合作夥伴整合

AWS Security Hub

AWS Security Hub: 合作夥伴整合

Table of Contents

第三方集成概述AWS Security Hub

本指南適用於AWS合作夥伴網絡 (APN) 合作夥伴，希望與AWS Security Hub。

作為 APN 合作夥伴，您可以通過下列一種或多個方式與 Security Hub 整合。

- 將問題清單傳送到 Security Hub
- 使用 Security Hub 的問題清單
- 兩者都將查找結果發送到 Security Hub 並使用來自安全
- 使用 Security Hub 作為託管安全服務提供商 (MSSP) 產品的中心
- 諮詢AWS客户瞭解如何部署和使用 Security Hub

本入門指南主要側重於將問題清單傳送到 Security Hub 的合作夥伴。

主題

為什麼選擇？AWS Security Hub?

AWS Security Hub提供跨 Security Hub 帳户的高優先級安全性警示和安全狀態的全方位檢視。Security Hub 允許像您這樣的合作夥伴將安全調查結果發送到 Security Hub，以便您的客户深入瞭解您生成的安全調查結果。

與 Security Hub 的集成可以通過以下方式增加價值。

- 滿足已請求 Security Hub 集成的客户
- 為您的客户提供其AWS與安全性相關問題清單
- 允許新客户在尋找提供與特定類型安全事件相關調查結果的合作夥伴時發現您的解決方案

在構建與 Security Hub 的集成之前，請檢查集成的原因。如果您的客户希望 Security Hub 與您的產品集成，則集成的可能性更大。您可以完全出於市場營銷原因或獲取新客户構建集成。但是，如果您在沒有任何當前客户輸入的情況下構建集成，並且不考慮客户的需求，則集成可能無法產生預期的結果。

準備將問題清單傳送到AWS Security Hub

作為 APN 合作夥伴，在 Security Hub 團隊允許您作為查找提供商之前，您無法將信息發送到 Security Hub 為您的客户。若要啟用為問題清單提供商，您必須完成下列入步驟。這樣做可以確保您和您的客户獲得積極的 Security Hub 體驗。

完成入職步驟後，請務必遵循the section called “創建和更新調查結果的原則”、the section called “ASFF 映射指導方針”，以及the section called “使用指導方針BatchImportFindingsAPI”。

1. 將您的安全查找結果映射到AWSSecurity 問題清單格式 (ASFF)。
2. 構建您的集成體繫結構，將調查結果推送到正確的區域 Security Hub 端點。為此，您可以定義是否要從您自己的AWS帳户或從您客户的帳户中進行。
3. 讓您的客户將產品訂閱到他們的帳户。若要這樣做，他們可以使用主控台或EnableImportFindingsForProductAPI 操作。請參閱管理產品整合中的AWS Security Hub 使用者指南。

   您也可以為他們訂閱產品。若要這樣做，您可以使用跨賬户角色來訪問EnableImportFindingsForProduct代表客户執行 API 操作。

   此步驟建立了為該帳户接受來自該產品的查找結果所需的資源策略。

以下博客文章討論了與 Security Hub 的一些現有合作夥伴集成。

- 宣佈雲託管人與AWS Security Hub
- 使用AWS Fargate和 Prowler 發送關於AWS服務到 Security Hub
- 如何匯入AWS Config將評估作為 Security Hub 中的問題清單

準備接收來自AWS Security Hub

要接收來自AWS Security Hub，請使用下列其中一個選項：

- 讓客户自動將所有調查結果發送到CloudWatch事件 客户可以創建特定的CloudWatch事件規則將查找結果發送到特定目標（如 SIEM 或 S3 存儲桶）。
- 讓您的客户從 Security Hub 控制台中選擇特定的查找結果或查找結果組，然後對其採取措施。

例如，您的客户可以將調查結果發送到 SIEM、票證系統、聊天平台或修正工作流。這將是客户在 Security Hub 內執行的警報分類工作流的一部分。

這些被稱為自定義操作。當用户執行自定義操作時，CloudWatch事件為這些特定的查找結果創建。作為合作夥伴，您可以利用此功能並構建CloudWatch事件規則或目標，供客户用作自定義操作的一部分。請注意，此功能不會自動將特定類型或類的所有查找結果發送到CloudWatch事件 此功能用於用户對特定的查找結果採取操作。

下列博客文章概述了使用與 Security Hub 和CloudWatch自訂動作的事件。

- 如何整合AWS Security Hub使用自訂動作PagerDuty
- 如何啟用自訂動作AWS Security Hub
- 如何匯入AWS Config將評估作為 Security Hub 中的問題清單

用於學習的資源AWS Security Hub

以下材料可以幫助您更好地瞭解AWS Security Hub解決方案和方式AWS客户可以使用該服務。

- 介紹AWS Security Hub視頻
- Security Hub 用户指南
- Security Hub API 參考
- 入門網絡研討會

我們還鼓勵您在您的AWS帳户，並獲得一些服務的實踐經驗。

合作夥伴先決條件

在您可以開始與AWS Security Hub，您必須符合下列條件之一：

- 您是一個AWS選擇級別合作夥伴或更高級別。
- 您已加入AWSISV 合作夥伴，並且您用於 Security Hub 成的產品已完成AWS基礎技術審查 (FTR)。該產品然後被授予一個「審查AWS徽章

您還必須與AWS。

集成使用案例及所需許可

AWS Security Hub允許AWS客户接收來自 APN 合作夥伴的調查結果。合作夥伴的產品可能會在客户的AWS帳户。客户帳户中的權限配置因合作夥伴產品使用的模型而有所不同。

