合作夥伴整合指南

AWS Security Hub

AWS Security Hub: 合作夥伴整合指南

Table of Contents

第三方與 整合的概觀 AWS Security Hub

本指南適用於想要與 建立整合的 AWS 合作夥伴網路 (APN) 合作夥伴 AWS Security Hub。

身為 APN 合作夥伴，您可以透過下列一種或多種方式與 Security Hub 整合。

- 將問題清單傳送至 Security Hub
- 使用 Security Hub 的調查結果
- 兩者都會將問題清單傳送至 Security Hub 並使用問題清單
- 使用 Security Hub 做為受管安全服務提供者 (MSSP) 方案的中心
- 諮詢 AWS 客戶如何部署和使用 Security Hub

本入門指南主要著重於將問題清單傳送至 Security Hub 的合作夥伴。

主題

為什麼要與 整合 AWS Security Hub？

AWS Security Hub 提供 Security Hub 帳戶中高優先順序安全提醒和安全狀態的完整檢視。Security Hub 可讓像您這樣的合作夥伴將安全調查結果傳送至 Security Hub，讓您的客戶深入了解您產生的安全調查結果。

與 Security Hub 的整合可以透過下列方式新增值。

- 滿足請求 Security Hub 整合的客戶
- 為您的客戶提供與 AWS 安全相關的調查結果的單一檢視
- 允許新客戶在尋找提供特定類型安全事件相關調查結果的合作夥伴時，探索您的解決方案

建立與 Security Hub 的整合之前，請先檢查整合的原因。如果您的客戶想要將 Security Hub 與您的產品整合，整合就更有可能成功。您可以僅基於行銷原因或取得新客戶而建置整合。不過，如果您在沒有目前客戶輸入的情況下建置整合，且未考慮客戶的需求，整合可能不會產生預期的結果。

準備將問題清單傳送至 AWS Security Hub

身為 APN 合作夥伴，您無法將資訊傳送給客戶 Security Hub，直到 Security Hub 團隊啟用您做為調查結果提供者。若要啟用 做為調查結果提供者，您必須完成下列加入步驟。這樣做可確保您和客戶的 Security Hub 獲得正面體驗。

當您完成加入步驟時，請務必遵循 the section called “用於建立和更新問題清單的 Tenet”、 the section called “ASFF 映射的指導方針”和 中的準則the section called “使用 `BatchImportFindings` API 的指導方針”。

1. 將您的安全問題清單映射至 AWS 安全問題清單格式 (ASFF)。
2. 建置您的整合架構，將問題清單推送至正確的 Regional Security Hub 端點。若要這樣做，您可以定義要從自己的 AWS 帳戶還是從客戶帳戶內傳送問題清單。
3. 讓您的客戶將產品訂閱到其帳戶。若要這樣做，他們可以使用 主控台或 `EnableImportFindingsForProduct` API 操作。請參閱 AWS Security Hub 使用者指南中的管理產品整合。

   您也可以為他們訂閱產品。若要這樣做，您可以使用跨帳戶角色來代表客戶存取 `EnableImportFindingsForProduct` API 操作。

   此步驟會建立所需的資源政策，以接受該帳戶的該產品調查結果。

下列部落格文章討論一些現有的合作夥伴與 Security Hub 的整合。

- 宣布雲端託管整合 AWS Security Hub
- 使用 AWS Fargate 和 Prowler 將有關 AWS 服務的安全組態問題清單傳送至 Security Hub
- 如何在 Security Hub 中將 AWS Config 規則評估匯入為調查結果

準備從 接收問題清單 AWS Security Hub

若要從 接收問題清單 AWS Security Hub，請使用下列其中一個選項：

- 讓您的客戶自動將所有調查結果傳送至 CloudWatch Events。客戶可以建立特定的 CloudWatch 事件規則，將問題清單傳送至特定目標，例如 SIEM 或 S3 儲存貯體。
- 讓您的客戶從 Security Hub 主控台中選取特定問題清單或問題清單群組，然後對其採取行動。

例如，您的客戶可以將問題清單傳送到 SIEM、票證系統、聊天平台或修復工作流程。這將是客戶在 Security Hub 中執行的警示分類工作流程的一部分。

這些稱為自訂動作。當使用者採取自訂動作時，會為這些特定問題清單建立 CloudWatch 事件。身為合作夥伴，您可以利用此功能，並建置 CloudWatch 事件規則或目標，供客戶做為自訂動作的一部分使用。請注意，此功能不會自動將特定類型或類別的所有調查結果傳送至 CloudWatch Events。此功能可供使用者對特定問題清單採取動作。

下列部落格文章概述了針對自訂動作使用與 Security Hub 和 CloudWatch Events 整合的解決方案。

- 如何整合 AWS Security Hub 自訂動作與 PagerDuty
- 如何在 中啟用自訂動作 AWS Security Hub
- 如何在 Security Hub 中將 AWS Config 規則評估匯入為調查結果

了解 的資源 AWS Security Hub

下列資料可協助您更了解 AWS Security Hub 解決方案，以及 AWS 客戶如何使用 服務。

- 影片簡介 AWS Security Hub
- Security Hub 使用者指南
- Security Hub API 參考
- 加入網路研討會

我們也鼓勵您在其中一個 AWS 帳戶中啟用 Security Hub，並取得一些服務的實際操作體驗。

合作夥伴先決條件

您必須先符合下列其中一項條件 AWS Security Hub，才能開始與 整合：

- 您是 AWS Select Tier 合作夥伴或更高階。
- 您已加入 AWS ISV 合作夥伴路徑，且您用於 Security Hub 整合的產品已完成AWS 基礎技術審查 (FTR)。然後，產品會獲授予「檢閱者 AWS」徽章。

您還必須與 簽訂相互保密協議 AWS。

整合使用案例和必要的許可

AWS Security Hub 允許 AWS 客戶從 APN 合作夥伴接收調查結果。合作夥伴的產品可能會在客戶 AWS 帳戶內外執行。客戶帳戶中的許可組態會根據合作夥伴產品使用的模型而有所不同。

在 Security Hub 中，客戶一律會控制哪些合作夥伴可以將問題清單傳送到客戶的帳戶。客戶可以隨時撤銷合作夥伴的許可。

若要讓合作夥伴將安全調查結果傳送到其帳戶，客戶會先訂閱 Security Hub 中的合作夥伴產品。訂閱步驟對於以下概述的所有使用案例都是必要的。如需客戶如何管理產品整合的詳細資訊，請參閱AWS Security Hub 《使用者指南》中的管理產品整合。

客戶訂閱合作夥伴產品後，Security Hub 會自動建立受管資源政策。此政策授予合作夥伴產品許可，以使用 `BatchImportFindings` API 操作將問題清單傳送到客戶帳戶的 Security Hub。

以下是與 Security Hub 整合之合作夥伴產品的常見案例。此資訊包含每個使用案例所需的額外許可。

合作夥伴託管：從合作夥伴帳戶傳送的問題清單

此使用案例涵蓋在自己的 AWS 帳戶中託管產品的合作夥伴。若要傳送 AWS 客戶的安全調查結果，合作夥伴會從合作夥伴產品帳戶呼叫 `BatchImportFindings` API 操作。

在此使用案例中，客戶帳戶只需要在客戶訂閱合作夥伴產品時建立的許可。

在合作夥伴帳戶中，呼叫 `BatchImportFindings` API 操作的 IAM 主體必須具有允許主體呼叫 的 IAM 政策`BatchImportFindings`。

