限。在暫時性安全登入資料過期之前發生涉及暫時性安全登入資料的安全事件時，您可能需要變更現有暫時性安全登入資料的有效許可。這可以使用 內的 IAM 服務 AWS Management Console完成。臨時安全登入資料也可以發行給 IAM 使用者（而不是 IAM 角色）；不過，截至撰寫本文時， 內沒有撤銷 IAM 使用者臨時安全登入資料的選項 AWS Management Console。對於使用者的 IAM 存取金鑰遭到建立臨時安全登入資料之未經授權的使用者入侵的安全事件，可以使用兩種方法撤銷臨時安全登入資料：
  - 將內嵌政策連接至 IAM 使用者，以防止根據安全字符問題時間進行存取（請參閱停用臨時安全憑證許可中的拒絕存取在特定時間之前發行的臨時安全憑證一節，以取得更多詳細資訊）。
  - 刪除擁有遭入侵存取金鑰的 IAM 使用者。視需要重新建立使用者。

- AWS WAF - 未經授權的使用者採用的某些技術包括常見的惡意流量模式，例如包含 SQL Injection 和跨網站指令碼 (XSS) 的請求。 AWS WAF 可以設定為使用 AWS WAF 內建規則陳述式來比對和拒絕採用這些技術的流量。

下圖顯示技術和存取限制的範例，其中事件回應者輪換存取金鑰或移除 IAM 政策，以防止 IAM 使用者存取 Amazon S3 儲存貯體。



技術和存取遏制範例

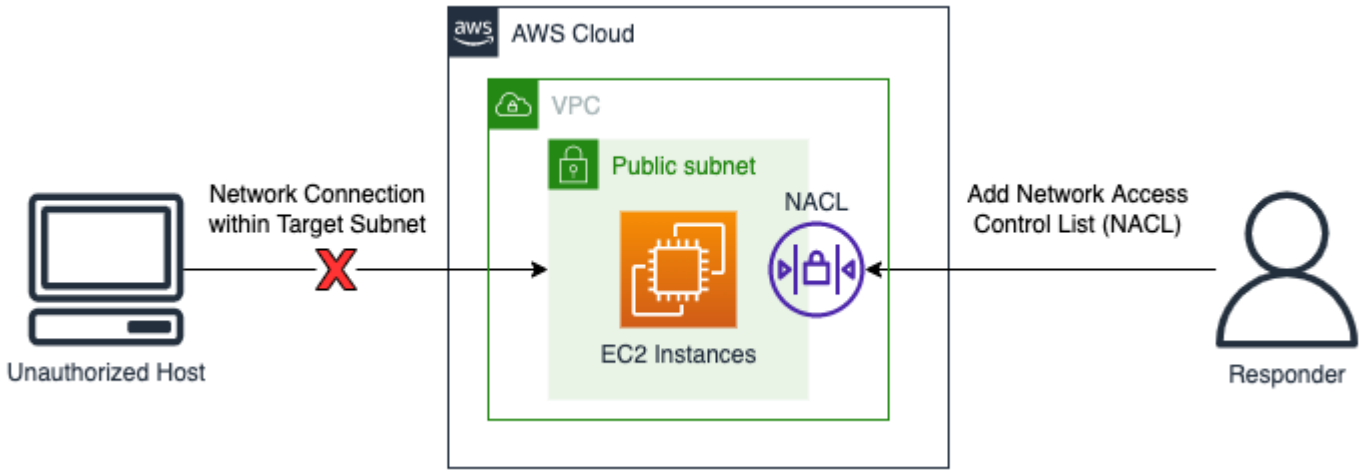
目的地遏制

目的地遏制是在 環境中篩選或路由的應用程式，以防止存取目標主機或資源。在某些情況下，目的地遏制也涉及一種恢復能力形式，以驗證合法資源是否複寫以取得可用性；資源應與這些恢復能力形式分離以隔離和遏制。使用 AWS 服務抑制目的地的範例包括：

- 網路 ACLs – 在包含 AWS 資源的子網路上設定的網路 ACLs （網路 ACLs) 可以新增拒絕規則。這些拒絕規則可以套用以防止存取特定 AWS 資源；不過，套用網路存取控制清單 （網路 ACL) 會影響子網路上的每個資源，而不只是未經授權存取的資源。網路 ACL 中列出的規則會以由上而下順序處理，因此現有網路 ACL 中的第一個規則應設定為拒絕對目標資源和子網路的未經授權流量。或者，可以使用傳入和傳出流量的單一拒絕規則建立全新的網路 ACL，並與包含目標資源的子網路相關聯，以防止使用新的網路 ACL 存取子網路。
- 關閉 – 完全關閉資源可以有效地包含未經授權使用的影響。關閉資源也會防止業務需求的合法存取，並防止取得揮發性鑑識資料，因此這應該是有目的的決策，而且應該根據組織的安全政策進行判斷。

- 隔離 VPCs – 隔離 VPCs可用來有效抑制資源，同時提供合法流量的存取權（例如防毒 (AV) 或需要存取網際網路或外部管理主控台的 EDR 解決方案）。隔離 VPCs可以在安全事件之前預先設定，以允許有效的 IP 地址和連接埠，而且目標資源可以在作用中安全事件期間立即移至此隔離 VPC，以包含資源，同時允許目標資源在事件回應的後續階段期間傳送和接收合法流量。使用隔離 VPC 的一個重要方面是，在使用前需要在新的隔離 VPC 中關閉和重新啟動資源，例如 EC2 執行個體。現有的 EC2 執行個體無法移至另一個 VPC 或其他可用區域。若要這樣做，請依照如何將 Amazon EC2 執行個體移至另一個子網路、可用區域或 VPC 中所述的步驟進行？
- Auto Scaling 群組和負載平衡器 – AWS 連接到 Auto Scaling 群組和負載平衡器的資源應在目的地遏制程序中分離和取消註冊。您可以使用 AWS Management Console AWS CLI、 和 AWS SDK 來執行 AWS 資源分離和取消註冊。