在 Security Hub 中，客户始終控制哪些合作夥伴可以將調查結果發送到客户的帳户。客户可以隨時撤銷合作夥伴的權限。

為了使合作夥伴能夠向其帳户發送安全查找結果，客户首先訂閱 Security Hub 中的合作夥伴產品。訂閱步驟對於下面概述的所有使用案例都是必需的。如需有關客户如何管理產品集成的詳細信息，請參見管理產品整合中的AWS Security Hub使用者指南。

客户訂閱合作夥伴產品後，Security Hub 會自動創建託管資源策略。政策會授予合作夥伴產品使用BatchImportFindingsAPI 操作，以將問題清單傳送到客户帳號的 Security Hub。

以下是與 Security Hub 集成的合作夥伴產品的常見情況。這些信息包括每個用例所需的其他權限。

合作夥伴託管：來自合作夥伴賬户的調查

此使用案例涵蓋了在自己的AWS帳户。若要發送AWS客户，合作夥伴調用BatchImportFindingsAPI 操作，從合作夥伴產品帳户。

對於此使用案例，客户帳户只需要客户訂閱合作夥伴產品時建立的權限。

在合作夥伴賬户中，調用BatchImportFindingsAPI 操作必須具有 IAM 政策，允許委託人呼叫BatchImportFindings。

使合作夥伴產品能夠在 Security Hub 中向客户發送調查結果是一個兩步過程：

1. 客户在 Security Hub 中創建合作夥伴產品的訂閱。
2. Security Hub 會在客户確認後生成正確的託管資源策略。

要發送與客户帳户相關的安全調查結果，合作夥伴產品使用自己的憑據調用BatchImportFindingsAPI 操作。

以下是一個 IAM 策略示例，該策略向合作夥伴賬户中的委託人授予必要的 Security Hub 權限。

```
{
    "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：從客户帳户發送的調查結果

此使用案例涵蓋了在自己的AWS帳户，但使用跨賬户角色訪問客户的帳户。他們呼叫BatchImportFindingsAPI 操作，從客户帳號。

對於此用例，要調用BatchImportFindingsAPI 操作時，合作夥伴賬户將承擔客户賬户中的客户管理 IAM 角色。

此呼叫是從客户的帳户發出的。因此，託管資源策略必須允許在呼叫中使用合作夥伴產品帳户的產品 ARN。Security Hub 託管資源策略授予合作夥伴產品帳户和合作夥伴產品 ARN 的權限。產品 ARN 是合作夥伴作為提供商的唯一標識符。由於呼叫不來自合作夥伴產品帳户，因此客户必須明確授予合作夥伴產品向 Security Hub 發送查找結果的權限。

合作夥伴和客户帳户之間的跨賬户角色的最佳做法是使用合作夥伴提供的外部標識符。此外部標識符是客户賬户中跨賬户策略定義的一部分。夥伴在擔任角色時必須提供標識符。當授予時，外部標識符可提供額外的安全層AWS帳號的存取權限。唯一標識符可確保合作夥伴使用正確的客户帳户。

使合作夥伴產品能夠使用跨賬户角色向 Security Hub 中的客户發送調查結果，分為四個步驟：

1. 客户或使用跨賬户角色代表客户工作的合作夥伴在 Security Hub 中開始訂閱產品。
2. Security Hub 會在客户確認後生成正確的託管資源策略。
3. 客户可以手動配置或使用AWS CloudFormation。如需跨帳號角色的詳細信息，請參提供AWS由第三方擁有的帳中的IAM User Guide。
4. 產品安全地存儲客户角色和外部 ID。

接下來，產品會將問題清單傳送到 Security Hub：

1. 產品調用AWS Security Token Service(AWS STS）以擔任客户角色。

2. 產品調用BatchImportFindingsAPI 操 Security Hub，使用代入角色的臨時證書。

此為 IAM 政策的範例，可將必要的 Security Hub 許可授予合作夥伴的跨帳户角色。

```
{
    "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"
        }
    ]
}
```

所以此Resource部分標識特定產品訂閱。這可確保合作夥伴只能發送客户訂閱的合作夥伴產品的調查結果。

客户託管：從客户賬户發送的調查結果

此使用案例涵蓋了具有部署在客户的AWS帳户。所以此BatchImportFindingsAPI 是從客户賬户中運行的解決方案調用的。

對於此使用案例，必須向合作夥伴產品授予其他權限才能調用BatchImportFindingsAPI。授予此權限的方式因合作夥伴解決方案及其在客户帳户中的配置方式而有所不同。

此方法的一個示例是在客户賬户中的 EC2 實例上運行的合作夥伴產品。此 EC2 實例必須附加一個 EC2 實例角色，該角色授予該實例調用BatchImportFindingsAPI 操作。這允許 EC2 實例向客户的賬户發送安全調查結果。

此使用案例在功能上等同於客户將調查結果加載到他們擁有的產品的帳户中的情況。

客户允許合作夥伴產品將調查結果從客户的帳户發送到 Security Hub 中的客户：

1. 客户將合作夥伴產品部署到他們的AWS帳户手動使用AWS CloudFormation或其他部署工具。
2. 客户定義了合作夥伴產品在將調查結果發送到 Security Hub 時使用的必要 IAM 策略。
3. 客户將策略附加到合作夥伴產品的必要組件，例如 EC2 實例、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開發套件或AWS CLI呼叫BatchImportFindingsAPI 操 Security Hub。它從附加策略的客户帳户中的組件發出呼叫。
2. 在 API 調用期間，將生成必要的臨時證書，以允許BatchImportFindings呼叫成功。

以下是 IAM 策略示例，該策略向客户賬户中的合作夥伴產品授予必要的 Security Hub 權限。