讓合作夥伴產品在 Security Hub 中傳送問題清單給客戶是一個兩步驟的程序：

1. 客戶在 Security Hub 中建立合作夥伴產品的訂閱。
2. Security Hub 會產生正確的受管資源政策，其中包含客戶的確認。

若要傳送與客戶帳戶相關的安全調查結果，合作夥伴產品會使用自己的登入資料來呼叫 `BatchImportFindings` API 操作。

以下是 IAM 政策的範例，該政策授予合作夥伴帳戶中的委託人必要的 Security Hub 許可。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:*:product-subscription/company-
name/product-name"
        }
    ]
}
```

合作夥伴託管：從客戶帳戶傳送的問題清單

此使用案例涵蓋在其自己的 AWS 帳戶中託管產品的合作夥伴，但使用跨帳戶角色來存取客戶的帳戶。他們從客戶的帳戶呼叫 `BatchImportFindings` API 操作。

在此使用案例中，若要呼叫 `BatchImportFindings` API 操作，合作夥伴帳戶會擔任客戶帳戶中的客戶受管 IAM 角色。

此呼叫是從客戶的帳戶進行。因此，受管資源政策必須允許在呼叫中使用合作夥伴產品帳戶的產品 ARN。Security Hub 受管資源政策會授予合作夥伴產品帳戶和合作夥伴產品 ARN 的許可。產品 ARN 是合作夥伴作為供應商的唯一識別符。由於呼叫不是來自合作夥伴產品帳戶，客戶必須明確授予許可，讓合作夥伴產品將問題清單傳送到 Security Hub。

合作夥伴和客戶帳戶之間跨帳戶角色的最佳實務是使用合作夥伴提供的外部識別符。此外部識別符是客戶帳戶中跨帳戶政策定義的一部分。合作夥伴在擔任角色時必須提供識別符。外部識別符在將 AWS 帳戶存取權授予合作夥伴時提供額外的安全層。唯一識別符可確保合作夥伴使用正確的客戶帳戶。

使用跨帳戶角色，讓合作夥伴產品將問題清單傳送給 Security Hub 中的客戶，分為四個步驟：

1. 客戶或合作夥伴使用代表客戶工作的跨帳戶角色，開始訂閱 Security Hub 中的產品。
2. Security Hub 會產生正確的受管資源政策，其中包含客戶的確認。
3. 客戶可手動或使用 來設定跨帳戶角色 AWS CloudFormation。如需跨帳戶角色的資訊，請參閱《IAM 使用者指南》中的提供存取第三方擁有 AWS 的帳戶。
4. 產品會安全地存放客戶角色和外部 ID。

接下來，產品會將問題清單傳送至 Security Hub：

1. 產品會呼叫 AWS Security Token Service (AWS STS) 以擔任客戶角色。

2. 產品會使用擔任角色的臨時登入資料呼叫 Security Hub 上的 BatchImportFindings API 操作。

以下是將必要的 Security Hub 許可授予合作夥伴的跨帳戶角色的 IAM 政策範例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

政策的 Resource區段識別特定產品訂閱。這可確保合作夥伴只能傳送客戶訂閱之合作夥伴產品的調查結果。

客戶託管：從客戶帳戶傳送的問題清單

此使用案例涵蓋合作夥伴，其擁有部署在客戶 AWS 帳戶中的產品。BatchImportFindings API 是從客戶帳戶中執行的解決方案呼叫。

對於此使用案例，必須授予合作夥伴產品呼叫 BatchImportFindings API 的額外許可。授予此許可的方式會因合作夥伴解決方案以及其在客戶帳戶中的設定方式而有所不同。

此方法的範例為在客戶帳戶中的 EC2 執行個體上執行的合作夥伴產品。此 EC2 執行個體必須連接 EC2 執行個體角色，以授予該執行個體呼叫 BatchImportFindings API 操作的能力。這可讓 EC2 執行個體將安全調查結果傳送至客戶帳戶。

此使用案例在功能上等同於客戶將調查結果載入其帳戶，以取得其擁有的產品。

客戶可讓合作夥伴產品在 Security Hub 中將調查結果從客戶的帳戶傳送給客戶：

1. 客戶使用 AWS CloudFormation或其他部署工具，將合作夥伴產品手動部署到其 AWS 帳戶。
2. 客戶為合作夥伴產品定義必要的 IAM 政策，以便在將問題清單傳送到 Security Hub 時使用。
3. 客戶會將政策連接到合作夥伴產品的必要元件，例如 EC2 執行個體、容器或 Lambda 函數。

現在，產品可以將問題清單傳送到 Security Hub：

1. 合作夥伴產品使用 AWS SDK 或 AWS CLI 來呼叫 Security Hub 中的 BatchImportFindings API 操作。它會從附加政策的客戶帳戶中的元件進行呼叫。
2. 在 API 呼叫期間，會產生必要的臨時憑證，以允許BatchImportFindings呼叫成功。

以下是將必要的 Security Hub 許可授予客戶帳戶中合作夥伴產品的 IAM 政策範例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-2:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

合作夥伴加入程序

身為合作夥伴，您可以預期完成幾個高階步驟，做為加入程序的一部分。您必須完成這些步驟，才能將安全調查結果傳送到 AWS Security Hub。

1. 您開始與 APN 合作夥伴團隊或 Security Hub 團隊互動，並表達成為 Security Hub 合作夥伴的興趣。您可以識別要新增至 Security Hub 通訊管道的電子郵件地址。
2. AWS 為您提供 Security Hub 合作夥伴加入資料。
3. 您受邀使用 Security Hub 合作夥伴 Slack 管道，您可以在其中提出與整合相關的問題。
4. 您向 APN 合作夥伴聯絡人提供產品整合清單草案以供審核。

   產品整合資訊清單包含用來建立與 整合之合作夥伴產品 Amazon Resource Name (ARN) 的資訊 AWS Security Hub。

   它為 Security Hub 團隊提供顯示在 Security Hub 主控台中合作夥伴提供者頁面上的資訊。它也用於提議與整合相關的新受管洞見，以新增至 Security Hub 洞見程式庫。

   此初始版本的產品整合資訊清單不需要擁有完整詳細資訊。但至少應包含使用案例和資料集資訊。

   如需資訊清單和必要資訊的詳細資訊，請參閱產品整合資訊清單。
5. Security Hub 團隊會為您的產品提供產品 ARN。您可以使用 ARN 將問題清單傳送至 Security Hub。
6. 您可以建置整合，將問題清單傳送至 Security Hub 或從 Security Hub 接收問題清單。

   將問題清單映射至 ASFF

   若要將問題清單傳送至 Security Hub，您必須將問題清單映射至 AWS 安全問題清單格式 (ASFF)。

   ASFF 提供一致的問題清單描述，可在安全服務、合作夥伴和客戶安全系統之間 AWS 共用。這可減少整合工作、鼓勵常用語言，並為實作者提供藍圖。

   ASFF 是用來傳送問題清單的必要線路通訊協定格式 AWS Security Hub。調查結果以 JSON 文件表示，其遵循 ASFF JSON 結構描述和 RFC-7493 I-JSON 訊息格式。如需 ASFF 結構描述的詳細資訊，請參閱AWS Security Hub 《 使用者指南》中的AWS 安全調查結果格式 (ASFF)。

   請參閱 the section called “ASFF 映射的指導方針”。

建置和測試整合

您可以使用您 AWS 擁有的帳戶，完成整合的所有測試。這樣做可讓您完全了解問題清單在 Security Hub 中的顯示方式。它還可協助您了解客戶對您的安全調查結果的體驗。

您可以使用 `BatchImportFindings` API 操作，將新的和更新的調查結果傳送至 Security Hub。

在整個 Security Hub 整合的建置過程中， AWS 鼓勵您讓 APN 合作夥伴聯絡人隨時了解整合進度。您也可以向 APN 合作夥伴聯絡人尋求整合問題的協助。

請參閱 the section called “使用 BatchImportFindings API 的指導方針”。

7. 您會示範與 Security Hub 產品團隊的整合。此整合必須使用 Security Hub 團隊擁有的帳戶進行示範。

   如果他們對整合感到滿意，Security Hub 團隊會核准繼續將您列為供應商。
8. 您 AWS 提供最終資訊清單以供審核。
9. Security Hub 團隊會在 Security Hub 主控台中建立提供者整合。然後，客戶可以探索和啟用整合。
10. （選用） 您為了提升 Security Hub 整合而進行其他行銷活動。請參閱 Go-to-market活動。

    Security Hub 建議您至少提供下列資產。
    - 工作整合的示範影片 （最多 3 分鐘）。影片會用於行銷目的，並張貼到 AWS YouTube 頻道。
    - 要新增至 Security Hub 初次呼叫投影片平台的單軸架構圖表。

Go-to-market活動

合作夥伴也可以參與選用的行銷活動，以協助解釋和提升其 AWS Security Hub 整合。

如果您想要建立與 Security Hub 相關的行銷內容，請在發佈內容之前，將草稿傳送給 APN 合作夥伴經理進行審核和核准。這可確保每個人都在傳訊上保持一致。

AWS 合作夥伴網路 (APN) 合作夥伴可以使用 APN 合作夥伴行銷中心和市場開發資金 (MDF) 計畫來建立行銷活動並取得資金支援。如需這些計劃的詳細資訊，請聯絡您的合作夥伴經理。

Security Hub 合作夥伴頁面上的項目

核准成為 Security Hub 合作夥伴之後，您的解決方案就會顯示在AWS Security Hub 合作夥伴頁面上。

若要列在此頁面上，請將下列詳細資訊提供給 APN 合作夥伴聯絡人。這可能是您的合作夥伴開發經理 (PDM)、合作夥伴解決方案架構師 (PSA) 或傳送電子郵件至 <securityhub-pms@amazon.com>。

- 解決方案的簡短描述、其與 Security Hub 的整合，以及與 Security Hub 的整合為客戶提供的值。此描述限制為 700 個字元，包括空格。
- 描述您解決方案的頁面 URL。該網站應專屬於您的 AWS 整合，更具體地是您的 Security Hub 整合。它應該專注於客戶體驗和客戶使用整合時收到的價值。
- 標誌的高解析度副本，600 x 300 像素。如需此標誌需求的詳細資訊，請參閱 the section called “合作夥伴標誌頁面”。

新聞稿

身為核准的合作夥伴，您可以選擇性地在您的網站和公共關係管道上發佈新聞發佈。新聞稿必須由 核准 AWS。

發佈 新聞稿之前，您必須將其提交至 AWS ，以供 APN 合作夥伴行銷、Security Hub 領導階層和 AWS 外部安全服務 (ESS) 檢閱。新聞稿可以包含 ESS VP 的建議引號。

若要啟動此程序，請使用您的 PDM。我們有 10 個工作天的服務層級協議 (SLA) 可供檢閱 新聞稿。