下圖示範了目的地遏制的範例，其中事件回應分析師將網路 ACL 新增至子網路，以封鎖來自未經授權主機的網路連線請求。



目的地遏制範例

Summary

遏制是事件回應程序的一個步驟，可以是手動或自動化。整體遏制策略應符合組織的安全政策和業務需求，並確認在根除和復原之前，盡可能有效地減輕負面影響。

根除

與安全事件回應相關的根除是移除可疑或未經授權的資源，以努力將帳戶返回已知的安全狀態。根除策略取決於多個因素，這取決於組織的業務需求。

NIST SP 800-61 電腦安全事件處理指南提供幾個清除步驟：

1. 識別並緩解所有遭到利用的漏洞。
2. 移除惡意軟體、不適當的材料和其他元件。
3. 如果發現更多受影響的主機（例如，新的惡意軟體感染），請重複偵測和分析步驟來識別所有其他受影響的主機，然後包含並消除它們的事件。

對於 AWS 資源，這可以透過透過 CloudWatch Logs 和 Amazon GuardDuty 等可用日誌或自動化工具偵測到的事件進一步改進。這些事件應該是判斷應執行哪些修補以將環境正確還原至已知安全狀態的基礎。

根除的第一步是判斷哪些資源在 AWS 帳戶中受到影響。這可透過分析可用的日誌資料來源、資源和自動化工具來完成。

- 識別您帳戶中 IAM 身分所採取的未經授權的動作。
- 識別您帳戶的未經授權存取或變更。
- 識別建立未經授權的資源或 IAM 使用者。
- 識別具有未經授權變更的系統或資源。

識別資源清單後，您應該評估每個資源，以確定是否刪除或還原資源對業務的影響。例如，如果 Web 伺服器託管您的商業應用程式，並刪除它會導致停機時間，則您應該考慮從已驗證的安全備份復原資源，或從乾淨的 AMI 重新啟動系統，然後再刪除受影響的伺服器。

完成業務影響分析後，請使用日誌分析中的事件進入帳戶並執行適當的補救措施，例如：

- 輪換或刪除金鑰 - 此步驟會移除演員繼續在帳戶中執行活動的能力。
- 輪換可能未經授權的 IAM 使用者登入資料。
- 刪除無法辨識或未經授權的資源。

> **Important**
>
> 如果您必須保留資源以進行調查，請考慮備份這些資源。例如，如果您因法規、合規或法律原因必須保留 Amazon EC2 執行個體，請在移除執行個體之前建立 Amazon EBS 快照。

- 對於惡意軟體感染，您可能需要聯絡 AWS Partner 或其他廠商。 AWS 不提供惡意軟體分析或移除的原生工具。不過，如果您使用適用於 Amazon EBS 的 GuardDuty 惡意軟體模組，則建議可能可用於提供的調查結果。

清除已識別受影響的資源後， AWS 建議您對帳戶執行安全性審查。這可以使用 AWS Config 規則、使用 Prowler 和 ScoutSuite 等開放原始碼解決方案，或透過其他廠商來完成。您也應考慮對面向公有（網際網路） 的資源執行漏洞掃描，以評估剩餘風險。

根除是事件回應程序的一個步驟，可以根據事件和受影響的資源手動或自動化。整體策略應符合組織的安全政策和業務需求，並確認移除不適當的資源或組態時可減輕負面影響。

復原

復原是將系統還原至已知安全狀態、在還原之前驗證備份是否安全或不受事件影響、測試系統在還原後是否正常運作，以及解決與安全事件相關的漏洞的程序。

復原的順序取決於您組織的需求。在復原過程中，您應該執行業務影響分析，以判斷至少：

- 業務或相依性優先順序
- 還原計畫
- 身分驗證和授權

NIST SP 800-61 電腦安全事件處理指南提供數個復原系統的步驟，包括：

- 從乾淨的備份還原系統。
  - 在還原至系統之前，請確認已評估備份，以確保沒有感染，並防止安全事件再次發生。

    備份應定期評估，作為災難復原測試的一部分，以確認備份機制正常運作，且資料完整性符合復原點目標。
  - 如果可能，請在識別為根本原因分析一部分的第一個事件時間戳記之前使用 的備份。
- 從頭開始重建系統，包括使用自動化從信任來源重新部署，有時在新 AWS 帳戶中。
- 以乾淨的版本取代遭入侵的檔案。

  您應該在執行此操作時特別小心。您必須絕對確定您要復原的檔案是已知安全且不受事件影響的檔案
- 安裝修補程式。
- 變更密碼。
  - 這包括可能遭到濫用的 IAM 主體密碼。
  - 如果可能，我們建議在最低權限策略中使用 IAM 委託人和聯合身分的角色。
- 限制網路周邊安全性 （防火牆規則集、邊界路由器存取控制清單）。

復原資源後，請務必擷取經驗教訓，以更新事件回應政策、程序和指南。

總而言之，必須實作復原程序，以促進返回已知的安全操作。復原可能需要很長的時間，並且需要與遏制策略的緊密連結，才能平衡對重新感染風險的業務影響。復原程序應包含還原資源和服務、IAM 主體，以及執行帳戶安全性審查以評估剩餘風險的步驟。