```
{
    "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"
        }
    ]
}
```

合作夥伴入職流程

作為合作夥伴，您可以期待完成幾個高級別步驟，作為入職流程的一部分。您必須完成這些步驟，然後才能將安全查找結果發送到AWS Security Hub。

1. 您可以與 APN 合作夥伴團隊或 Security Hub 團隊開展合作，並表示有興趣成為 Security Hub 的合作夥伴。您可以確定要添加到 Security Hub 通信渠道的電子郵件地址。
2. AWS為您提供 Security Hub 合作夥伴入職材料。
3. 您將被邀請使用 Security Hub 合作夥伴 Slack 渠道，您可以在該渠道中詢問與您的集成相關的問題。
4. 您可以向 APN 合作夥伴聯繫人提供產品集成清單草稿以供審核。

   商品集成清單包含用於創建合作夥伴產品亞馬遜資源名稱 (ARN) 的信息，以便與AWS Security Hub。

   它為 Security Hub 團隊提供了顯示在 Security Hub 控制台的合作夥伴提供商頁面上的信息。它還用於提出與集成相關的新託管見解，以添加到 Security Hub 洞察庫。

   此初始版本的產品集成清單不一定具有完整的詳細信息。但它至少應該包含用例和數據集信息。

   如需清單和所需信息的詳細資訊，請參產品整合資訊。
5. Security Hub 團隊為您的產品提供產品 ARN。您可以使用 ARN 將問題清單傳送到 Security Hub。
6. 您可以構建集成以向 Security Hub 發送查找結果或從安全中心接收查找結果。

   將調查結果映射到 ASFF

   要將查找結果發送到 Security Hub，您必須將您的查找結果映射到AWSSecurity 問題清單格式 (ASFF)。

   ASFF 提供了一致的調查結果描述，可以在AWS安全服務、合作夥伴和客户安全系統。這減少了集成工作，鼓勵使用通用語言，併為實施者提供了藍圖。

   ASFF 是必需的線路協議格式，用於將查找結果發送到AWS Security Hub。查找結果表示為符合 ASFF JSON 架構和 RFC-7493 I-JSON 消息格式的 JSON 文檔。有關 ASFF 架構的詳細信息，請參閱AWS安全問題清單格式 (ASFF)中的AWS Security Hub使用者指南。

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

構建和測試集成

您可以使用AWS帳户。這樣做可以讓您完全瞭解查找結果在 Security Hub 中的顯示方式。它還可以幫助您瞭解客户對您的安全發現的體驗。

您使用BatchImportFindingsAPI 操作，將新問題清單傳送到 Security Hub。

在構建 Security Hub 集成的整個過程中，AWS鼓勵您隨時向 APN 合作夥伴聯繫人通報您的集成進度。您也可以向 APN 合作夥伴聯繫人尋求有關集成問題的幫助。

請參閱the section called “使用指導方針BatchImportFindingsAPI”。

7. 您將向 Security Hub 產品團隊演示集成。必須使用 Security Hub 團隊擁有的帳户來演示此集成。

   如果他們對集成感到滿意，則 Security Hub 團隊會批準前進將您列為提供商。
8. 您提供AWS並提供最終清單供審查.
9. Security Hub 團隊在 Security Hub 控制台中創建提供程序集成。然後，客户可以發現並啟用集成。
10. （可選）您參與其他營銷工作，以促進您的 Security Hub 集成。請參閱Go-to-market活動。

    至少，Security Hub 建議您提供以下資產。
    - 一個演示視頻（最多 3 分鐘）的工作集成。該視頻用於市場營銷目的，並發佈到AWS YouTube頻道。
    - 用於添加到 Security Hub 第一個呼叫幻燈片的單幻燈片體繫結構圖。

Go-to-market活動

合作夥伴還可以參與可選的營銷活動，以幫助解釋和推廣他們的AWS Security Hub整合。

如果要創建與 Security Hub 相關的自己的營銷內容，請在發佈內容之前將草稿發送給 APN 合作夥伴經理以供審核和批準。這可確保每個人都在消息傳遞上保持一致。

AWS合作夥伴網絡 (APN) 合作夥伴可以使用 APN 合作夥伴營銷中心和市場開發基金 (MDF) 計劃來創建營銷活動並獲得資金支持。有關這些計劃的詳細信息，請聯繫您的合作夥伴經理。