AWS 合作夥伴網路 (APN) 部落格

我們也可以協助您將撰寫的部落格項目發佈到 APN 部落格。部落格項目必須著重於客戶案例和使用案例。它不能僅以整合啟動合作夥伴為中心。

如果您有興趣，請聯絡您的 PDM 或 PSA 以開始程序。APN 部落格可能需要 8 週或更長的時間才能進行最終核准和發佈。

APN 部落格的重要須知

當您建立部落格文章時，請記住下列項目。

部落格文章的內容是什麼？

合作夥伴文章應具備教育性，並提供有關 AWS 與客戶相關的主題的深入專業知識。

理想長度不超過 1，500 個字。讀者重視深度的教育內容，以教導他們可能遇到的情況 AWS。

內容應該是 APN 部落格的原始內容。請勿重新利用現有部落格文章或白皮書等來源的內容。

發佈至 APN 部落格的其他限制為何？

只有進階或卓越理財方案合作夥伴可以張貼到 APN 部落格。具有 APN 計劃指定之 Select 合作夥伴有例外狀況，例如 Service Delivery。

每個合作夥伴每年僅限張貼三篇文章。擁有數萬個 APN 合作夥伴，其涵蓋範圍 AWS 必須公平。

每個文章都必須有技術發起人，他們可以驗證解決方案或使用案例。

編輯部落格文章發佈前需要多長時間？

在您提交部落格文章的第一個完整長度草稿之後，編輯需要四到六週的時間。

為什麼要寫入 APN 部落格？

APN 部落格文章可提供下列優點。

- 可信度 – 對於 APN 合作夥伴而言，擁有 發佈的故事 AWS 會影響全球客戶。
- 可見性 – APN 部落格是 中最熱門的部落格之一，2019 年 AWS 有 179 萬個頁面檢視，包括受影響的流量。
- 業務 – APN 合作夥伴貼文具有連線按鈕，可透過 APN Customer Engagements (ACE) 計畫產生潛在客戶。

哪種類型的內容最適合？

下列類型的內容最適合 APN 部落格文章。

- 技術內容是最受歡迎的案例類型。這包括解決方案焦點和操作方式資訊。超過 75% 的讀者會查看此技術內容。
- 客戶重視 200 級或更高層級的故事，這些案例示範了某些項目的運作方式 AWS ，或 APN 合作夥伴如何為客戶解決業務問題。
- 由技術專家或主題專家撰寫的文章到目前為止表現最佳。

配量表或行銷表

滑桿工作表是一頁文件，概述您的產品、其整合架構和聯合客戶使用案例。

如果您為整合建立剪貼表，請將副本傳送給 Security Hub 團隊。他們會將其新增至合作夥伴頁面。

白皮書或電子書

如果您建立概述產品、其整合架構和聯合客戶使用案例的白皮書或電子書，請將副本傳送給 Security Hub 團隊。他們會將其新增至 Security Hub 合作夥伴頁面。

網路研討會

如果您確實執行有關整合的網路研討會，請將網路研討會的記錄傳送給 Security Hub 團隊。團隊將從合作夥伴頁面連結至它。

團隊也可以提供 Security Hub 主題專家來參加您的網路研討會。

示範影片

為了行銷目的，您可以製作工作整合的示範影片。在您的影片平台帳戶中張貼此類影片，Security Hub 團隊將從合作夥伴頁面連結至該影片。

產品整合資訊清單

每個 AWS Security Hub 整合合作夥伴都必須完成產品整合資訊清單，以提供提議整合所需的詳細資訊。

Security Hub 團隊會以多種方式使用此資訊：

- 建立您的網站清單
- 建立 Security Hub 主控台的產品卡
- 通知產品團隊您的使用案例。

為了評估提議整合的品質和提供的資訊，Security Hub 團隊會使用 the section called “產品準備檢查清單”。此檢查清單會判斷您的整合是否已準備好啟動。

您提供的所有技術資訊也必須反映在您的文件中。

您可以從 AWS Security Hub 合作夥伴頁面的資源區段下載 PDF 版本的產品整合資訊清單。請注意，合作夥伴頁面不適用於中國（北京）和中國（寧夏）區域。

目錄

- 心跳問題清單
- AWS Security Hub 主控台資訊
  - 公司資訊
  - 產品資訊

使用案例和行銷資訊

下列使用案例可協助您 AWS Security Hub 針對不同用途進行設定。

尋找提供者和消費者使用案例

獨立軟體廠商 (ISV) 的必要項目。

若要描述與 整合相關的使用案例 AWS Security Hub，請回答下列問題。如果您不打算傳送或接收問題清單，請注意本節中的 ，然後完成下一節。

下列資訊必須反映在您的文件中。

- 您會傳送問題清單、接收問題清單或兩者？
- 如果您打算傳送問題清單，您會傳送哪些類型的問題清單？ 您會傳送所有問題清單或特定問題清單子集嗎？
- 如果您計劃接收調查結果，您會如何處理這些調查結果？ 您會收到哪些類型的調查結果？ 例如，您是否會收到客戶選擇的所有問題清單、特定類型的問題清單，或僅收到特定問題清單？
- 您是否打算更新問題清單？ 如果是，您會更新哪些欄位？ Security Hub 建議您更新問題清單，而不是一律建立新的問題清單。更新現有的問題清單有助於降低客戶的問題清單噪音。

  若要更新問題清單，您可以傳送問題清單，其中具有指派給您已傳送問題清單的問題清單 ID。

若要取得有關使用案例和資料集的早期意見回饋，請聯絡 APN 合作夥伴或 Security Hub 團隊。

諮詢合作夥伴 (CP) 使用案例

如果您是 Security Hub 諮詢合作夥伴，則為必要。

為您的 Security Hub 工作提供兩個客戶使用案例。這些可以是私有使用案例。Security Hub 團隊不會在任何位置公告這些內容。他們應該描述下列其中一個或兩個動作。

- 如何協助客戶啟動 Security Hub？ 例如，您是否協助客戶使用專業服務、Terraform 模組或 AWS CloudFormation 範本？
- 您如何協助客戶操作和擴展 Security Hub？ 例如，您是否提供回應或修復範本、建置自訂整合，或使用商業智慧工具來設定執行儀表板？

資料集

如果您將問題清單傳送到 Security Hub，則為必要。

針對您要傳送至 Security Hub 的調查結果，請提供下列資訊。

- 以原生格式呈現的調查結果，例如 JSON 或 XML
- 如何將調查結果轉換為 AWS 安全調查結果格式 (ASFF) 的範例

如果您需要 ASFF 的任何更新以支援整合，請告知 Security Hub 團隊。

架構

如果您將問題清單傳送至 Security Hub 或從 Security Hub 接收問題清單，則為必要。

描述您將如何與 Security Hub 整合。此資訊也必須反映在您的文件中。

您必須提供架構圖表。準備架構圖表時，請考慮下列事項：

- 您將使用哪些 AWS 服務、作業系統代理程式等？
- 如果您要將問題清單傳送至 Security Hub，您會從客戶 AWS 帳戶或自己的 AWS 帳戶傳送問題清單嗎？
- 如果您將收到問題清單，您將如何使用 CloudWatch Events 整合？
- 您將如何將調查結果轉換為 ASFF？
- 您將如何批次處理問題清單、追蹤問題清單狀態，以及避免限流限制？

組態

如果您將問題清單傳送至 Security Hub 或從 Security Hub 接收問題清單，則為必要。

描述客戶如何設定您與 Security Hub 的整合。

您至少必須使用 AWS CloudFormation 範本或類似的基礎設施，例如程式碼範本。有些合作夥伴提供使用者介面以支援一鍵式整合。

組態應該不會超過 15 分鐘。您的產品文件也必須提供整合的組態指引。

每位客戶每天的平均調查結果

如果您將問題清單傳送到 Security Hub，則為必要。

您預期每個月會向 Security Hub 傳送多少個問題清單更新（平均和最大）？ 可接受大小估算的順序。

Latency (延遲)

如果您將問題清單傳送到 Security Hub，則為必要。

您將多快批次處理問題清單並將其傳送至 Security Hub？ 換言之，從在產品中建立問題清單到將問題清單傳送到 Security Hub 的延遲為何？

此資訊必須反映在您的整合產品文件中。這是客戶的常見問題。

公司和產品描述

所有與 Security Hub 的整合都需要。

簡要描述您的公司和產品，並特別強調 Security Hub 整合的性質。我們在 Security Hub 合作夥伴頁面上使用此項目。

如果您要將多個產品與 Security Hub 整合，您可以為每個產品提供單獨的描述，但我們會將它們合併為合作夥伴頁面上的單一項目。

每個描述不能超過 700 個字元，且只能包含空格。

合作夥伴網站資產

所有與 Security Hub 的整合都需要。

您至少必須提供 URL 供 Security Hub 合作夥伴頁面上的進一步了解超連結使用。它應該是行銷登陸頁面，說明您的產品和 Security Hub 之間的整合。

如果您將多個產品與 Security Hub 整合，您可以為它們擁有單一登陸頁面。Security Hub 建議此登陸頁面包含組態指示的連結。

您也可以提供其他資源的連結，例如部落格、網路研討會、示範影片或白皮書。Security Hub 也會從其合作夥伴頁面連結至這些項目。

合作夥伴標誌頁面

所有 Security Hub 整合都需要。

提供標誌的 URL 以顯示在 Security Hub 合作夥伴頁面上。標誌必須符合下列條件：

- 大小：600 x 300 像素
- 裁剪：無填充的緊密
- 背景：透明
- 格式：PNG

Security Hub 主控台的標誌

所有整合都需要。

提供淺色模式和深色模式標誌的 URLs，以顯示在 Security Hub 主控台上。

標誌必須符合下列條件：

- 格式：SVG
- 大小：175 x 40 像素。如果較大，映像應該使用該比率。
- 裁切：無填充緊密
- 背景：透明

如需小型標誌的詳細指導方針，請參閱 the section called “主控台標誌的指導方針”。

調查結果類型

如果您將問題清單傳送到 Security Hub，則為必要。

提供記錄您使用的 ASFF 格式問題清單類型的資料表，以及它們如何與您的原生問題清單類型保持一致。如需 ASFF 中調查結果類型的詳細資訊，請參閱AWS Security Hub 《使用者指南》中的 ASFF 類型分類。

我們建議您也在產品文件中包含此資訊。

熱線

所有與 Security Hub 的整合都需要。

提供技術聯絡窗口的電子郵件地址和電話號碼或呼叫器號碼。Security Hub 將與此聯絡人溝通任何技術問題，例如整合不再運作時。

同時提供全年無休的聯絡窗口，解決高嚴重性的技術問題。

心跳問題清單

如果您將問題清單傳送到 Security Hub，建議使用。

您可以每五分鐘傳送一次「heartbeat」調查結果給 Security Hub，指出您和 Security Hub 的整合功能正常運作嗎？

如果可以，請使用問題清單類型 執行此操作`Heartbeat`。

AWS Security Hub 主控台資訊

將 JSON 文字提供給包含下列資訊的 AWS Security Hub 團隊。Security Hub 使用此資訊來建立您的產品 ARN、在主控台中顯示供應商清單，並在 Security Hub 洞見程式庫中包含您提議的受管洞見。

公司資訊

公司資訊提供有關貴公司的資訊。範例如下：