結論

每個操作階段都有獨特的目標、技術、方法和策略。表 4 摘要說明這些階段，以及本節涵蓋的一些技術和方法。

表 4 – 操作階段：目標、技術和方法

階段	目標	技術和方法
偵測	識別潛在的安全事件。	• 偵測的安全控制 • 行為和規則型偵測 • 以人員為基礎的偵測
分析	判斷安全事件是否為事件，並評估事件的範圍。	• 驗證和範圍提醒 • 查詢日誌 • 威脅情報 • 自動化
遏制	最小化並限制安全事件的影響。	• 來源遏制 • 技術和存取限制 • 目的地遏制
根除	移除與安全事件相關的未經授權資源或成品。	• 遭入侵或未經授權的登入資料輪換或刪除 • 未經授權的資源刪除 • 移除惡意軟體 • 安全性掃描
復原	將系統還原至已知的良好狀態，並監控這些系統，以確保不會傳回威脅。	• 從備份還原系統 • 從頭開始重建的系統 • 已遭入侵的檔案取代為乾淨版本

事後處理

威脅態勢不斷變化，因此組織有效保護環境的能力也務必同樣保持動態。持續改進的關鍵是反覆查看事件和模擬的結果，以改善您的功能，以有效地偵測、回應和調查可能的安全事件、減少可能的漏洞、回應時間，以及返回安全操作。下列機制可協助您驗證組織是否具備最新功能和知識，以便在任何情況下有效回應。

建立從事件中學習的架構

實作經驗教訓的架構和方法不僅有助於改善事件回應功能，也有助於防止事件重複發生。透過從每個事件中學習，您可以協助避免重複相同的錯誤、暴露或錯誤設定，不僅可以改善您的安全狀態，還可以將因可預防的情況而損失的時間降至最低。

實作經驗教訓是非常重要的，其可在高層級實現以下幾點：

- 什麼時候開設經驗教訓課程？
- 經驗教訓課程中包含哪些內容？
- 經驗教訓課程的進行方式？
- 這個課程的參與者以及參與方式？
- 如何識別待改善之處？
- 如何確保有效追蹤和實作改善項目？

除了列出的這些高階成果之外，請務必提出正確的問題，以從程序中衍生出最高價值（導致可行改善的資訊）。考慮這些問題，有助您發起經驗教訓的討論：

- 事件是什麼？
- 第一次識別事件的時間？
- 事件的識別方式？
- 哪些系統對活動發出提醒？
- 涉及哪些系統、服務和資料？
- 具體發生的事件？
- 哪些方面做得很好？
- 哪些方面做得不好？
- 哪個流程或程序失敗或未能擴展以回應事件？
- 在以下幾個領域有哪些可以改善之處：

- 人物
  - 需要聯絡的對象實際上是否有空，並且聯絡人清單是最新的嗎？
  - 人們是否缺少有效回應和調查事件所需的培訓或能力？
  - 適當的資源是否已準備就緒且可供使用？
- 流程
  - 是否遵循流程和程序？
  - 是否已記錄並提供這類事件的流程和程序？
  - 是否缺少必要的流程和程序？
  - 回應人員是否能夠即時存取所需的資訊以回應問題？
- 技術
  - 現有的提醒系統是否能有效地識別活動，並據以發出提醒？
  - 是否需要改善現有提醒，或是需要針對此類事件建立新的提醒？
  - 現有的工具是否允許對事件進行有效的調查（搜尋/分析）？
- 可以做什麼來協助加快這類事件的識別速度？
- 可以做什麼來協助避免這類事件再次發生？
- 負責改善計畫的人是誰，您將如何測試是否已實作此計畫？
- 要實作和測試之額外監控/預防性控制/程序的時間表為何？

此清單並非全包式，旨在作為識別組織和業務需求的起點，以及如何分析這些需求，以最有效地從事件中學習並持續改善您的安全狀態。最重要的是透過將經驗教訓納入事件回應流程，文件和利害關係人期望的標準部分。

建立成功的指標

指標是有效衡量、評估和改善事件回應功能的必要指標。如果沒有指標，則沒有參考可準確測量或甚至識別您的組織效能（或未）。對於尋求建立期望和參考以實現卓越營運的組織而言，事件回應中有一些常見的指標是很好的起點。

平均偵測時間

平均偵測時間是發現潛在安全事件所需的平均時間。具體而言，這是從第一個入侵指標出現到初始識別或提醒之間的時間。

您可以使用此指標來追蹤偵測和警示系統的效能。有效的偵測和提醒機制是驗證可能的安全事件不會停留在您的環境中的關鍵。

平均偵測時間越高，就越需要建立額外或更有效的提醒和機制，以識別和探索可能的安全事件。平均偵測時間越短，偵測和提醒機制的運作就越好。

確認的平均時間

確認的平均時間是確認潛在安全事件並排定優先順序所需的平均時間。具體而言，這是產生警示與 SOC 成員或事件回應人員識別並排定警示優先順序以進行處理之間的時間。

您可以使用此指標來追蹤您的團隊處理和排定警示優先順序的程度。如果您的團隊無法有效識別警示並排定優先順序，則回應將會延遲且無效。

確認的平均時間越高，就越需要驗證您的團隊是否獲得適當的資源和訓練，以快速確認可能的回應安全事件並排定其優先順序。確認的平均時間越短，您的團隊就越能回應安全提醒，表示他們已做好充分準備，並能夠妥善排定優先順序。