Security Hub 合作夥伴頁面上的條目

在您被批準為 Security Hub 合作夥伴後，您的解決方案可以顯示在AWS Security Hub合作夥伴頁。

要在此頁面上列出，請向您的 APN 合作夥伴聯繫人提供以下詳細信息。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)，或者發送電子郵件至<securityhub-pms@amazon.com>。

- 簡要說明瞭您的解決方案、其與 Security Hub 的集成以及與 Security Hub 集成為客户提供的價值。此描述限製為 700 個字符（包括空格）。
- 描述您的解決方案的頁面的 URL。本網站應特定於您的AWS集成，更具體地説，您的 Security Hub 集成。它應關注客户體驗以及客户在使用集成時獲得的價值。
- 您的徽標的高分辨率副本，為 600 x 300 像素。關於此徽標的詳細資訊，請參the section called “標誌的合作夥伴頁面”。

按稿

作為認可的合作夥伴，您可以選擇在您的網站和公共關係渠道上發佈新聞稿。新聞稿必須由AWS。

在發佈新聞稿之前，您必須將其提交到AWS，以供 APN 合作夥伴營銷、Security Hub 領導層和AWS外部安全事務處. 新聞稿可包括一份關於 ESS 副總裁的建議報價。

要啟動此過程，請使用 PDM。我們的服務級別協議 (SLA) 為期 10 個工作日，以查看新聞稿。

AWS合作夥伴網絡 (APN) 博客

我們還可以幫助您發佈您創作的博客條目到 APN 博客。博客條目必須側重於客户案例和使用案例。它不能僅僅侷限於成為集成發佈合作夥伴。

如果您有興趣，請聯繫您的 PDM 或 PSA 開始該過程。APN 博客可能需要 8 周或更長時間才能獲得最終批準和發佈。

關於 APN 博客需要瞭解的關鍵事項

當您建立博客文章時，請謹記下列事項。

什麼進入博客文章？

合作夥伴職位應該是教育性的，並提供深入的專業知識，涉及AWS客户。

理想的長度不超過 1500 個字。讀者重視深入的教育內容，教導他們AWS。

內容應該是 APN 博客的原創內容。請勿重新調整來自源（如現有博客文章或白皮書）的內容。

發佈到 APN 博客的其他限制是什麼？

只有高級或高級級別合作夥伴才能發佈到 APN 博客。具有 APN 計劃指定（如服務交付）的選定合作夥伴存在例外情況。

每個夥伴每年限於 3 個員額。擁有成千上萬的 APN 合作夥伴，AWS必須是公平的覆蓋範圍.

每個帖子都必須有一名技術贊助商，他們可以驗證解決方案或使用案例。

編輯博客文章需要多長時間才能發佈？

在您提交博客文章的第一篇完整草稿後，需要四到六週的時間進行編輯。

為什麼要寫 APN 博客？

APN 博客文章可提供以下優勢。

- 可信度— 對於 APN 合作夥伴，有一個由AWS可以影響全球客户。
- Visibility— APN 博客是讀取最多的博客之一，位於AWS，2019 年的頁面瀏覽量為 179 萬次，包括受影響的流量。
- 商業— APN 合作夥伴帖子具有連接按鈕，可以通過 APN 客户互動 (ACE) 計劃生成潛在客户。

什麼類型的內容最適合？

以下類型的內容最適合 APN 博客文章。

- 技術內容是最流行的故事類型。這包括解決方案聚焦和操作方法信息。超過 75% 的讀者看到這一技術內容。
- 客户重視 200 級或更高級別的故事，這些故事展示了某些內容如何運作AWS或 APN 合作夥伴如何為客户解決業務問題。
- 技術專家或主題專家撰寫的帖子表現最佳。

光滑的工作表或營銷表

光滑的表格是一個單頁的文檔，概述了您的產品、其集成體繫結構和聯合客户使用案例。

如果您為集成創建了一個光滑的工作表，請將副本發送給 Security Hub 團隊。他們會將其添加到合作夥伴頁面。

白皮書或電子書

如果您創建了概述產品、其集成體繫結構和聯合客户使用案例的白皮書或電子書，請將副本發送給 Security Hub 團隊。他們會將其添加到 Security Hub 合作夥伴頁面。

網路研討會

如果您舉辦了有關集成的網絡研討會，請將網絡研討會的記錄發送給 Security Hub 團隊。團隊將從合作夥伴頁面鏈接到它。

團隊還可以提供 Security Hub 主題專家參加您的網絡研討會。

示範影片

出於營銷目的，您可以製作工作集成的演示視頻。在您的視頻平台帳户上發佈此視頻，Security Hub 團隊將從合作夥伴頁面鏈接到該視頻。

產品整合資訊