```
{
    "id": "example",
    "name": "Example Corp",
    "description": "Example Corp is a network security company that monitors your
 network for vulnerabilities.",
}
```

公司資訊包含下列欄位：

欄位	必要	描述
`id`	是	公司的唯一識別符。公司識別符在各公司之間必須是唯一的。

欄位	必要	描述
		這可能會與 相同或相似name。 類型：字串 長度下限：5 個字元 長度上限：24 個字元 允許的字元：小寫字母、數字和連字號 必須以小寫字母開頭。必須以小寫字母或數字結尾。
name	是	要在 Security Hub 主控台上顯示的提供者公司名稱。 類型：字串 長度上限：16 個字元
description	是	要在 Security Hub 主控台上顯示的提供者公司描述。 類型：字串 長度上限：200 個字元

產品資訊

本節提供產品的相關資訊。範例如下：

```
{
    "IntegrationTypes": ["SEND_FINDINGS_TO_SECURITY_HUB"],
    "id": "example-corp-network-defender",
    "regionsNotSupported": "us-west-1",
    "commercialAccountNumber": "111122223333",
    "govcloudAccountNumber": "444455556666",
    "chinaAccountNumber": "777788889999",
    "name": "Example Corp Product",
```

```
    "description": "Example Corp Product is a managed threat detection service.",
    "importType": "BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT",
    "category": "Intrusion Detection Systems (IDS)",
    "marketplaceUrl": "marketplace_url",
    "configurationUrl": "configuration_url"
}
```

產品資訊包含下列欄位。

欄位	必要	描述
IntegrationType	是	指出您的產品是否將問題清單傳送至 Security Hub、從 Security Hub 接收問題清單，還是同時傳送和接收問題清單。 如果您是諮詢合作夥伴，請將此欄位保留空白。 類型：字串陣列 有效值：SEND_FINDINGS_TO_SECURITY_HUB | RECEIVE_FINDINGS_FROM_SECURITY_HUB
id	是	產品的唯一識別符。這些必須在公司內是唯一的。它們在各公司之間不需要是唯一的。這可能會與 相同或相似name。 類型：字串 長度下限：5 個字元 長度上限：24 個字元 允許的字元：小寫字母、數字和連字號 必須以小寫字母開頭。必須以小寫字母或數字結尾。
regionsNotSupported	是	您不支援下列哪些 AWS 區域？ 換句話說，在 Security Hub 主控台的合作夥伴頁面中，哪些區域不應該顯示您為選項？

欄位	必要	描述
		類型：字串 僅提供區域碼。例如：`us-west-1` 。 如需區域清單，請參閱 中的區域端點AWS 一般參考。 的區域代碼 AWS GovCloud (US) 為 `us-gov-west-1` （適用於 AWS GovCloud （美國西部））和 `us-gov-east-1` (for AWS GovCloud （美國東部））。 中國區域的區域代碼為 `cn-north-1` （適用於中國 （北京））和 `cn-northwest-1` （適用於中國 （寧夏））。
`commercialAccountNumber`	是	AWS 區域產品的主要 AWS 帳戶號碼。 如果您將問題清單傳送至 Security Hub，則您提供的帳戶會根據您傳送問題清單的來源而定。 • 從您的 AWS 帳戶。在此情況下，請提供您用來提交調查結果的帳號。 • 從客戶的 AWS 帳戶。在此情況下，Security Hub 建議您提供用於測試整合的主要帳戶號碼。 理想情況下，您會在所有區域的所有產品使用相同的帳戶。如果無法這麼做，請聯絡 Security Hub 團隊。 如果您只從 Security Hub 收到調查結果，則不需要此帳戶號碼。 類型：字串

欄位	必要	描述
`govcloudAccountNumber`	否	AWS GovCloud (US) 區域產品的主要 AWS 帳戶號碼 （ 如果您的產品可在 中使用 AWS GovCloud (US))。 如果您將問題清單傳送至 Security Hub，則您提供的帳戶會根據您傳送問題清單的來源而定。 • 從您的 AWS 帳戶。在此情況下，請提供您用來提交調查結果的帳號。 • 從客戶的 AWS 帳戶。在此情況下，Security Hub 建議您提供用於測試整合的主要帳戶號碼。 理想情況下，您在所有區域的所有 AWS GovCloud (US) 產品都使用相同的帳戶。如果無法這麼做，請聯絡 Security Hub 團隊。 如果您只從 Security Hub 收到調查結果，則不需要此帳戶號碼。 類型：字串

欄位	必要	描述
chinaAccountNumber	否	中國區域產品的主要 AWS 帳戶號碼（如果您的產品在中國區域提供）。 如果您將問題清單傳送至 Security Hub，則您提供的帳戶會根據您傳送問題清單的來源而定。 • 從您的 AWS 帳戶。在此情況下，請提供您用來提交調查結果的帳號。 • 從客戶的 AWS 帳戶。在此情況下，Security Hub 建議您提供用於測試產品整合的主要帳戶號碼。 理想情況下，您在所有中國區域的所有產品都使用相同的帳戶。如果無法這麼做，請聯絡 Security Hub 團隊。 如果您只從 Security Hub 收到調查結果，這可以是您在中國區域擁有的任何帳戶。 類型：字串
name	是	要在 Security Hub 主控台上顯示的提供者產品名稱。 類型：字串 長度上限：24 個字元
description	是	要在 Security Hub 主控台上顯示的提供者產品描述。 類型：字串 長度上限：200 個字元

欄位	必要	描述
importType	是	合作夥伴的資源政策類型。 在合作夥伴加入程序中，您可以指定下列其中一個資源政策，也可以指定 NEITHER。 • 使用 BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT ，您只能從產品 ARN 中列出的帳戶將問題清單傳送至 Security Hub。 • 使用 時BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT ，您只能從訂閱您的客戶帳戶傳送問題清單。 類型：字串 有效值： BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT | BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT | NEITHER

欄位	必要	描述
category	是	定義您產品的類別。您的選擇會顯示在 Security Hub 主控台上。 選擇最多三個類別。 不允許自訂選擇。如果您認為您的類別遺失，請聯絡 Security Hub 團隊。 類型：陣列 可用的類別： • API Firewall • Asset Management • AV Scanning and Sandboxing • Backup and Disaster Recovery • Breach and Attack Simulation • Bug Bounty Platform • Certificate Management • Cloud Access Security Broker • Cloud Security Posture Management • Configuration and Patch Management • Configuration Management Database (CMDB) • Consulting Partner • Container Security • Cyber Range • Data Access Management • Data Classification • Data Loss Prevention • Data Masking and Tokenization