平均回應時間

平均回應時間是開始對潛在安全事件的初始回應所需的平均時間。具體而言，這是從可能安全事件的初始提醒或探索到採取第一個回應動作之間的時間。這類似於平均確認時間，但與簡單辨識或確認情況相比，這是特定回應動作（例如，取得系統資料、包含系統）的測量。

您可以使用此指標來追蹤您的準備程度，以回應安全事件。如前所述，準備是有效回應的關鍵。請參閱本文件的 the section called “準備”一節。

回應的平均時間愈長，就愈需要驗證您的團隊都已正確訓練如何回應，以便有效記錄和使用回應程序。回應的平均時間越短，您的團隊就越能識別已識別警示的適當回應，並執行必要的回應動作，以開始返回安全操作的旅程。

包含的平均時間

平均遏制時間是遏制潛在安全事件所需的平均時間。具體而言，這是從潛在安全事件的初始提醒或發現到有效防止攻擊者或遭入侵系統進一步傷害的回應動作完成之間的時間。

您可以使用此指標來追蹤您的團隊緩解或遏制可能安全事件的能力。無法快速有效地遏制可能的安全事件會增加可能進一步入侵的影響、範圍和暴露。

平均遏制時間越高，建置知識和功能的需求就越高，以快速有效地緩解和遏制您遇到的安全事件。控制的平均時間越短，您的團隊就越能理解和採用必要的措施來緩解和控制已識別的威脅，以減少對業務的影響、範圍和風險。

復原的平均時間

復原的平均時間是完全傳回來自可能安全事件的安全操作所需的平均時間。具體而言，這是從潛在安全事件的初始提醒或探索到業務恢復正常運作和安全，而不受事件影響之間的時間。

您可以使用此指標來追蹤您的團隊在安全事件發生後，將系統、帳戶和環境送回安全操作的有效性。無法快速或有效地恢復安全操作不僅會影響安全性，還會增加對業務及其操作的影響和費用。

復原的平均時間越高，您的團隊和環境就越需要準備適當的機制（例如，容錯移轉程序和 CI/CD 管道，以安全重新部署乾淨系統），以將安全事件對營運和業務的影響降至最低。復原的平均時間越短，您的團隊就越能有效地將安全事件對營運和業務的影響降至最低。

攻擊者停留時間

攻擊者停留時間是未經授權的使用者可存取系統或環境的平均時間。這類似於要包含的平均時間，但時間範圍從攻擊者取得系統或環境存取權的初始時間開始，可能早於初始提醒或探索。

您可以使用此指標來追蹤有多少系統和機制一起運作，以減少攻擊者或威脅影響您環境的時間、存取和機會。減少攻擊者停留時間應該是您的團隊和業務的首要任務。

攻擊者停留時間越高，就越需要識別事件回應程序的哪些部分需要改進，以確保您的團隊能夠最大限度地減少環境中威脅或攻擊的影響和範圍。攻擊者停留時間越短，您的團隊就越能將威脅或攻擊者在環境中擁有的時間和機會降至最低，最終降低對您的營運和業務的風險和影響。

指標摘要

建立和追蹤事件回應的指標可讓您有效地測量、評估和改善事件回應功能。為了達成此目的，本節中會反白顯示許多常見的事件回應指標。表 5 摘要說明這些指標。

表 5 – 事件回應指標

指標	描述
平均偵測時間	探索潛在安全事件所需的平均時間
確認的平均時間	確認（和排定優先順序）可能的安全事件所需的平均時間
平均回應時間	開始對潛在安全事件的初始回應所需的平均時間
包含的平均時間	包含可能安全事件所需的平均時間

指標	描述
復原的平均時間	完全傳回來自可能安全事件之安全操作所需的平均時間
攻擊者停留時間	攻擊者可以存取系統或環境的平均時間

使用入侵指標 (IOCs)

入侵指標 (IOC) 是在網路、系統或環境中觀察到的成品，可以（具有高度可信度）識別惡意活動或安全事件。IOCs可以以各種形式存在，包括 IP 地址、網域、網路層級成品，例如 TCP 旗標或承載、系統或主機層級成品，例如可執行檔、檔案名稱和雜湊、日誌檔案項目或登錄項目等。它們也可以是項目或活動的組合，例如系統上存在特定項目或成品（特定檔案或一組檔案和登錄項目）、依特定順序執行的動作（從特定 IP 登入系統，接著特定異常命令），或網路活動（進出特定網域的異常傳入或傳出流量），這些動作可能指出特定威脅、攻擊或攻擊者方法。

當您努力反覆改善事件回應計畫時，您應該實作架構來收集、管理和利用 IOCs做為一種機制，以持續建置和改善偵測和提醒，並改善調查的速度和有效性。您可以從將 IOCs 的收集和管理納入事件回應程序的分析和調查階段開始。透過主動識別、收集和儲存 IOCs 作為程序的標準部分，您可以建置資料儲存庫（做為更全面的威脅情報計劃的一部分），進而用於改善現有的偵測和警示、建立額外的偵測和警示、識別之前看到成品的位置和時間、建置和參考文件，以了解先前如何進行涉及相符 IOCs調查等。