每個AWS Security Hub整合合作夥伴都必須完成產品整合資訊清單，以提供所提議整合的必要詳細資料。

安全性中樞小組會以下列幾種方式使用此資訊：

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

若要評估提議的整合品質和提供的資訊，Security Hub 小組會使用the section called “產品準備情況清單”. 此檢查清單決定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文件中。

您可以從合AWS Security Hub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，合作夥伴頁面在中國 (中國) 和中國 (寧夏) 區域提供。

內容

- 心跳發現
- 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針對不同目的進行設定。

尋找提供者和消費者使用案例

獨立軟體廠商 (ISV) 需要。

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發現項目，請注意，在本節中，然後完成下一節。

下列資訊必須反映在您的文件中。

- 你會發送發現，接收發現，或兩者兼而有之？
- 如果您打算傳送發現項目，您會傳送哪些類型的發現項目？ 您是否會傳送所有發現項目或特定的發現項目子集？
- 如果您計劃收到調查結果，您將如何處理這些發現？ 您將收到哪些類型的發現？ 例如，您是否會收到所有發現項目、特定類型的發現項目，還是只收到客戶選取的特定搜尋結果？
- 您計劃更新發現項目嗎？ 如果是這樣，您將更新哪些字段？ Security Hub 建議您更新發現項目，而不是永遠建立新發現項目。更新現有的發現有助於減少客戶的發現噪音。

  若要更新發現項目，您可以傳送包含指派給您已傳送之發現項目的尋找項目 ID 的發現項目。

若要儘早取得使用案例和資料集的意見反應，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，則需要此項。

為您使用 Security Hub 的工作提供兩個客戶使用案例。這些可以是私人用例。Security Hub 小組不會在任何地方公告它們。這些名稱應該描述下列其中一個或兩個動作。

- 您如何幫助客戶引導 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？
- 您如何協助客戶運作及擴充 Security Hub？ 例如，您是否提供了回應或補救範本、內建的自訂整合，或是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。

針對您將傳送至 Security Hub 的發現項目，請提供下列資訊。

- 以其原生格式顯示的發現項目，例如 JSON 或 XML
- 您將如何將問題清單轉換為AWS安全問題清單格式 (ASFF)

如果您需要對 ASFF 進行任何更新，以支援您的整合，請告知 Security Hub 小組。

架構

如果您將問題清單傳送到 Security Hub 或從 Security Hub 接收問題清單。

說明您將如何與 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。準備架構圖時，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？
- 如果您要將發現項目傳送至 Security Hub，您是否會從客戶AWS帳戶或您自己AWS的帳戶傳送發現項目？
- 如果您將收到調查結果，您將如何使用 CloudWatch 事件整合？
- 您將如何將調查結果轉換為 ASFF？
- 您將如何批量調查結果，跟踪發現狀態，並避免節流限制？

組態

如果您將問題清單傳送到 Security Hub 或從 Security Hub 接收問題清單。

說明客戶將如何設定與 Security Hub 的整合。

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

組態應該花不超過 15 分鐘。您的產品說明文件也必須提供整合的組態指引。

每位客戶每天的平均搜尋結果

如果您將問題清單傳送到 Security Hub。

您預計每月有多少個尋找更新 (平均和上限) 傳送至整個客戶群的 Security Hub？ 數量級估計是可以接受的。

Latency (延遲)

如果您將問題清單傳送到 Security Hub。