欄位	必要	描述
		• Database Activity Monitoring • DDoS Protection • Deception • Device Control • Dynamic Application Security Testing • Data Encryption • Email Gateway • Encrypted Search • Endpoint Detection and Response (EDR) • Endpoint Forensics • Forensics Toolkit • Fraud Detection • Governance, Risk, and Compliance (GRC) • Host-based Intrusion Detection (HIDs) • Human Resources Information System • Interactive Application Security Testing (IAST) • Instant Messaging • IoT Security • IT Security Training • IT Ticketing and Incident Management • Managed Security Service Provider (MSSP) • Micro-Segmentation

欄位	必要	描述
		• Multi-Cloud Management • Multi-Factor Authentication • Network Access Control (NAC) • Network Firewall • Network Forensics • Network Intrusion Detection Systems (IDS) • Network Intrusion Prevention Systems (IPS) • Phishing Simulation and Training • Privacy Operations • Privileged Access Management • Rogue Device Detection • Runtime Application Self-Protection (RASP) • Secure Web Gateway
marketplaceUrl	否	產品 AWS Marketplace 目的地的 URL。URL 會顯示在 Security Hub 主控台中。 類型：字串 這必須是 AWS Marketplace URL。 如果您沒有 AWS Marketplace 清單，請將此欄位保留空白。

欄位	必要	描述
`configurationUrl`	是	與 Security Hub 整合之產品文件的 URL。此內容託管在您的網站或您管理的網頁上，例如 GitHub 頁面。 類型：字串 您的文件應包含下列資訊。 • 組態指示 • 範本的連結 AWS CloudFormation （如有必要） • 整合使用案例的相關資訊 • Latency (延遲) • ASFF 映射 • 包含的問題清單類型 • 架構

準則和檢查清單

當您準備 AWS Security Hub 整合所需的資料時，請使用這些準則。

準備檢查清單用於在 Security Hub 提供給 Security Hub 客戶之前對整合進行最終審核。

主題

要在主控台上 AWS Security Hub 顯示的標誌指導方針

若要在 AWS Security Hub 主控台上顯示標誌，請遵循這些準則。

淺色和深色模式

您必須同時提供淺色模式和深色模式版本的標誌。

格式

SVG 檔案格式

背景顏色

Transparent

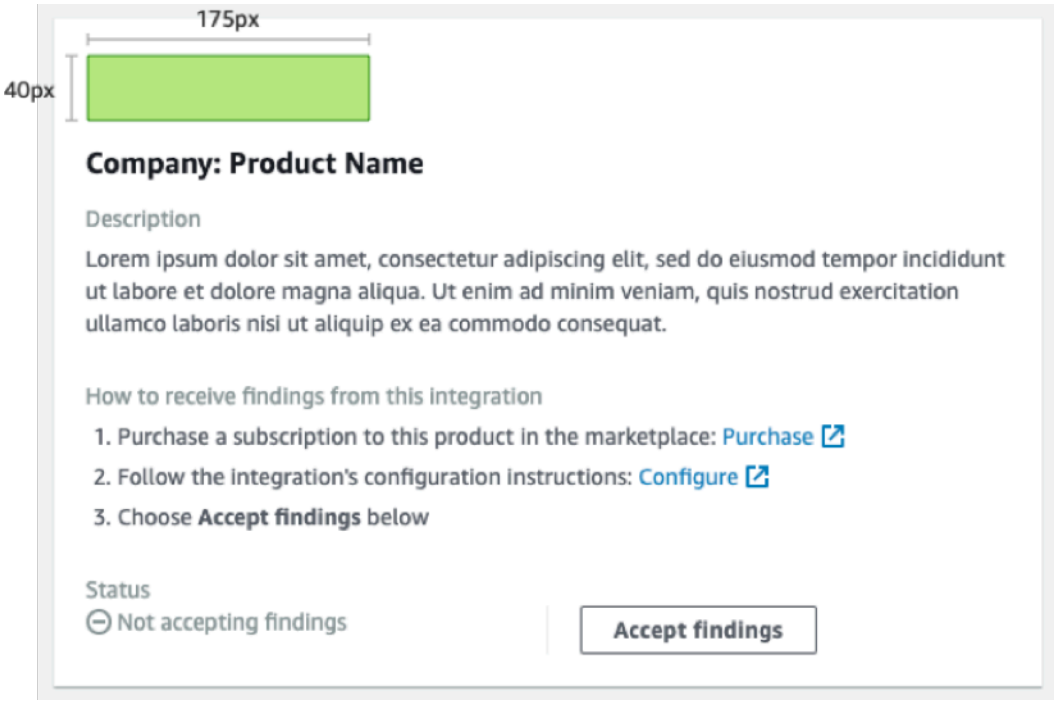
大小

理想比率為寬 175 像素 x 高 40 像素。

最小高度為 40 px。

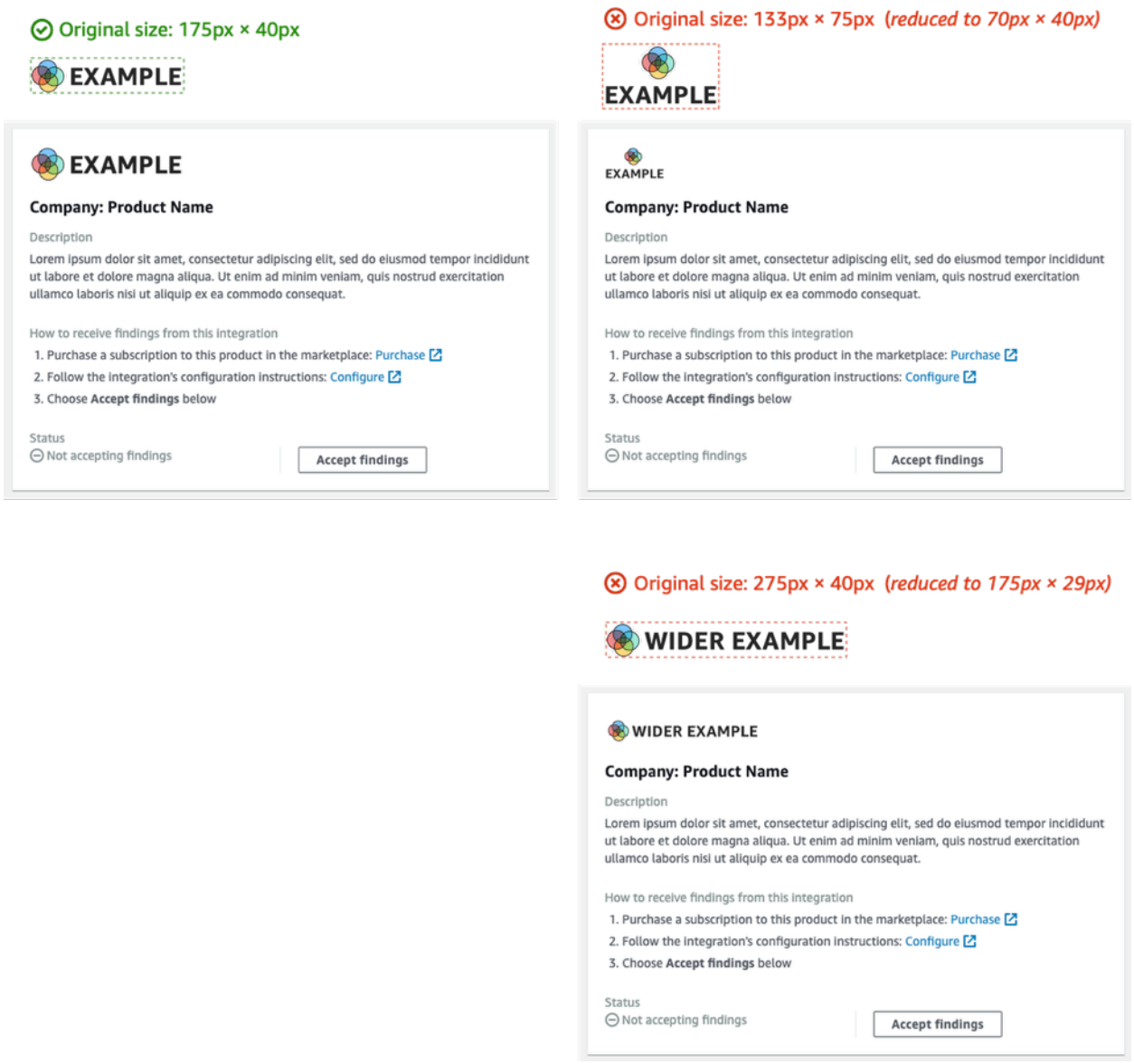
矩形標誌效果最佳。

下圖顯示 Security Hub 主控台上顯示的理想標誌。



如果您的標誌不符合這些維度，Security Hub 會將大小縮減為最大高度 40 px，最大寬度 175 px。這會影響標誌在 Security Hub 主控台上的顯示方式。

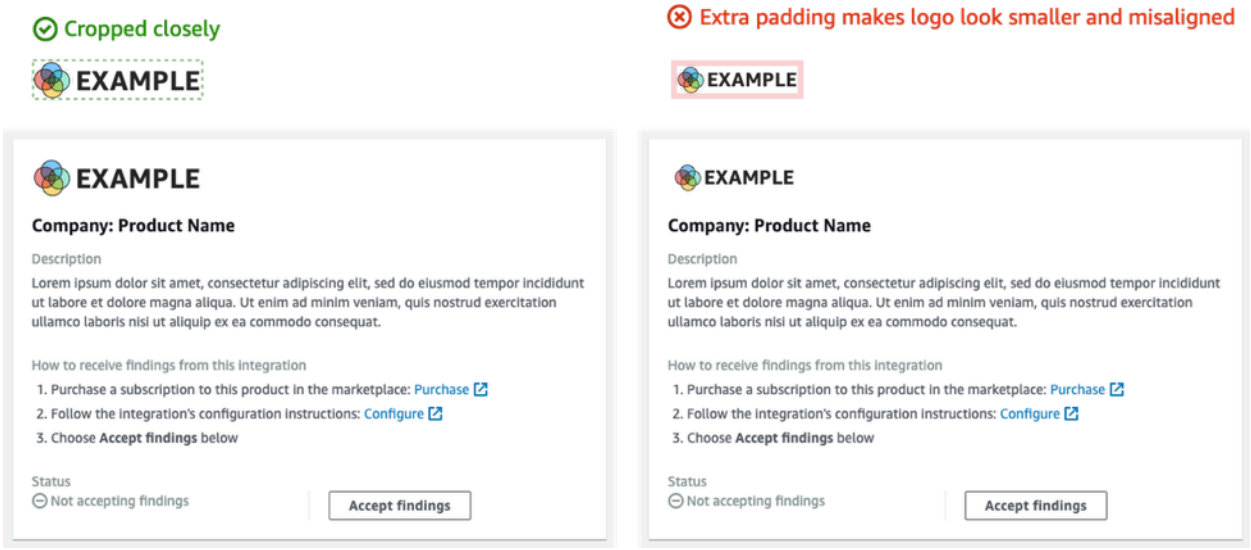
下圖比較使用理想大小的標誌與更寬或更高的標誌的顯示。



裁切

盡可能將標誌影像裁切得接近。請勿提供額外的填補。

下圖顯示緊密裁切的標誌與具有額外填充的標誌之間的差異。



用於建立和更新問題清單的 Tenet

當您規劃如何在 中建立和更新問題清單時 AWS Security Hub，請記住下列原則。

將調查結果具體化，讓客戶可以輕鬆地對其採取行動。

客戶想要自動化回應和修補動作，並將調查結果與其他調查結果建立關聯。為了支援這一點，問題清單應具有下列特性：

- 他們通常應該處理單一或主要資源。
- 它們應該具有單一問題清單類型。
- 他們應該處理單一安全事件。

當問題清單包含多個安全事件的資料時，客戶更難對問題清單採取行動。

將所有問題清單欄位映射至 AWS 安全問題清單格式 (ASFF)。允許客戶依賴 Security Hub 作為事實來源。

客戶預期您原生調查結果格式的每個欄位也會在 Security Hub ASFF 中顯示。

客戶希望所有資料都出現在調查結果的 Security Hub 版本中。遺失資料會導致他們失去對 Security Hub 的信任，做為安全資訊的中央來源。

將問題清單的備援降到最低。請勿讓問題清單磁碟區的客戶不堪負荷。

Security Hub 不是一般日誌管理工具。您應該將高度可行的調查結果傳送到 Security Hub，客戶可以直接回應、修復或與其他調查結果建立關聯。

當問題清單只有次要變更時，請更新問題清單，而不是建立新的問題清單。

當問題清單發生重大變更時，例如嚴重性分數或資源識別符，請建立新的問題清單。

例如，即時為個別連接埠掃描建立問題清單並非高度可行。由於連接埠掃描會持續發生，因此會產生大量調查結果。更吸引人且更精確的是，只需更新上次掃描時間，並從 TOR 節點掃描 MongoDB 連接埠上的單一調查結果。

允許客戶自訂其調查結果，讓他們更有意義。

客戶希望能夠調整特定問題清單欄位，使其更符合其環境或需求。

例如，客戶希望能夠根據帳戶類型或調查結果相關聯的資源類型，新增備註、標籤和調整嚴重性分數。

將問題清單映射到 AWS 安全問題清單格式 (ASFF) 的指導方針

使用下列準則將您的問題清單映射至 ASFF。如需每個 ASFF 欄位和物件的詳細說明，請參閱AWS Security Hub 《 使用者指南》中的AWS 安全調查結果格式 (ASFF)。

識別資訊

`SchemaVersion` 始終是 `2018-10-08`。

`ProductArn` 是 AWS Security Hub 指派給您的 ARN。

`Id` 是 Security Hub 用來為問題清單編製索引的值。問題清單識別符必須是唯一的，以確保不會覆寫其他問題清單。若要更新問題清單，請使用相同的識別符重新提交問題清單。

`GeneratorId` 可以與 相同`Id`，也可以參考離散的邏輯單位，例如 Amazon GuardDuty 偵測器 ID、AWS Config 記錄器 ID 或 IAM Access Analyzer ID。

Title 和 Description

`Title` 應該包含有關受影響資源的一些資訊。 限制`Title`為 256 個字元，包括空格。

將較長的詳細資訊新增至 `Description`。 限制`Description`為 1024 個字元，包括空格。您可以考慮將截斷新增至描述。範例如下：