持續教育和訓練

教育和訓練是不斷發展和持續的工作，應刻意追求和維護。有多種機制可以驗證您的團隊是否保持與不斷發展的技術狀態和威脅態勢相符的意識、知識和功能。

一種機制是採用持續教育作為團隊目標和營運的標準部分。如準備一節所述，您的事件回應人員和利益相關者必須接受有效訓練，以偵測、回應和調查其中的事件 AWS。不過，教育不是「一次完成」的工作。必須持續進行教育，以確認您的團隊持續了解最新的技術進展、更新和改進，以改善回應的有效性和效率，以及新增或更新可用於改善調查和分析的資料。

另一個機制是驗證模擬是否定期執行（例如每季），並專注於業務的特定成果。請參閱本文件的 the section called “執行定期模擬”一節。

雖然執行初始桌面練習是產生初始基準以進行改善的好方法，但持續測試是持續改進和維護最新up-to-date且準確反映目前操作狀態的關鍵。針對最新和最關鍵的安全情況以及最重要或最新的回應功能進行

測試，並將學到的經驗納入教育、操作和程序/程序，將驗證您是否能夠持續改善整體的回應程序和程式。

結論

當您繼續雲端旅程時，請務必考慮您 AWS 環境的基本安全事件回應概念。您可以結合可用的控制項、雲端功能和修補選項，協助您改善雲端環境的安全性。您也可以在採用可改善回應速度的自動化功能時啟動小型 並反覆執行，以便在安全事件發生時做好更好的準備。

貢獻者

本文件的目前和過去參與者包括：

- Anna McAbee，Amazon Web Services 資深安全解決方案架構師
- Freddy Kasprzykowski，Amazon Web Services 資深安全顧問
- Jason Hurst，Amazon Web Services 資深安全工程師
- Jonathon Poling，Amazon Web Services 首席安全顧問
- Josh Du Lac，Amazon Web Services 安全解決方案架構資深經理
- Paco Hope，Amazon Web Services 首席安全工程師
- Ryan Tick，Amazon Web Services 資深安全工程師
- Amazon Web Services 資深安全工程師 Steve de Vera

附錄 A：雲端功能定義

AWS 提供超過 200 個雲端服務和數千種功能。其中許多提供原生偵測、預防性和回應功能，而其他功能則可用於架構自訂安全解決方案。本節包含與雲端事件回應最相關的服務子集。

主題

- 記錄和事件
- 可見性和提醒
- 自動化
- 安全儲存
- 未來和自訂安全功能

記錄和事件

AWS CloudTrail – 支援 AWS 帳戶控管、合規、營運稽核和風險稽核 AWS CloudTrail 的服務。使用 CloudTrail，您可以記錄、持續監控和保留與跨 AWS 服務之動作相關的帳戶活動。CloudTrail 提供 AWS 帳戶活動的事件歷史記錄，包括透過 AWS Management Console、 AWS SDKs、命令列工具和其他 AWS 服務採取的動作。此事件歷史記錄可簡化安全分析、資源變更追蹤和故障診斷。CloudTrail 會記錄兩種不同類型的 AWS API 動作：

- CloudTrail 管理事件 （也稱為控制平面操作） 會顯示對您帳戶中資源 AWS 執行的管理操作。這包括建立 Amazon S3 儲存貯體和設定記錄等動作。
- CloudTrail 資料事件 （也稱為資料平面操作） 會顯示在您 AWS 帳戶中的資源上執行或在其中執行的資源操作。這些操作通常是大量活動。這包括 Amazon S3 物件層級 API 活動 （例如 `GetObject`、 `DeleteObject`和 `PutObject` API 操作） 和 Lambda 函數叫用活動等動作。

AWS Config – AWS Config 是一項服務，可讓客戶評估、稽核和評估 AWS 資源的組態。 AWS Config 會持續監控和記錄您的 AWS 資源組態，並可讓您根據所需的組態自動評估記錄的組態。透過 AWS Config，客戶可以手動或自動檢閱 AWS 資源之間組態和關係的變更、詳細的資源組態歷史記錄，並根據客戶準則中指定的組態來判斷整體合規性。這可簡化合規稽核、安全分析、變更管理和操作故障診斷。

Amazon EventBridge – Amazon EventBridge 提供近乎即時的系統事件串流，描述 AWS 資源的變更，或 API 呼叫的發佈時間 AWS CloudTrail。使用您可以快速設定的簡單規則，您可以比對事件並將它們路由到一或多個目標函數或串流。EventBridge 在操作變更時會查覺到。EventBridge 可以回應這些操作變更，並視需要採取修正動作，方法是傳送訊息以回應環境、啟用 函數、進行變更，以及擷取狀態資訊。有些安全服務，例如 Amazon GuardDuty，會以 EventBridge 事件的形式產生輸出。許多安全服務也提供將輸出傳送至 Amazon S3 的選項。

Amazon S3 存取日誌 – 如果敏感資訊存放在 Amazon S3 儲存貯體中，客戶可以啟用 Amazon S3 存取日誌來記錄對該資料的每次上傳、下載和修改。此日誌與記錄儲存貯體本身變更的 CloudTrail 日誌（例如變更存取政策和生命週期政策） 是分開的，此外也是如此。值得注意的是，存取日誌記錄會盡最大努力交付。大多數儲存貯體的要求，為日誌記錄結果適合組態，交付日誌記錄。並不保證伺服器記錄的完成程度與時間先後順序。

Amazon CloudWatch Logs – 客戶可以使用 Amazon CloudWatch Logs，透過 CloudWatch Logs 代理程式監控、存放和存取源自 Amazon EC2 執行個體中執行之作業系統、應用程式和其他來源的日誌檔案。CloudWatch Logs 可以是 AWS CloudTrail Route 53 DNS 查詢、VPC 流程日誌、Lambda 函數等的目的地。然後，客戶可以從 CloudWatch Logs 擷取相關聯的日誌資料。