您將多快速批次處理問題清單傳送到 Security Hub？ 換句話說，從產品中建立發現項目到傳送至 Security Hub 的延遲為何？

此資訊必須反映在您的產品文件中，才能進行整合。這是客戶的常見問題。

公司及產品說明

與 Security Hub 的所有整合都需要。

簡要說明您的公司和產品，並特別著重於 Security Hub 整合的性質。我們在 Security Hub 合作夥伴頁面上使用此功能。

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

每個描述不得超過 700 個字元 (含空格)。

夥伴網站資產

與 Security Hub 的所有整合都需要。

您至少必須在 Security Hub 合作夥伴頁面上提供用於深入瞭解超連結的 URL。它應該是描述產品與 Security Hub 之間整合的行銷登陸頁面。

如果您將多個產品與 Security Hub 整合，您可以為其建立單一登陸頁面。Security Hub 建議此登陸頁面包含設定指示的連結。

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 也會從他們的合作夥伴頁面連結到這些資訊。

標誌的合作夥伴頁面

所有 Security Hub 整合都需要。

提供標誌的 URL，以顯示在 [安全中心合作夥伴] 頁面上。標誌必須符合下列條件：

- 尺寸：600 x 300 像素
- 裁剪：緊，沒有填充
- 背景：透明
- 格式:PNG 格式

Security Hub 主控台的圖誌

所有整合都需要。

提供要在 Security Hub 主控台上顯示之淺色模式和深色模式圖誌的 URL。

圖誌必須符合下列條件：

- 格式：SVG 格式
- 尺寸：175 x 40 像素。如果較大，圖像應該使用該比例。
- 裁剪：緊無填充
- 背景：透明

如需小標誌的詳細指南，請參閱the section called “控制台徽標的指南”。

尋找類型

如果您將問題清單傳送到 Security Hub。

提供一個表格，此表格會記錄您使用的 ASFF 格式的尋找項目類型，以及它們與原生發現項目類型的對齊方式。如需在 ASFF 中尋找型態的詳細資訊，請參閱《AWS Security Hub使用者指南》中的ASFF 的類型分類。

建議您也在產品文件中提供這項資訊。

熱線

與 Security Hub 的所有整合都需要。

提供技術聯絡人的電子郵件地址、電話號碼或呼叫器號碼。Security Hub 會就任何技術問題 (例如當整合不再有效時) 與此連絡人溝通。

此外，針對高嚴重性的技術問題，提供全年無休的聯絡窗口。

心跳發現

建議您在將問題清單傳送到 Security Hub。

您是否可以每五分鐘傳送一次「活動訊號」，表示您與 Security Hub 的整合功能正常運作？

如果可以的話，請使用查找類型來執行此操作`Heartbeat`。

AWS Security Hub主控台資訊

提供 JSON 文字給包含下列資訊的AWS Security Hub團隊。Security Hub 會使用此資訊建立您的產品 ARN、在主控台中顯示提供者清單，並在 Security Hub 深入解析程式庫中包含您提議的受管理見解。

公司資訊

公司信息提供有關您公司的信息。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	公司的唯一識別碼。公司識別碼在公司間必須是唯一的。

欄位	必要	描述
		這可能與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 主控台上顯示之提供者公司的說明。 類型：字串 長度上限：200 個字元

產品資訊

此區段提供您產品的相關資訊。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發現項目傳送至 Security Hub、接收來自 Security Hub 的發現項目，或同時傳送和接收發現項目。 如果您是諮詢合作夥伴，請將此欄位留空。 類型：字串陣列 有效值：SEND_FINDINGS_TO_SECURITY_HUB | RECEIVE_FINDINGS_FROM_SECURITY_HUB
id	是	產品的唯一識別碼。這些名稱在公司內必須是唯一的。這些名稱在公司間不需要是唯一的。這可能與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	您不支援以下哪些AWS地區？ 換句話說，Security Hub 在哪些地區不應該在 Security Hub 控制台的合作夥伴頁面中顯示您作為選項？