```
"Title": "Instance i-12345678901 is vulnerable to CVE-2019-1234",
```

```
"Description": "Instance i-12345678901 is vulnerable to CVE-2019-1234. This
 vulnerability affects version 1.0.1 of widget-1 and earlier, and can lead to buffer
 overflow when someone sends a ping.",
```

調查結果類型

您可以在 中提供問題清單類型資訊FindingProviderFields.Types。

Types 應符合 ASFF 的分類類型。

如有需要，您可以指定自訂分類器（第三個命名空間）。

時間戳記

ASFF 格式包含幾個不同的時間戳記。

CreatedAt 和 UpdatedAt

您必須UpdatedAt在每次BatchImportFindings呼叫每個問題清單時提交 CreatedAt和 。

這些值必須符合 Python 3.8 中的 ISO8601 格式。

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

FirstObservedAt 和 LastObservedAt

FirstObservedAt 當您的系統觀察到問題清單時， 和 LastObservedAt 必須相符。如果您不記錄此資訊，則不需要提交這些時間戳記。

這些值符合 Python 3.8 中的 ISO8601 格式。

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

Severity

您可以在 FindingProviderFields.Severity 物件中提供嚴重性資訊，其中包含下列欄位。

Original

您系統的嚴重性值。 Original 可以是任何字串，以容納您使用的系統。

`Label`

問題清單嚴重性的必要 Security Hub 指標。允許的值如下所示。

- `INFORMATIONAL` – 找不到問題。
- `LOW` – 問題不需要自行執行動作。
- `MEDIUM` – 必須解決問題，但不能緊急解決。
- `HIGH` – 問題必須以優先順序處理。
- `CRITICAL` – 問題必須立即修復，以避免進一步傷害。

合規的調查結果應一律`Label`設定為 `INFORMATIONAL`。`INFORMATIONAL` 問題清單範例是通過安全檢查的調查結果，以及已修復的問題 AWS Firewall Manager 清單。

客戶通常會依嚴重性排序問題清單，為其安全營運團隊提供待辦事項清單。將問題清單嚴重性設定為 `HIGH`或 時，請保守。 `CRITICAL`

您的整合文件必須包含您的映射原理。

Remediation

`Remediation` 有兩個元素。這些元素在 Security Hub 主控台上合併。

`Remediation.Recommendation.Text` 會出現在調查結果詳細資訊的修復區段中。其超連結為 的值`Remediation.Recommendation.Url`。

目前，只有來自 Security Hub 標準、IAM Access Analyzer 和 Firewall Manager 的調查結果會顯示有關如何修復調查結果的文件超連結。

SourceUrl

只有在您可以為主控台提供特定調查結果的深層連結 URL `SourceUrl`時，才能使用 。否則，請將其從映射中省略。

Security Hub 不支援此欄位的超連結，但會在 Security Hub 主控台上公開。

Malware, Network, Process, ThreatIntelIndicators

如適用，請使用 `Malware`、`Process`、 `Network`或 `ThreatIntelIndicators`。每個物件都會在 Security Hub 主控台中公開。在您傳送的調查結果內容中使用這些物件。

例如，如果您偵測到對已知命令和控制節點進行傳出連線的惡意軟體，請在 中提供 EC2 執行個體的詳細資訊Resource.Details.AwsEc2Instance。提供該 EC2 執行個體的相關 Network、Malware和 ThreatIntelIndicator 物件。

Malware

Malware 是一個清單，最多可接受五個陣列的惡意軟體資訊。讓惡意軟體項目與資源和調查結果相關。

每個項目都有下列欄位。

Name

惡意軟體的名稱。值是最多 64 個字元的字串。

Name 應該來自經過審核的威脅情報或研究員來源。

Path

惡意軟體的路徑。此值最多為 512 個字元的字串。 Path 應為 Linux 或 Windows 系統檔案路徑，但下列情況除外。

- 如果您根據 YARA 規則掃描 S3 儲存貯體或 EFS 共用中的物件，則 Path是 S3：// 或 HTTPS 物件路徑。
- 如果您掃描 Git 儲存庫中的檔案，則 Path是 Git URL 或複製路徑。

State

惡意軟體的狀態。允許的值為 OBSERVED | REMOVAL_FAILED | REMOVED。

在問題清單標題和描述中，請確定您提供惡意軟體所發生情況的內容。

例如，如果 Malware.State是 REMOVED，則調查結果標題和描述應該反映您的產品已移除路徑上的惡意軟體。

如果 Malware.State是 OBSERVED，則調查結果標題和描述應反映您的產品遇到路徑上的此惡意軟體。

Type

指出惡意軟體的類型。允許的值為 ADWARE | BLENDED_THREAT | BOTNET_AGENT | COIN_MINER | EXPLOIT_KIT KEYLOGGER | | MACRO | POTENTIALLY_UNWANTED | SPYWARE | RANSOMWARE REMOTE_ACCESS | ROOTKIT | TROJAN | | | VIRUS | | WORM。

如果您需要 的額外值Type，請聯絡 Security Hub 團隊。

Network

Network 是單一物件。您無法新增多個網路相關詳細資訊。映射欄位時，請使用下列準則。

目的地和來源資訊

目的地和來源可輕鬆對應 TCP 或 VPC 流程日誌或 WAF 日誌。當您描述有關攻擊問題清單的網路資訊時，它們更難使用。

一般而言，來源是攻擊來源，但可能有其他來源，如下所示。您應該在文件中說明來源，並在問題清單標題和描述中加以描述。

- 對於 EC2 執行個體的 DDoS 攻擊，來源是攻擊者，但真正的 DDoS 攻擊可能會使用數百萬個主機。目的地是 EC2 執行個體的公有 IPv4 地址。 Direction是 IN。
- 對於觀察到從 EC2 執行個體與已知命令和控制節點通訊的惡意軟體，來源是 EC2 執行個體的 IPV4 地址。目的地是 命令和控制節點。 Direction是 0UT。您也可以提供 Malware和 ThreatIntelIndicators。

Protocol

Protocol 一律對應至網際網路指派號碼授權機構 (IANA) 註冊名稱，除非您可以提供特定通訊協定。您應該一律使用此項目並提供連接埠資訊。

Protocol 獨立於來源和目的地資訊。只有在合理時才提供。

Direction

Direction 一律與 AWS 網路邊界相關。

- IN 表示它正在進入 AWS (VPC， 服務）。
- 0UT 表示它正在結束 AWS 網路邊界。

Process

Process 是單一物件。您無法新增多個程序相關詳細資訊。映射欄位時，請使用下列準則。

Name

Name 應該符合可執行檔的名稱。它最多接受 64 個字元。

Path

Path 是程序可執行檔的檔案系統路徑。它最多接受 512 個字元。

Pid, **ParentPid**

Pid 和 ParentPid應符合 Linux 程序識別符 (PID) 或 Windows 事件 ID。若要區分，請使用 EC2 Amazon Machine Image (AMI) 提供資訊。客戶可能會區分 Windows 和 Linux。

時間戳記 (**LaunchedAt** 和 **TerminatedAt**)

如果您無法可靠地擷取此資訊，且其對於毫秒並不精確，請勿提供此資訊。

如果客戶倚賴時間戳記進行鑑識調查，則沒有時間戳記會比擁有錯誤的時間戳記更好。

ThreatIntelIndicators

ThreatIntelIndicators 接受最多五個威脅情報物件的陣列。

對於每個項目， Type 位於特定威脅的內容中。允許的值為 DOMAIN | EMAIL_ADDRESS | HASH_MD5 | HASH_SHA1 | HASH_SHA256 | HASH_SHA512 | IPV4_ADDRESS | IPV6_ADDRESS MUTEX | | PROCESS | URL。

以下是如何映射威脅情報指標的一些範例：

- 您找到一個您知道與 Cobalt Strike 相關聯的程序。您從 FireEye 的部落格中了解到這一點。

  將 Type 設定為 PROCESS。也請為 程序建立 Process 物件。
- 您的郵件篩選條件找到某人從已知惡意網域傳送已知雜湊套件。

  建立兩個ThreatIntelIndicator物件。一個物件適用於 DOMAIN。另一個用於 HASH_SHA1。
- 您找到具有 Yara 規則的惡意軟體 (Loki、Fenrir、Awss3VirusScan、BinaryAlert)。

  建立兩個ThreatIntelIndicator物件。其中一個是惡意軟體。另一個用於 HASH_SHA1。

Resources

對於 Resources，請盡可能使用我們提供的資源類型和詳細資訊欄位。Security Hub 會持續將新資源新增至 ASFF。若要接收 ASFF 變更的每月日誌，請聯絡 <securityhub-partners@amazon.com>。

如果您無法將資訊符合模型化資源類型的詳細資訊欄位中的資訊，請將其餘的詳細資訊對應至 Details.Other。

對於未在 ASFF 中建模的資源，請將 Type設定為 Other。如需詳細資訊，請使用 Details.Other。

您也可以使用Other資源類型進行非AWS 調查結果。

ProductFields

只有在您無法為 使用另一個策劃欄位Resources或描述性物件，例如 ThreatIntelIndicators、或 ProductFields時Network，才能使用 Malware。

如果您確實使用 ProductFields，則必須為此決策提供嚴格的理由。

合規

只有在問題清單與合規相關Compliance時才使用 。

Security Hub Compliance會針對根據控制項產生的問題清單使用 。

Firewall Manager 使用 Compliance 做為其調查結果，因為它們與合規相關。

受限的欄位

這些欄位旨在讓客戶追蹤對調查結果的調查。

請勿映射到這些欄位或物件。

- Note
- UserDefinedFields
- VerificationState
- Workflow

對於這些欄位，映射到FindingProviderFields物件中的欄位。請勿映射至最上層欄位。

- Confidence – 只有在您的服務具有類似的功能，或您的調查結果 100% 站立時，才包含可信度分數 (0-99)。
- Criticality – 關鍵性分數 (0-99) 旨在表達與調查結果相關聯的資源的重要性。
- RelatedFindings – 只有在您可以追蹤與相同資源或問題清單類型相關的問題清單時，才提供相關的問題清單。若要識別相關調查結果，您必須參考已在 Security Hub 中調查結果的調查結果識別符。

使用 BatchImportFindings API 的指導方針

使用 BatchImportFindings API 操作將問題清單傳送到 時 AWS Security Hub，請使用下列準則。

- 您必須BatchImportFindings使用與調查結果相關聯的帳戶來呼叫 。關聯帳戶的識別符是調查結果的AwsAccountId屬性值。
- 傳送您可以傳送的最大批次。Security Hub 每個批次最多接受 100 個調查結果，每個調查結果最多接受 240 KB，每個批次最多接受 6 MB。
- 調節速率限制為每個區域每個帳戶 10 TPS，爆量為 30 TPS。
- 如果存在限流或網路問題，您必須實作機制來保留問題清單的狀態。您也需要調查結果狀態，以便在調查結果移入和移出合規時提交調查結果更新。
- 如需有關字串長度上限和其他限制的資訊，請參閱AWS Security Hub 《 使用者指南》中的AWS 安全調查結果格式 (ASFF)。

產品準備檢查清單

AWS Security Hub 和 APN 合作夥伴團隊使用此檢查清單來驗證整合已準備就緒。

ASFF 映射

這些問題與問題清單映射到 AWS 安全問題清單格式 (ASFF) 有關。

合作夥伴的所有調查結果資料是否都對應到 ASFF？

以某種方式將所有問題清單映射到 ASFF。

使用已整理的欄位，例如模型化資源類型、Malware、 Network或 ThreatIntelIndicators。

ProductFields 視需要將任何其他項目映射至 Resource.Details.Other或 。

合作夥伴是否使用**Resource.Details**欄位，例如 **AwsEc2instance**、 **AwsS3Bucket**和 **Container**？ 合作夥伴是否使用 **Resource.Details.Other** 定義未在 ASFF 中建模的資源詳細資訊？

盡可能使用提供的欄位，來尋找問題清單，例如 EC2 執行個體、S3 儲存貯體和安全群組。

Resource.Details.Other 只有在沒有直接比對時，才將與資源相關的其他資訊映射至 。

合作夥伴是否將值映射至 **UserDefinedFields**？

請勿選擇 UserDefinedFields。

考慮使用另一個策劃的欄位，例如 Resource.Details.Other或 ProductFields。

合作夥伴是否將可映射到其他 ASFF 欄位的資訊映射到 **ProductFields** ？

ProductFields 僅用於產品特定資訊，例如版本控制資訊、產品特定嚴重性問題清單，或無法映射到已整理欄位或 的其他資訊Resources.Details.Other。

合作夥伴是否匯入自己的 時間戳記**FirstObservedAt**？

FirstObservedAt 時間戳記旨在記錄在產品中觀察到問題清單的時間。如果可能，請映射此欄位。

合作夥伴是否為每個問題清單識別符提供產生的唯一值，但他們想要更新的問題清單除外？

Security Hub 中的所有問題清單都會以問題清單識別符 (Id 屬性） 為索引。此值必須一律是唯一的，以確保問題清單不會意外更新。

您也應該維持調查結果識別符狀態，以便更新調查結果。

合作夥伴是否提供將調查結果映射到產生器 ID 的值？

GeneratorID 不應具有與問題清單 ID 相同的值。

GeneratorID 應該能夠透過產生問題清單的方式，以邏輯方式連結問題清單。

這可以是產品 （ 產品 A - 漏洞與產品 A - EDR) 或類似項目中的子元件。

合作夥伴是否以與其產品相關的方式使用必要的問題清單類型命名空間？ 合作夥伴是否在其調查結果類型中使用建議的調查結果類型類別或分類器？

問題清單類型分類應緊密對應至產品產生的問題清單。

AWS 安全調查結果格式中概述的第一層命名空間是必要的。

您可以針對第二層和第三層命名空間 （類別或分類器） 使用自訂值。

如果合作夥伴有網路資料，是否在 **Network** 欄位中擷取網路流程資訊？

如果您的產品擷取 NetFlow 資訊，請將其映射到 Network 欄位。

如果合作夥伴有程序資料，是否會在 **Process** 欄位中擷取程序 (PID) 資訊？

如果您的產品擷取程序資訊，請將其映射到 Process 欄位。

如果合作夥伴有惡意軟體資料，是否會在 **Malware** 欄位中擷取惡意軟體資訊？

如果您的產品擷取惡意軟體資訊，請將其映射到 `Malware` 欄位。

如果合作夥伴有威脅情報資料，是否會在 **ThreatIntelIndicators** 欄位中擷取威脅情報資訊？