Amazon VPC 流程日誌 – VPC 流程日誌可讓客戶擷取往返 VPCs 網路介面之 IP 流量的相關資訊。啟用流程日誌後，它們可以串流到 Amazon CloudWatch Logs 和 Amazon S3。VPC Flow Logs 可協助客戶處理許多任務，例如疑難排解為何特定流量未到達執行個體、診斷過於嚴格的安全群組規則，以及將其用作監控 EC2 執行個體流量的安全工具。使用最新版本的 VPC 流程記錄來取得最強大的欄位。

AWS WAF 日誌 – AWS WAF 支援完整記錄服務檢查的所有 Web 請求。客戶可以將它們存放在 Amazon S3 中，以滿足合規和稽核要求，以及偵錯和鑑識。這些日誌協助客戶判斷啟動規則和封鎖 Web 請求的根本原因。日誌可以與第三方 SIEM 和日誌分析工具整合。

Route 53 Resolver 查詢日誌 – Route 53 Resolver 查詢日誌可讓您記錄 Amazon Virtual Private Cloud (Amazon VPC) 內資源所做的所有 DNS 查詢。無論是 Amazon EC2 執行個體、 AWS Lambda 函數或容器，如果它存在於您的 Amazon VPC 中並提出 DNS 查詢，則此功能會記錄它；然後，您可以探索並更好地了解應用程式的運作方式。

其他 AWS 日誌 – AWS 持續為具有新記錄和監控功能的客戶發行服務功能。如需有關每個 AWS 服務可用功能的資訊，請參閱我們的公有文件。

可見性和提醒

AWS Security Hub – AWS Security Hub 為客戶提供高優先順序安全提醒和跨 AWS 帳戶合規狀態的完整檢視。Security Hub 會彙總、組織 Amazon GuardDuty、Amazon Inspector、Amazon Macie 和 AWS Partner 解決方案等 AWS 服務的問題清單，並排定其優先順序。調查結果會以視覺化方式摘要在具有可操作圖形和資料表的整合儀表板上。您也可以根據組織遵循的 AWS 最佳實務和產業標準，使用自動化合規檢查來持續監控您的環境。

Amazon GuardDuty – Amazon GuardDuty 是一種受管威脅偵測服務，會持續監控惡意或未經授權的行為，協助客戶保護 AWS 帳戶和工作負載。它會監控活動，例如異常 API 呼叫或潛在未經授權的部署，指出對 Amazon EC2 執行個體、Amazon S3 儲存貯體或惡意行為者偵察的可能帳戶或資源遭到入侵。

GuardDuty 透過整合式威脅情報摘要，使用機器學習來偵測帳戶和工作負載活動的異常狀況，藉此識別可疑的惡意行為者。偵測到潛在威脅時，服務會向 GuardDuty 主控台和 CloudWatch Events 傳送詳細的安全提醒。這可讓警示變得可行且易於整合到現有的事件管理和工作流程系統中。

GuardDuty 也提供兩個附加元件來監控具有特定服務的威脅：Amazon GuardDuty for Amazon S3 protection 和 Amazon GuardDuty for Amazon EKS protection。Amazon S3 保護可讓 GuardDuty 監控物件層級 API 操作，以識別 Amazon S3 儲存貯體內資料的潛在安全風險。Kubernetes 保護可讓 GuardDuty 偵測 Amazon EKS 內 Kubernetes 叢集的可疑活動和潛在入侵。

Amazon Macie – Amazon Macie 是一種採用 AI 的安全服務，可透過自動探索、分類和保護存放在 中的敏感資料，協助防止資料遺失 AWS。Macie 使用機器學習 (ML) 來識別敏感資料，例如個人身分識別資訊 (PII) 或智慧財產權、指派商業價值，並提供此資料在組織中存放位置及其使用方式的可見

性。Amazon Macie 會持續監控資料存取活動是否有異常，並在偵測到未經授權存取或意外資料外洩的風險時傳送提醒。

AWS Config 規則 – AWS Config 規則代表資源的偏好組態，並針對相關資源上的組態變更進行評估，如 所記錄 AWS Config。您可以查看針對儀表板上資源組態評估規則的結果。使用 AWS Config 規則，您可以從組態角度評估整體合規和風險狀態、檢視一段時間內的合規趨勢，以及找出導致資源不符合規則的組態變更。

AWS Trusted Advisor – AWS Trusted Advisor 是一種線上資源，可透過最佳化您的 AWS 環境來協助您降低成本、提高效能和提高安全性。 Trusted Advisor 提供即時指引，協助您遵循 AWS 最佳實務來佈建資源。商業和企業支援計劃客戶可以使用整組 Trusted Advisor 檢查，包括 CloudWatch Events 整合。

Amazon CloudWatch – Amazon CloudWatch 是一種監控服務，適用於 AWS 雲端 資源和您執行的應用程式 AWS。您可以使用 CloudWatch 來收集和追蹤指標、收集和監控日誌檔案、設定警示，並自動回應 AWS 資源的變更。CloudWatch 可以監控 AWS 資源，例如 Amazon EC2 執行個體、Amazon DynamoDB 資料表和 Amazon RDS 資料庫執行個體，以及應用程式和服務產生的自訂指標，以及應用程式產生的任何日誌檔案。您可以使用 Amazon CloudWatch 來全面了解資源使用率、應用程式效能和運作狀態。您可以使用這些洞見來做出相應反應，並讓您的應用程式順利執行。