欄位	必要	描述
		類型：字串 僅提供區域代碼。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。 的區域代碼為`us-gov-west-1` (AWS GovCloud (US)用於AWS GovCloud (美國西部)) 和`us-gov-east-1` (用於AWS GovCloud (美國東部))。 中國地區的區域代碼為`cn-north-1` (適用於中國 (北京)) 和`cn-northwest-1` (中國 (寧夏))。
`commercialAccountNumber`	是	「AWS區域」產品的主要AWS科目編號。 如果您將發現項目傳送至 Security Hub，則您提供的帳戶會根據您傳送發現項目的位置而定。 • 從您的AWS帳戶。在此情況下，請提供您用來提交發現項目的帳號。 • 從客戶的AWS帳戶。在此情況下，Security Hub 建議您提供用來測試整合的主要帳戶號碼。 理想情況下，您將在所有區域中對所有產品使用相同的帳戶。如果這是不可能的，請連絡 Security Hub 小組。 如果您只收到來自 Security Hub 的發現項目，則不需要此帳號。 類型：字串

欄位	必要	描述
`govcloudAccountNumber`	否	「AWS GovCloud (US)地區」產品的主要AWS帳戶號碼 (如果您的產品在中提供AWS GovCloud (US))。 如果您將發現項目傳送至 Security Hub，則您提供的帳戶會根據您傳送發現項目的位置而定。 • 從您的AWS帳戶。在此情況下，請提供您用來提交發現項目的帳號。 • 從客戶的AWS帳戶。在此情況下，Security Hub 建議您提供用來測試整合的主要帳戶號碼。 理想情況下，您對所有AWS GovCloud (US)區域的所有產品都使用相同的帳戶。如果這是不可能的，請連絡 Security Hub 小組。 如果您只收到來自 Security Hub 的發現項目，則不需要此帳號。 類型：字串

欄位	必要	描述
chinaAccountNumber	否	中國地區產品的主要AWS帳戶號碼 (如果您的產品在中國地區有售)。 如果您將發現項目傳送至 Security Hub，則您提供的帳戶會根據您傳送發現項目的位置而定。 • 從您的AWS帳戶。在此情況下，請提供您用來提交發現項目的帳號。 • 從客戶的AWS帳戶。在此情況下，Security Hub 建議您提供用來測試產品整合的主要帳戶號碼。 理想情況下，您在所有中國地區的所有產品都使用相同的帳戶。如果這是不可能的，請連絡 Security Hub 小組。 如果您只收到來自 Security Hub 的調查結果，這可以是您在中國地區擁有的任何帳戶。 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說明。 類型：字串 長度上限：200 個字元

欄位	必要	描述
importType	是	合作夥伴的資源策略類型。 在合作夥伴上線程序期間，您可以指定下列其中一項資源政策，或者您可以指定NEITHER。 • 使用時BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT，您只能從產品 ARN 中列出的帳戶將發現項目傳送至安全中樞。 • 使用時BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT，您只能從訂閱您的客戶帳戶傳送發現項目。 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	定義產品的類別。您的選擇會顯示在安全中樞主控台上。 最多可選擇三個類別。 不允許自訂選取項目。如果您認為您的類別遺失，請連絡 Security Hub 團隊。 類型：陣列 可用類別： • 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 會顯示在資訊安全中心主控台中。 類型：字串 這必須是一個AWS Marketplace網址。 如果您沒有物AWS Marketplace品，請將此欄位留空。

欄位	必要	描述
`configurationUrl`	是	與 Security Hub 整合的相關產品文件的 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 您的文件應該包含下列資訊。 • 組態說明 • 連結至AWS CloudFormation範本 (如有必要) • 有關您用於整合的使用案例的資訊 • Latency (延遲) • ASFF 映射 • 包括問題清單類型 • 架構