如果您的產品擷取威脅情報資訊，請將其映射到 `ThreatIntelIndicators` 欄位。

合作夥伴是否提供調查結果的可信度評分？ 如果這麼做，是否提供理由？

每當您使用此欄位時，請在文件和資訊清單中提供理由。

合作夥伴是否針對問題清單中的資源 ID 使用正式 ID 或 ARN？

識別 AWS 資源時，最佳實務是使用 ARN。如果 ARN 無法使用，請使用正式資源 ID。

整合設定和函數

這些問題與整合的設定和day-to-day函數有關。

合作夥伴是否提供infrastructure-as-code(IaC) 範本，以部署與 Security Hub 的整合，例如 Terraform AWS CloudFormation或 AWS Cloud Development Kit (AWS CDK)？

對於將從客戶帳戶傳送問題清單或使用 CloudWatch Events 取用問題清單的整合，需要某種形式的 IaC 範本。

AWS CloudFormation 為偏好，但也可以使用 AWS CDK 或 Terraform。

合作夥伴產品是否在其主控台上具有一鍵式設定，以便與 Security Hub 整合？

有些合作夥伴產品會在其產品中使用切換或類似機制來啟用整合。這可能需要自動佈建資源和許可。如果您從產品帳戶傳送問題清單，則一鍵式設定是偏好的方法。

合作夥伴是否只傳送有價值的問題清單？

一般而言，您應該只將具有安全價值的問題清單傳送給 Security Hub 客戶。

Security Hub 不是一般日誌管理工具。您不應將所有可能的日誌傳送至 Security Hub。

合作夥伴是否提供估計，估計每位客戶每天要傳送多少問題清單，以及頻率（平均和爆量）？

唯一調查結果的數量會用來計算 Security Hub 的負載。唯一調查結果定義為具有與其他調查結果不同 ASFF 映射的調查結果。

例如，如果一個問題清單僅填入 `ThreatIntelIndicators` ，另一個僅填入 `Resources.Details.AWSEc2Instance`，則這兩個問題清單是兩個唯一的問題清單。

合作夥伴是否具有處理 4xx 和 5xx 錯誤的適當方式，使其不會受到節制，且所有問題清單都可以稍後傳送？

BatchImportFindings API 操作目前有 30–50 TPS 的爆量率。如果傳回 4xx 或 5xx 錯誤，您必須保留這些失敗問題清單的狀態，以便稍後可以重試。您可以透過無效字母佇列或其他 AWS 傳訊服務，例如 Amazon SNS 或 Amazon SQS 來執行此操作。

合作夥伴是否維護其調查結果的狀態，以便他們知道封存不再存在的調查結果？

如果您計劃透過覆寫原始調查結果 ID 來更新調查結果，則必須有保留狀態的機制，以便為正確的調查結果更新正確的資訊。

如果您提供問題清單，請勿使用 BatchUpdateFindings操作來更新問題清單。此操作只能由客戶使用。只有在調查問題清單並採取行動BatchUpdateFindings時，您才能使用 。

合作夥伴是否以不影響先前傳送成功調查結果的方式處理重試？

您應該有一個機制，以便在發生錯誤時保留原始調查結果 IDs，以免錯誤地複製或覆寫成功的調查結果。

合作夥伴是否透過使用現有問題清單的問題清單 ID 呼叫 **BatchImportFindings**操作來更新問題清單？

若要更新問題清單，您必須提交相同的問題清單 ID 來覆寫現有的問題清單。

BatchUpdateFindings 操作只能由客戶使用。

合作夥伴是否使用 **BatchUpdateFindings** API 更新問題清單？

如果您對問題清單採取動作，您可以使用 BatchUpdateFindings操作來更新特定欄位。

合作夥伴是否提供有關問題清單建立與從其產品傳送至 Security Hub 之間的延遲量的資訊？

您應該將延遲降至最低，以確保客戶盡快在 Security Hub 中看到問題清單。

資訊清單中需要此資訊。

如果合作夥伴的架構是從客戶帳戶傳送問題清單到 Security Hub，他們是否成功證明這一點？ 如果合作夥伴的架構是從自己的帳戶傳送問題清單到 Security Hub，他們是否成功證明這一點？

在測試期間，問題清單必須成功從您擁有的帳戶傳送，而該帳戶不同於為產品 ARN 提供的帳戶。

從產品 ARN 擁有者的帳戶傳送問題清單，可以略過 API 操作中的某些錯誤例外狀況。

合作夥伴是否提供活動訊號調查結果給 Security Hub？

若要顯示您的整合正常運作，您應該傳送活動訊號調查結果。活動訊號調查結果每五分鐘傳送一次，並使用調查結果類型 `Heartbeat`。

如果您從產品帳戶傳送問題清單，這很重要。

合作夥伴是否在測試期間與 Security Hub 產品團隊的帳戶整合？

在生產前驗證期間，您應該將問題清單範例傳送至 Security Hub 產品團隊 AWS 的帳戶。這些範例示範問題清單已正確傳送和映射。

文件

這些問題與您提供的整合文件有關。

合作夥伴是否在專用網站上託管其文件？

文件應該以靜態網頁、wiki、Read the Docs 或其他專用格式託管在您的網站上。

在 GitHub 上託管文件不符合專用網站需求。

合作夥伴文件是否提供如何設定 Security Hub 整合的說明？

您可以使用 IaC 範本或主控台型「一鍵式」整合來設定整合。

合作夥伴文件是否提供其使用案例的描述？

您在資訊清單中提供的使用案例也應該在文件中描述

合作夥伴文件是否提供他們所傳送調查結果的理由？

您應該提供所傳送問題清單類型的原理。

例如，您的產品可能會產生漏洞、惡意軟體和防毒的調查結果，但您只會將漏洞和惡意軟體調查結果傳送至 Security Hub。在這種情況下，您必須提供不傳送防毒問題清單的原因。

合作夥伴文件是否提供合作夥伴如何將調查結果映射到 ASFF 的理由？

您應該提供將產品原生調查結果映射至 ASFF 的原理。客戶想要知道在何處尋找特定產品資訊。

合作夥伴文件是否提供有關合作夥伴更新問題清單的方式，以及更新問題清單的指引？

提供客戶如何保留狀態、確保等冪，以及使用up-to-date覆寫問題清單的相關資訊。

合作夥伴文件是否說明問題清單延遲？

將延遲降至最低，以確保客戶盡快在 Security Hub 中看到問題清單。

資訊清單中需要此資訊。

合作夥伴文件是否說明其嚴重性評分如何對應至 ASFF 嚴重性評分？

提供如何映射`Severity.Original`到 的資訊`Severity.Label`。

例如，如果您的嚴重性值是字母等級 (A、B、C)，您應該提供如何將字母等級對應至嚴重性標籤的資訊。

合作夥伴文件是否提供可信度評分的理由？

如果您提供可信度分數，則應對這些分數進行排名。

如果您使用靜態填入的可信度分數或衍生自人工智慧或機器學習的映射，您應該提供額外的內容。

合作夥伴文件是否會記下合作夥伴有和不支援哪些區域？

請注意 支援或不支援的區域，讓客戶知道哪些區域不嘗試整合。

產品卡資訊

這些問題與 Security Hub 主控台整合頁面上顯示的產品卡片有關。

提供的 AWS 帳戶 ID 是否有效且包含 12 位數？

帳戶識別碼長度為 12 位數。如果帳戶 ID 少於 12 位數，則產品 ARN 將無效。

產品描述是否包含 200 個或更少的字元？

資訊清單中 JSON 中提供的產品描述不應超過 200 個字元，包括空格。

組態連結是否會導致整合的文件？

組態連結應會導向您的線上文件。它不應導向您的主要網站或行銷頁面。

購買連結 （如果提供） 是否導致產品 AWS Marketplace 清單？

如果您提供購買連結，則必須用於 AWS Marketplace 項目。Security Hub 不接受非 託管的購買連結 AWS。

產品類別是否正確描述產品？

在資訊清單中，您最多可以提供三個產品類別。這些應該符合 JSON，而且不能是自訂的。您無法提供超過三個產品類別。

公司和產品名稱是否有效且正確？

公司名稱必須為 16 個字元或更少。

產品名稱必須為 24 個字元或更少。

產品卡 JSON 中的產品名稱必須與資訊清單中的名稱相符。

行銷資訊

這些問題與整合的行銷有關。

Security Hub 合作夥伴頁面的產品描述是否在 700 個字元以內，包括空格？

Security Hub 合作夥伴頁面最多只接受 700 個字元，包括空格。

團隊將編輯更長的描述。

Security Hub 合作夥伴頁面標誌是否不大於 600 x 300 px？

以 PNG 或 JPG 提供具有公司標誌且不超過 600 x 300 像素的可公開存取 URL。

進一步了解 Security Hub 合作夥伴頁面上的超連結是否會導致合作夥伴有關整合的專用網頁？

進一步了解連結不應導致合作夥伴的主要網站或文件資訊。

此連結應一律前往專屬網頁，其中包含整合的相關行銷資訊。

合作夥伴是否提供如何使用其整合的示範或教學影片？

示範或整合演練影片是選用的，但建議使用。

AWS 合作夥伴網路部落格文章是否與合作夥伴及其合作夥伴開發經理或合作夥伴開發代表一起發佈？

AWS 合作夥伴網路部落格文章應事先與合作夥伴開發經理或合作夥伴開發代表協調。

這些與您自行建立的任何部落格文章是分開的。

允許 4–6 週的前置時間。使用私有產品 ARN 進行測試後，應該開始這項工作。

是否發行了合作夥伴主導的新聞發佈？

您可以與您的合作夥伴開發經理或合作夥伴開發代表合作，從外部安全服務 VP 取得報價。您可以在您的新聞發佈中使用此引號。

是否發佈了合作夥伴主導的部落格文章？

您可以建立自己的部落格文章，以展示 Partner Network 部落格以外的 AWS 整合。

是否發行了合作夥伴主導的網路研討會？

您可以建立自己的網路研討會來展示整合。

如果您需要 Security Hub 團隊協助，請在使用私有產品 ARN 完成測試後，與產品團隊合作。

合作夥伴是否向 請求社交媒體支援 AWS？

發行後，您可以與 AWS 安全行銷主管合作，使用 AWS 官方社交媒體管道來共用網路研討會的詳細資訊。

AWS Security Hub 合作夥伴常見問答集

以下是有關設定和維護與 整合的常見問題 AWS Security Hub。

1. Security Hub 整合有哪些優點？
   - 客戶滿意度 – 與 Security Hub 整合的首要原因是您有客戶請求這樣做。

     Security Hub 是 AWS 客戶的安全和合規中心。其設計為 AWS 安全與合規專業人員每天了解其安全與合規狀態的第一站。

     聆聽您的客戶。他們將告訴您他們是否想要在 Security Hub 中查看您的問題清單。
   - 探索機會：我們在 Security Hub 主控台中推廣具有已認證的整合的合作夥伴，包括其 AWS Marketplace 清單的連結。這是讓客戶探索新安全產品的好方法。
   - 行銷機會 – 具有核准整合的供應商可以參與網路研討會、發佈新聞發佈、建立配量表，以及 AWS 向客戶示範其整合。
2. 有哪些類型的合作夥伴？
   - 將問題清單傳送到 Security Hub 的合作夥伴
   - 從 Security Hub 接收調查結果的合作夥伴
   - 同時傳送和接收調查結果的合作夥伴
   - 協助客戶在其環境中設定、自訂和使用 Security Hub 的諮詢合作夥伴
3. 與 Security Hub 的合作夥伴整合如何在高階運作？

   您可以從客戶帳戶內或自己的 AWS 帳戶收集調查結果，並將調查結果的格式轉換為 AWS 安全調查結果格式 (ASFF)。然後，將這些調查結果推送到適當的 Security Hub 區域端點。

   您也可以使用 CloudWatch Events 從 Security Hub 接收問題清單。
4. 完成與 Security Hub 整合的基本步驟是什麼？
   a. 提交您的合作夥伴資訊清單資訊。
   b. 如果您要將問題清單傳送至 Security Hub，請接收產品 ARNs 以搭配 Security Hub 使用。
   c. 將您的問題清單映射至 ASFF。請參閱 the section called “ASFF 映射的指導方針”。
   d. 定義您的架構，以將問題清單傳送至 Security Hub 並從中接收問題清單。遵循 中概述的原則the section called “用於建立和更新問題清單的 Tenet”。
   e. 為客戶建立部署架構。例如， AWS CloudFormation 指令碼可以實現此目的。
   f. 記錄您的設定，並為客戶提供組態指示。

g. 定義客戶可與產品搭配使用的任何自訂洞見（關聯規則）。

h. 示範您與 Security Hub 團隊的整合。

i. 提交行銷資訊以供核准（網站語言、新聞發佈、架構投影片、影片、剪貼表）。

5. 提交合作夥伴資訊清單的程序為何？ 而 AWS 服務是否將問題清單傳送到 Security Hub？

   若要提交資訊清單資訊給 Security Hub 團隊，請使用 <securityhub-partners@amazon.com>。

   您會在七天內收到產品 ARNs。

6. 我應該將哪些類型的問題清單傳送至 Security Hub？

   Security Hub 定價部分取決於擷取的調查結果數量。因此，您應該避免傳送未為客戶提供價值的問題清單。

   例如，某些漏洞管理廠商只會在可能的 10 個問題中，傳送常見漏洞評分系統 (CVSS) 分數為 3 或更高的問題清單。

7. 將問題清單傳送到 Security Hub 的方法有哪些？

   以下是主要方法：

   - 您可以使用 BatchImportFindings操作從自己的指定 AWS 帳戶傳送問題清單。
   - 您可以使用 BatchImportFindings操作從客戶帳戶內傳送問題清單。您可以使用擔任角色方法，但不需要這些方法。

   如需使用 的整體指導方針BatchImportFindings，請參閱 the section called “使用 BatchImportFindings API 的指導方針”。

8. 如何收集調查結果並將其推送至 Security Hub 區域端點？

   合作夥伴已對此使用不同的方法，因為它高度依賴解決方案的架構。

   例如，有些合作夥伴會建置 Python 應用程式，以部署為 AWS CloudFormation 指令碼。指令碼會從客戶環境收集合作夥伴的調查結果，將其轉換為 ASFF，並將其傳送至 Security Hub 區域端點。

   其他合作夥伴會建置完整的精靈，為客戶提供一鍵式體驗，將問題清單推送至 Security Hub。

9. 如何知道何時開始將問題清單傳送至 Security Hub？

   Security Hub 支援 BatchImportFindings API 操作的部分批次授權，因此您可以將所有問題清單傳送給 Security Hub 給所有客戶。

如果您的部分客戶尚未訂閱 Security Hub，Security Hub 不會擷取這些調查結果。它只會擷取批次中的授權調查結果。

10.我需要完成哪些步驟，才能將問題清單傳送至客戶的 Security Hub 執行個體？

a. 確保已備妥正確的 IAM 政策。

b. 為帳戶啟用產品訂閱 （資源政策）。使用 EnableImportFindingsForProduct API 操作或整合頁面。客戶可以這樣做，或者您可以使用跨帳戶角色來代表客戶採取行動。

c. 請確定調查結果ProductArn的 是您產品的公有 ARN。

d. 請確定調查結果AwsAccountId的 是客戶的帳戶 ID。

e. 根據 AWS 安全調查結果格式 (ASFF)，確保您的調查結果沒有任何格式不正確的資料。例如，會填入必要欄位，而且沒有無效的值。

f. 將問題清單批次傳送至正確的區域端點。

11.我必須具備哪些 IAM 許可才能傳送問題清單？

必須針對呼叫 或其他 API 呼叫的 IAM 使用者BatchImportFindings或角色設定 IAM 政策。

最簡單的測試是從管理員帳戶執行此操作。您可以將這些限制為 action: 'securityhub:BatchImportFindings'和 resource: *<productArn and/or productSubscriptionArn>*。

相同帳戶中的資源可以使用 IAM 政策設定，而不需要資源政策。

若要排除來自 發起人的 IAM 政策問題BatchImportFindings，請為發起人設定 IAM 政策，如下所示：