Amazon Inspector – Amazon Inspector 是一種自動化安全評估服務，可協助改善部署在 上應用程式的安全性和合規性 AWS。Amazon Inspector 會自動評估應用程式是否有漏洞或與最佳實務的偏差。執行評估之後，Amazon Inspector 會產生安全調查結果的詳細清單，依嚴重性層級排定優先順序。這些調查結果可以直接檢閱，也可以作為詳細評估報告的一部分，這些報告可透過 Amazon Inspector 主控台或 API 取得。

Amazon Detective – Amazon Detective 是一項安全服務，可自動從您的 AWS 資源收集日誌資料，並使用機器學習、統計分析和圖形理論來建置一組連結的資料，讓您能夠更快、更有效率地進行安全調查。Detective 可以分析來自多個資料來源的數兆個事件，例如 VPC 流程日誌、CloudTrail 和 GuardDuty，並自動建立資源、使用者及其之間隨時間互動的統一互動式檢視。透過此統一檢視，您可以在一個位置視覺化所有詳細資訊和內容，以識別調查結果的基礎原因、深入了解相關的歷史活動，並快速判斷根本原因。

自動化

AWS Lambda – AWS Lambda 是一種無伺服器運算服務，可執行程式碼以回應事件，並自動為您管理基礎運算資源。您可以使用 Lambda AWS 來擴展具有自訂邏輯的其他服務，或建立您自己的後端服務，以 AWS 大規模運作、效能和安全性。Lambda 會在高可用性運算基礎設施上執行程式碼，並為您執行運算資源的管理。這包括伺服器和作業系統維護、容量佈建和自動擴展、程式碼和安全性修補程式部署，以及程式碼監控和記錄。您只需提供程式碼即可。

AWS Step Functions – AWS Step Functions 使用視覺化工作流程輕鬆協調分散式應用程式和微服務的元件。Step Functions 提供圖形主控台，可讓您將應用程式的元件排列和視覺化為一系列步驟。這可讓您輕鬆地建置和執行多步驟應用程式。Step Functions 會自動啟動和追蹤每個步驟，並在發生錯誤時重試，讓您的應用程式依預期順序執行。

Step Functions 會記錄每個步驟的狀態，因此當發生問題時，您可以快速診斷和偵錯問題。您可以變更和新增步驟，而無需編寫程式碼，因此您可以加快應用程式的發展和創新速度。 AWS Step Functions 是 AWS Serverless 的一部分，可讓您輕鬆協調無伺服器應用程式的 AWS Lambda 函數。您也可以使用 Step Functions 來使用 Amazon EC2 和 Amazon ECS 等運算資源進行微服務協調。

AWS Systems Manager – AWS Systems Manager 為您提供基礎設施的可見性和控制 AWS。Systems Manager 提供統一的使用者介面，讓您可以檢視來自多個 AWS 服務的操作資料，並可讓您自動化跨 AWS 資源的操作任務。使用 Systems Manager，您可以依應用程式分組資源、檢視用於監控和故障診斷的操作資料，以及對資源群組採取行動。Systems Manager 可以將執行個體保持在其定義的狀態、執行隨需變更，例如更新應用程式或執行 shell 指令碼，以及執行其他自動化和修補任務。

安全儲存

Amazon Simple Storage Service – Amazon S3 是物件儲存體，用於從任何地方存放和擷取任意數量的資料。它旨在提供 99.999999999% 的耐用性，並存放每個產業中市場領導者使用的數百萬個應用程式的資料。Amazon S3 提供全方位的安全性，旨在協助您符合法規要求。它讓客戶能夠靈活地管理成本最佳化、存取控制和合規的資料。Amazon S3 query-in-place功能，可讓您直接在 Amazon S3 中的靜態資料上執行強大的分析。Amazon S3 是高度支援的雲端儲存服務，整合來自第三方解決方案、系統整合商合作夥伴和其他 AWS 服務的最大社群之一。

Amazon S3 Glacier – Amazon S3 Glacier 是一種安全、耐用且成本極低的雲端儲存服務，可用於資料封存和長期備份。它旨在提供 99.999999999% 的耐用性，提供全面的安全性，旨在協助您滿足法規要求。S3 Glacier query-in-place功能，可讓您直接在靜態封存資料上執行強大的分析。為了降低成本，但適合各種擷取需求，S3 Glacier 提供三種存取封存的選項，從幾分鐘到幾個小時不等。

未來和自訂安全功能

上述服務和功能並非詳盡清單。 AWS 會持續新增新功能。如需詳細資訊，建議您檢閱 和AWS 雲端安全頁面的最新消息 AWS。除了 做為原生雲端服務 AWS 提供的安全服務之外，您可能還有興趣在 AWS 服務之外建置自己的功能。

雖然我們建議您在帳戶中啟用一組基本安全服務 AWS CloudTrail，例如 Amazon GuardDuty 和 Amazon Macie，但您可能最終想要擴展這些功能，以從您的日誌資產衍生額外的值。有許多可用的合作夥伴工具，例如我們的 APN 安全能力計劃中列出的工具。您也可以撰寫自己的查詢來搜尋日誌。透過 AWS 提供的大量受管服務，這從未如此簡單。還有許多額外的 AWS 服務可協助您進行本文範

圍外的調查，例如 Amazon Athena、Amazon OpenSearch Service、Amazon QuickSight、Amazon Machine Learning 和 Amazon EMR。