```
{
    Action: 'securityhub:*',
    Effect: 'Allow',
    Resource: '*'
}
```

請務必檢查呼叫者沒有Deny政策。取得該政策以使用之後，您可以將政策限制為下列內容：

```
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:<account>:product/mycompany/myproduct'
},
```

```
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:*:product-subscription/mycompany/
myproduct'
}
```

12.什麼是產品訂閱？

若要從特定合作夥伴產品接收問題清單，客戶 （或具有代表客戶的跨帳戶角色的合作夥伴） 必須建立產品訂閱。若要從 主控台執行此操作，他們會使用整合頁面。若要從 API 執行此操作，他們會使用 EnableImportFindingsForProduct API 操作。

產品訂閱會建立資源政策，授權合作夥伴的調查結果由客戶接收或傳送。如需詳細資訊，請參閱 使用案例和許可。

Security Hub 有下列類型的合作夥伴資源政策：

- BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT
- BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT

在合作夥伴加入程序中，您可以請求一種或兩種類型的政策。

使用 BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT時，您只能從產品 ARN 中列出的帳戶將問題清單傳送至 Security Hub。

使用 時BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT，您只能從訂閱您的客戶帳戶傳送問題清單。

13.假設客戶建立了管理員帳戶，並新增了幾個成員帳戶。客戶是否需要訂閱每個成員帳戶？ 或者，客戶是否只訂閱管理員帳戶，然後我可以針對所有成員帳戶中的資源傳送問題清單？

此問題會根據管理員帳戶註冊，詢問是否已為所有成員帳戶建立許可。

客戶必須為每個帳戶設定產品訂閱。他們可以透過 API 以程式設計方式執行此操作。

14.什麼是我的產品 ARN？

您的產品 ARN 是 Security Hub 為您產生的唯一識別符，用於提交問題清單。您會收到與 Security Hub 整合之每個產品的產品 ARN。正確的產品 ARN 必須是您傳送至 Security Hub 的每個調查結果的一部分。沒有產品 ARN 的調查結果會遭到捨棄。產品 ARN 使用以下格式：

`arn:aws:securityhub:[region code]:[account ID]:product/[company name]/[product name]`

請見此處範例：

`arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro`

針對部署 Security Hub 的每個區域，您會收到產品 ARN。帳戶 ID、公司和產品名稱是由您的合作夥伴資訊清單提交所決定。除了區域碼之外，您永遠不會變更任何與您產品 ARN 相關聯的資訊。區域碼必須符合您提交調查結果的區域。

常見的錯誤是變更帳戶 ID，以符合您目前工作的 帳戶。帳戶 ID 不會變更。您提交「主」帳戶 ID 做為資訊清單提交的一部分。此帳戶 ID 會鎖定在您的產品 ARN 中。

當 Security Hub 在新區域中啟動時，會自動使用標準區域代碼來產生這些區域的產品 ARNs。

每個帳戶也會自動使用私有產品 ARN 佈建。您可以在收到官方公有產品 ARN 之前，使用此 ARN 來測試您開發帳戶中的匯入問題清單。

15應使用哪種格式將問題清單傳送至 Security Hub？

問題清單必須以 AWS 安全問題清單格式 (ASFF) 提供。如需詳細資訊，請參閱AWS Security Hub《 使用者指南》中的AWS 安全調查結果格式 (ASFF)。

預期您的原生調查結果中的所有資訊都會完全反映在 ASFF 中。自訂欄位，例如`ProductFields`和`Resource.Details.Other`可讓您將不適合的資料映射到預先定義的欄位。

16要使用的正確區域端點是什麼？

您必須將問題清單傳送至與客戶帳戶相關聯的 Security Hub 區域端點。

17哪裡可以找到區域端點的清單？

請參閱 Security Hub 端點清單。

18我可以提交跨區域調查結果嗎？

Security Hub 尚不支援跨區域提交原生 AWS 服務的調查結果，例如 Amazon GuardDuty、Amazon Macie 和 Amazon Inspector。如果您的客戶允許，Security Hub 不會阻止您提交來自不同區域的調查結果。

在這種情況下，您可以從任何地方呼叫區域端點，ASFF 的資源資訊不必符合端點的區域。不過，`ProductArn` 必須符合端點的區域。

19.傳送問題清單批次的規則和準則是什麼？

您最多可以在 的單一呼叫中批次處理 100 個問題清單或 240 KB`BatchImportFindings`。將問題清單排入佇列並盡可能批次處理，直到達到此限制為止。

您可以從不同的帳戶批次處理一組問題清單。不過，如果批次中的任何帳戶未訂閱 Security Hub，則整個批次會失敗。這是 API Gateway 基準授權模型的限制。

請參閱 the section called “使用 BatchImportFindings API 的指導方針”。

20.我可以將更新傳送到我建立的問題清單嗎？

是，如果您提交具有相同產品 ARN 和相同問題清單 ID 的問題清單，則會覆寫該問題清單的先前資料。請注意，所有資料都會遭到覆寫，因此您應該提交完整的調查結果。

會針對新調查結果和調查結果更新來衡量和計費客戶。

21.我可以將更新傳送到其他人建立的調查結果嗎？

是，如果客戶授予您 `BatchUpdateFindings` API 操作的存取權，您可以使用該操作更新特定欄位。此操作旨在供客戶、SIEMs、票證系統和安全協調、自動化和回應 (SOAR) 平台使用。

22.問題清單如何過時？

Security Hub 會在上次更新日期後 90 天淘汰問題清單。經過這段時間後，會從 Security Hub OpenSearch 叢集中清除過時的問題清單。

如果您使用相同的問題清單 ID 更新問題清單，且問題清單已過時，則會在 Security Hub 中建立新的問題清單。

客戶可以使用 CloudWatch Events 將問題清單移出 Security Hub。這樣做可讓所有調查結果傳送到客戶選擇的目標。

一般而言，Security Hub 建議您每 90 天建立新的問題清單，並且不要永遠更新問題清單。

23.Security Hub 設置了哪些節流？

Security Hub 會調節 `GetFindings` API 呼叫，因為存取問題清單的建議方法是使用 CloudWatch Events。

Security Hub 不會在 API Gateway 和 Lambda 調用強制執行的內部服務、合作夥伴或客戶上執行任何其他限流。

24.對於從來源服務傳送到 Security Hub 的問題清單，SLAs 或預期的時間或延遲為何？

目標是盡可能在初始問題清單和問題清單更新中保持接近即時的時間。您應該在問題清單建立後五分鐘內將問題清單傳送到 Security Hub。

25.如何從 Security Hub 接收問題清單？

若要接收問題清單，請使用下列其中一種方法。

- 所有調查結果都會自動傳送至 CloudWatch Events。客戶可以建立特定的 CloudWatch Events 規則，將問題清單傳送至特定目標，例如 SIEM 或 S3 儲存貯體。此功能取代了舊版 `GetFindings` API 操作。
- 使用 CloudWatch Events 進行自訂動作。Security Hub 可讓客戶從主控台中選取特定問題清單或問題清單群組，並對其採取動作。例如，他們可以將問題清單傳送到 SIEM、票證系統、聊天平台或修復工作流程。這將是客戶在 Security Hub 中執行的警示分類工作流程的一部分。這些稱為自訂動作。

  當使用者選取自訂動作時，會為這些特定問題清單建立 CloudWatch 事件。您可以利用此功能，並建置 CloudWatch Events 規則和目標，供客戶做為自訂動作的一部分使用。請注意，此功能不會用來自動將特定類型或類別的所有調查結果傳送至 CloudWatch Events。這是供使用者對特定問題清單採取動作。

  您可以使用自訂動作 API 操作，例如 `CreateActionTarget`，自動為您的產品建立可用的動作（例如使用 AWS CloudFormation 範本）。您也可以使用 CloudWatch Events 規則 API 操作來建立與自訂動作相關聯的對應 CloudWatch Events 規則。您也可以使用 AWS CloudFormation 範本建立 CloudWatch Events 規則，從 Security Hub 自動擷取所有調查結果或具有特定特性的所有調查結果。

26.受管安全服務提供者 (MSSP) 成為 Security Hub 合作夥伴有哪些要求？

您必須示範 Security Hub 如何作為交付給客戶服務的一部分。

您應該有說明您使用 Security Hub 的使用者文件。

如果 MSSP 是調查結果提供者，他們必須示範將調查結果傳送至 Security Hub。

如果 MSSP 只收到來自 Security Hub 的調查結果，他們必須至少有 AWS CloudFormation 範本來設定適當的 CloudWatch Events 規則。

27.非 MSSP APN 諮詢合作夥伴成為 Security Hub 合作夥伴有哪些要求？

如果您是 APN 諮詢合作夥伴，您可以成為 Security Hub 合作夥伴。您應該提交兩個私有案例研究，以了解您如何協助特定客戶執行下列作業。

- 使用客戶需要的 IAM 許可設定 Security Hub。
- 使用 主控台中合作夥伴頁面上的組態指示，協助將已整合的獨立軟體廠商 (ISV) 解決方案連線至 Security Hub。
- 協助客戶進行自訂產品整合。
- 建立與客戶需求和資料集相關的自訂洞見。
- 建置自訂動作。
- 建置修復手冊。
- 建置符合 Security Hub 合規標準的 Quickstarts。這些必須由 Security Hub 團隊驗證。

案例研究不需要公開共享。

28.如何部署與客戶的 Security Hub 整合有哪些要求？

Security Hub 和合作夥伴產品之間的整合架構，在合作夥伴的解決方案運作方式方面，因合作夥伴而異。您應該確保整合的設定程序不會超過 15 分鐘。

如果您要將整合軟體部署到客戶 AWS 的環境，您應該利用 AWS CloudFormation 範本來簡化整合。有些合作夥伴已建立一鍵式整合，我們非常鼓勵這種方式。

29.我的文件要求是什麼？

您必須提供文件的連結，說明產品與 Security Hub 之間的整合和設定程序，包括範本的使用 AWS CloudFormation 。

該文件還應包含 ASFF 使用情況的相關資訊。具體而言，這應列出您用於不同調查結果的 ASFF 調查結果類型。如果您有任何預設洞見定義，建議您也在此包含這些定義。

考慮包含其他潛在資訊：

- 與 Security Hub 整合的使用案例
- 傳送的調查結果平均數量
- 您的整合架構
- 您執行和不支援的區域
- 問題清單建立和傳送到 Security Hub 之間的延遲
- 您是否更新問題清單

30.什麼是自訂洞見？

建議您為問題清單定義自訂洞見。Insights 是輕量的相互關聯規則，可協助客戶排定哪些問題清單和資源最需要關注和採取行動的優先順序。

Security Hub 具有 `CreateInsight` API 操作。您可以在客戶帳戶內建立自訂洞見，做為 AWS CloudFormation 範本的一部分。這些洞見會出現在客戶的主控台上。

31.我可以提交儀表板小工具嗎？

否，目前沒有。您只能建立受管洞見。

32.您的定價模式為何？

請參閱 Security Hub 定價資訊。

33.作為整合的最終核准程序的一部分，如何將調查結果提交至 Security Hub 示範帳戶？

使用您提供的產品 ARN，使用 `us-west-2`做為區域，將問題清單傳送至 Security Hub 示範帳戶。調查結果應該包含 ASFF `AwsAccountId` 欄位中的示範帳戶號碼。若要取得示範帳戶號碼，請聯絡 Security Hub 團隊。

請勿將任何敏感資料或個人身分識別資訊傳送給我們。此資料用於公開示範。當您傳送此資料給我們時，您即授權我們在示範中使用它。

34.**`BatchImportFindings`**提供哪些錯誤或成功訊息？

Security Hub 提供授權的回應和 的回應`BatchImportFindings`。更清晰的成功、失敗和錯誤訊息正在開發中。

35.來源服務負責處理什麼錯誤？

來源服務負責處理所有錯誤。它們必須處理錯誤訊息、重試、限流和警示。他們也必須處理透過 Security Hub 意見回饋機制傳送的意見回饋或錯誤訊息。

36.常見問題有哪些解決方法？

`AuthorizerConfigurationException` 是由格式不正確`AwsAccountId`或 引起的`ProductArn`。

故障診斷時，請注意下列事項：

- `AwsAccountId` 必須是 12 位數。
- `ProductArn` 必須採用下列格式：arn：aws：securityhub：*`<us-west-2 # us-east-1>`*：*`<accountId>`*：product/*`<company-id>`*/*`<product-id>`*

  帳戶 ID 不會與 Security Hub 團隊提供給您的產品 ARNs中包含的 ID 不同。

AccessDeniedException 當問題清單傳送至錯誤帳戶或從錯誤帳戶傳送，或帳戶沒有 時， 就會產生ProductSubscription。錯誤訊息將包含資源類型為 product或 的 ARNproduct-subscription。此錯誤只會在跨帳戶呼叫期間發生。如果您在 AwsAccountId和 中使用BatchImportFindings自己的帳戶呼叫相同帳戶ProductArn，操作會使用 IAM 政策，而且與無關ProductSubscriptions。

請確定您使用的客戶帳戶和產品帳戶是實際註冊的帳戶。有些合作夥伴已使用產品 ARN 中產品的 帳戶號碼，但請嘗試使用完全不同的帳戶來呼叫 BatchImportFindings。在其他情況下，它們會ProductSubscriptions為其他客戶帳戶建立，甚至為自己的產品帳戶建立。他們沒有ProductSubscriptions為嘗試匯入問題清單的客戶帳戶建立 。

37要將問題、評論和錯誤傳送到哪裡？

<securityhub-partners@amazon.com>

38對於與 全球 AWS 服務相關的項目，我要將問題清單傳送到哪個區域？ 例如，我可以將 IAM 相關調查結果傳送到哪裡？

將問題清單傳送到偵測到問題清單的相同區域。對於 IAM 等服務，您的解決方案可能會在多個區域中發現相同的 IAM 問題。在此情況下，調查結果會傳送至偵測到問題的每個區域。

如果客戶在三個區域中執行 Security Hub，而且全部三個區域中都偵測到相同的 IAM 問題，則將調查結果傳送至全部三個區域。

問題解決時，請將問題清單的更新傳送至您傳送原始問題清單的所有 區域。

合作夥伴整合指南的文件歷史記錄

下表說明本指南的文件更新。

變更	描述	日期
更新主控台標誌的需求	已更新合作夥伴資訊清單和標誌準則，指出合作夥伴必須提供淺色模式和深色模式版本的標誌，才能顯示在 Security Hub 主控台上。標誌必須是 SVG 格式。	2021 年 5 月 10 日
更新新整合合作夥伴的先決條件	Security Hub 現在也允許已加入 AWS ISV 合作夥伴路徑的合作夥伴，以及使用已完成 AWS 基礎技術審查 (FTR) 的整合產品。先前，所有整合合作夥伴都必須是 AWS 選取層合作夥伴。	2021 年 4 月 29 日
ASFF 中的新FindingProviderFields 物件	更新將問題清單映射至 ASFF 的資訊。對於 Confidence 、Criticality 、Severity、RelatedFindings 和 Types，合作夥伴將其值映射到 中的欄位FindingProviderFields 。	2021 年 3 月 18 日
建立和更新問題清單的新原則	新增了一組準則，用於在 Security Hub 中建立新問題清單和更新現有問題清單。	2020 年 12 月 4 日
本指南的初始版本	本合作夥伴整合指南提供 AWS 合作夥伴如何與 建立整合的相關資訊 AWS Security Hub。	2020 年 6 月 23 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。