附錄 B： AWS 事件回應資源

AWS 發佈資源，協助客戶開發事件回應功能。大多數的範例程式碼和程序都可以在外部 GitHub 公有 AWS 儲存庫中找到。以下是一些資源，提供如何執行事件回應的範例。

Playbook 資源

- 事件回應手冊架構 - 客戶建立、開發和整合安全手冊的範例架構，以準備使用 AWS 服務時的潛在攻擊案例。
- 事件回應手冊範例 - 涵蓋 AWS 客戶所面對常見案例的手冊。
- AWS CIRT 宣布推出五個公開可用的研討會。

鑑識資源

- 自動化事件回應和鑑識架構 – 此架構和解決方案提供標準數位鑑識程序，包含下列階段：遏制、取得、檢查和分析。它利用 AWS Λ 函數，以自動可重複的方式觸發事件回應程序。它提供帳戶隔離，以操作自動化步驟、存放成品並建立鑑識環境。
- 適用於 Amazon EC2 的自動鑑識協調器 – 此實作指南提供自助式解決方案，可擷取和檢查 EC2 執行個體和連接磁碟區中的資料，以便在偵測到潛在安全問題時進行鑑識分析。有一個部署解決方案的 AWS CloudFormation 範本。
- 如何在 中自動化鑑識磁碟收集 AWS – 此 AWS 部落格詳細說明如何設定自動化工作流程來擷取磁碟證據進行分析，以判斷潛在安全事件的範圍和影響。也包含部署解決方案的 AWS CloudFormation 範本。

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品產品和實務，這些產品和實務可能會有所變更，恕不另行通知，且 (c) 不會對 AWS 及其附屬公司、供應商或授權方提供「原樣」的任何承諾或保證。 AWS 產品或服務不提供任何類型的保證、聲明或條件，無論明示或暗示。 AWS 對其客戶的責任和責任由 AWS 協議控制，本文件不屬於，也不會修改 AWS 與其客戶之間的任何協議。

© 2024 Amazon Web Services， Inc. 或其附屬公司。保留所有權利。

文件歷史記錄

變更	描述	日期
新增 Amazon EventBridge 與 AWS 安全事件回應整合的頁面。	說明 Amazon EventBridge 如何在 AWS 安全事件回應中建構的新內容區段。	2025 年 6 月 26 日
更新 SLR 新增許可以支援服務權利。	AWSSecurityIncidentResponseTriageServiceRolePolicy 已更新，新增 security-ir：GetMembership、 security-ir：ListMemberships、 security-ir：UpdateCase、guardduty：ListFilters、guarduty：UpdateFilter、guardduty：DeleteFilter 和 guardduty：GetAdministratorAccount 許可。已新增 guardduty：GetAdministratorAccount，以協助管理委派帳戶中的 GuardDuty Auto-Archival 篩選條件。	2025 年 6 月 2 日
資源更新。	更新 https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html#playbook-resources：//。	2025 年 5 月 23 日
服務支援日文語言。	更新支援的組態，以識別日本當地時間的日文語言支援。全球支援英文。	2025 年 5 月 13 日
內容更新和客戶意見回饋。	將備註新增至 https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-	2025 年 5 月 9 日

變更	描述	日期
	membership-account.html：//。 更新了使用服務產生的案例和偵測和分析時的客戶體驗。 更新帳戶取消詳細資訊，以更清楚說明取消會員資格的帳單影響。	
新增三個新的支援區域。	已將三個新區域新增至 https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html。孟買、巴黎和聖保羅。	2025 年 5 月 7 日
更新：來自客戶對文件的評論的更新。	多個頁面上的拼寫和文法錯誤正確。 已更新 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/organizations_permissions.html，以準確反映 security-ir 做為服務字首。 已將 Route53 和 DNS 的相關備註新增至 https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html。	2025 年 2 月 7 日

變更	描述	日期
更新：來自客戶對文件的評論的更新。	將 https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html 更新為堆疊集範本。 已將項目 triage.security-ir.com 更正為 triage.security-ir.amazonaws.com 在 https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html：// 新增 AWSSupport-ContainEC2Reversible 的追蹤連線備註。 已修正 https：//https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html 上的中斷連結。 在 https：//https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html 新增成員資格帳戶的定義。 在 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/using-service-linked-roles.html 中新增管理 AWS Organizations 帳戶的澄清說明。	2024 年 12 月 20 日

變更	描述	日期
更新：來自客戶對文件的評論的更新。	移除文字 AWS AWS 中的多個重複項目。 修正 https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html 和 https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html 上的中斷連結。 https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html 的更新。從第一個段落移除 >。以 AWSSupport-ContainEC2Instance 取代 AWSSupport-ContainEC2Reversible。 AWSSupport-ContainEC2Instance 將 AWSSupport-ContainIAMReversible為 AWSSupport-ContainIAMPrincipal。將 AWSSupport-ContainS3Reversible為 AWSSupport-ContainS3Resource。 在 https：//https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html 上更新格式 告知客戶透過支援票證聯絡 CIRT 時，https：//https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-su	2024 年 12 月 10 日

變更	描述	日期
	pport.html 現在提供在支援表單中選取的選項。 移除 CloudWatch Events，並取代為 https：//https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html 上的 EventBridge。 https：//https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html 上的文法更新。 從 https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html 移除發佈日期，並以此表格中的更新取代。	
已更新： AWS 受管政策和服務連結角色。	受管政策和服務連結角色的更新。	2024 年 12 月 1 日
服務啟動	在 re：Invent 2024 啟動服務的初始服務文件	2024 年 12 月 1 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。