指導方針和清單

當您準備所需的材料AWS Security Hub集成，請使用這些準則。

就緒情況核對錶用於在 Security Hub 將其提供給 Security Hub 客户之前對集成進行最終審查。

主題

標識顯示在AWS Security Hub安慰

為了使徽標顯示在AWS Security Hub主控台，請遵循這些指導方針。

淺色和深色模式

您必須同時提供標誌的亮光模式和深色模式版本。

格式

SVG 檔案格式

Background color (背景顏色)

Transparent

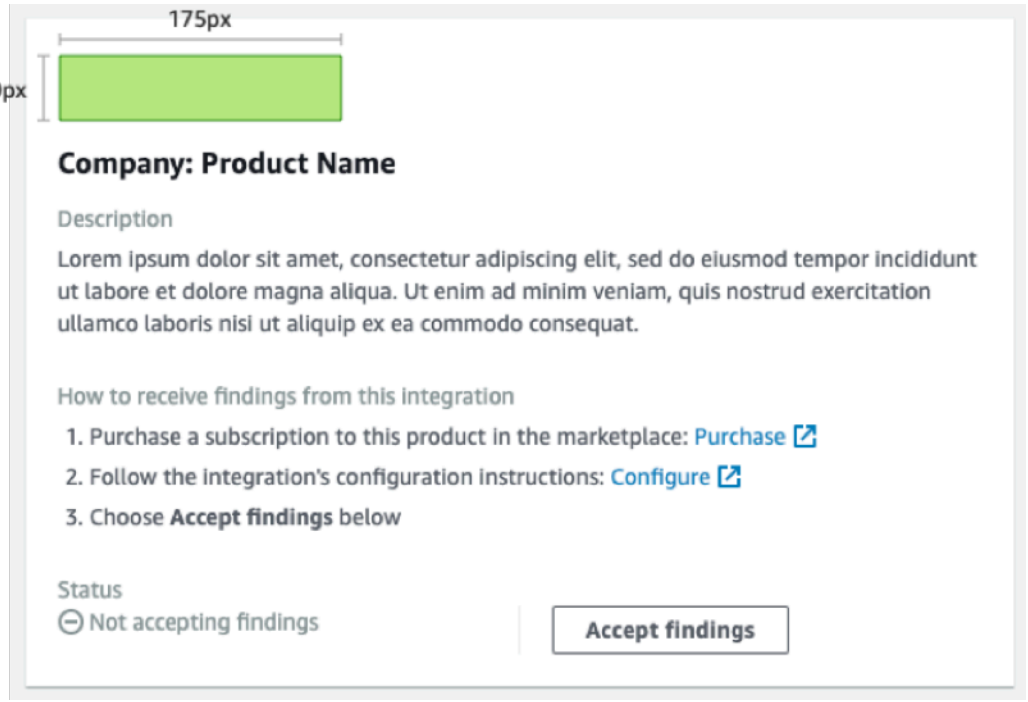
大小

理想的比率為 175 像素寬，40 像素高。

最小高度為 40 像素。

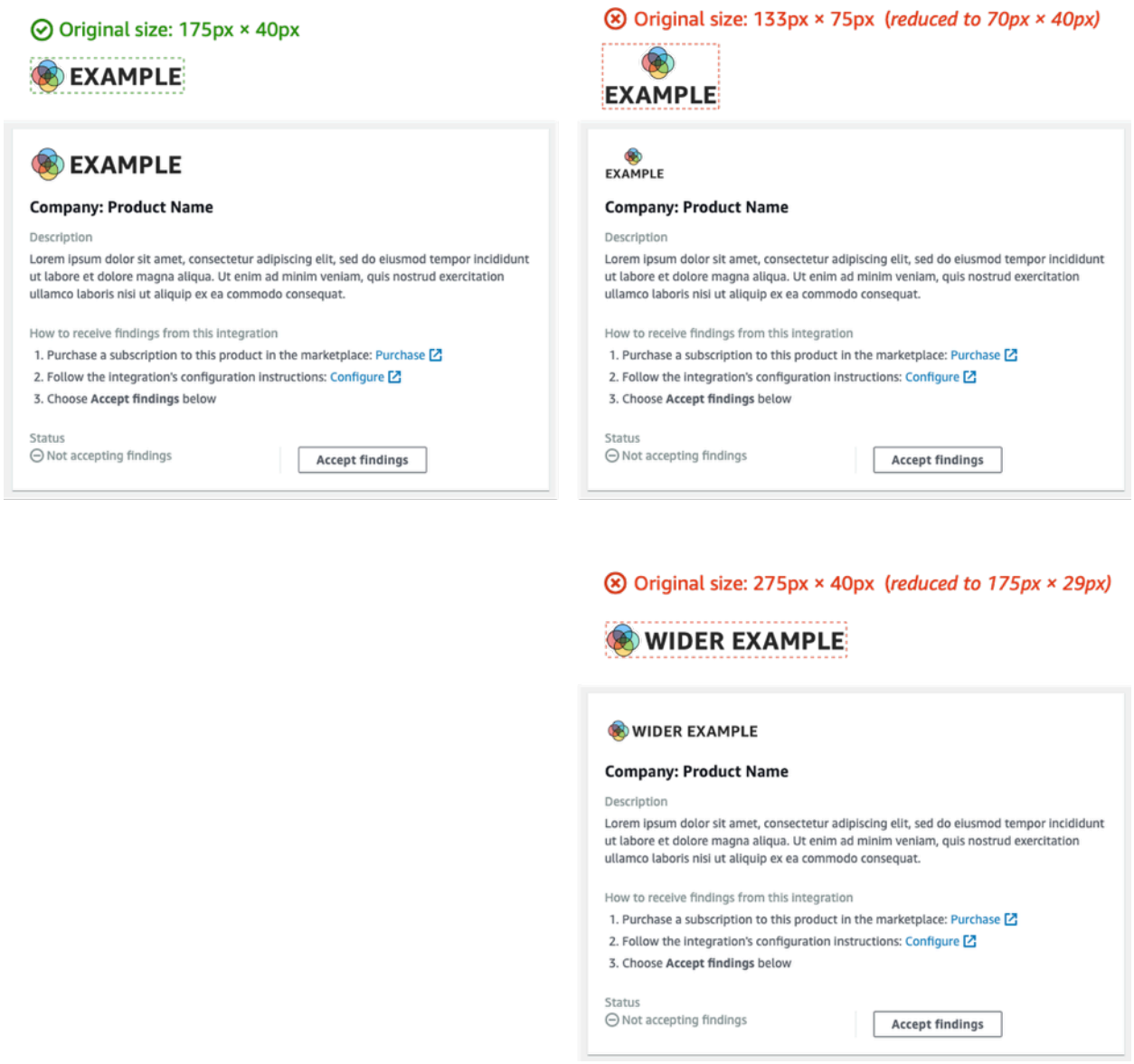
矩形徽標效果最佳。

下圖顯示了理想徽標在 Security Hub 控制台上的顯示方式。



如果您的徽標與這些尺寸不匹配，Security Hub 將尺寸縮小到 40 像素的最大高度，最大寬度為 175 像素。這會影響徽標在 Security Hub 控制台上的顯示方式。

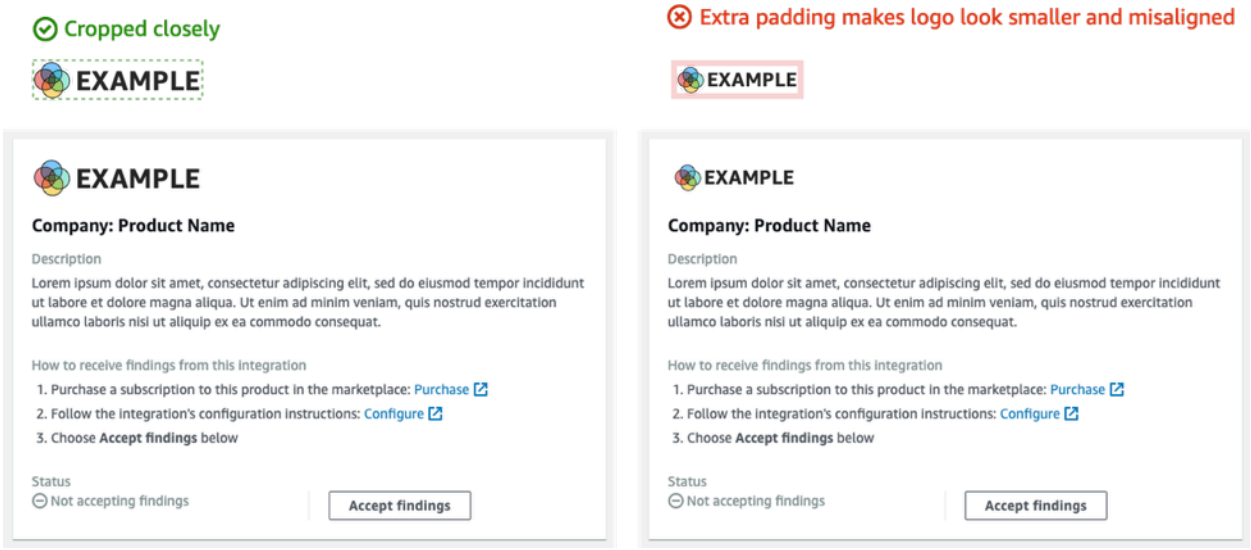
下圖將使用理想尺寸的徽標顯示與較寬或更高的徽標進行比較。



裁剪

儘可能靠近地裁剪徽標圖像。請勿提供額外的填充。

下圖顯示了緊密裁剪的徽標與具有額外填充的徽標之間的區別。



創建和更新調查結果的原則

在您規劃如何創建和更新AWS Security Hub，請謹記下列原則。

使調查結果具體化，以便客户可以輕鬆採取措施。

客户希望自動執行響應和補救操作，並將調查結果與其他調查結果關聯起來。為了支持這一點，調查結果應具有下列特性：

- 它們一般應該處理單一或主要資源。
- 他們應該有一個查找類型。
- 他們應該處理一個安全事件。

當查找結果包含多個安全事件的數據時，客户更難對查找結果採取措施。

將所有查找字段映射到AWS安全問題清單格式 (ASFF)。允許客户依賴 Security Hub 作為真相來源。

客户期望本機查找格式的每個字段也會在 Security Hub ASFF 中表示。

客户希望所有數據都存在於查找結果的 Security Hub 版本中。缺少數據會導致他們失去對作為安全信息的核心來源的安全 Hub 的信任。

最大限度地減少發現冗餘。不要因為查找卷而壓倒客户。

Security Hub 不是常規日誌管理工具。您應將調查結果發送到 Security Hub，這些調查結果非常可操作，客户可以直接響應、修正或與其他調查結果關聯。

如果查找結果只有一個小的更改，請更新查找結果，而不是創建新的查找結果。

當查找結果發生重大更改時（如嚴重性分數或資源標識符），請創建新的查找結果。

例如，為單個端口掃描實時創建查找結果不是高度可操作的。由於端口掃描可以持續進行，因此會產生大量的發現。簡單地更新上次掃描時間和掃描計數，以便從 TOR 節點上對 MongoDB 端口進行端口掃描的單個查找結果更具吸引力和精確性。

允許客户自定義他們的調查結果，使其更有意義。

客户希望能夠調整某些查找字段，使其與其環境或要求更加相關。

例如，客户希望能夠根據帳户類型或查找結果關聯的資源類型添加註釋、標籤和調整嚴重性分數。

將調查結果映射到AWS安全問題清單格式 (ASFF)

請使用下列準則將您的調查結果映射到 ASFF。有關每個 ASFF 字段和對象的詳細説明，請參閱AWS安全問題清單格式 (ASFF)中的AWS Security Hub使用者指南。

識別信息

`SchemaVersion` 始終是 `2018-10-08`。

`ProductArn`是 ARN，AWS Security Hub分配給你。

`Id`是 Security Hub 用於索引查找結果的值。查找結果標識符必須是唯一的，以確保其他查找結果不會被覆蓋。要更新查找結果，請使用相同的標識符重新提交查找結果。

`GeneratorId`可以與`Id`或者可以引用離散邏輯單元，例如亞馬遜GuardDuty偵測器 ID、AWS Config記錄器 ID 或 IAM 訪問分析器 ID。

Title 與 Description

`Title`應該包含有關受影響資源的一些信息。`Title`限製為 256 個字元，包括空格。

將更長的詳細信息添加到`Description`。`Description`限製為 1024 個字元，包括空格。您可以考慮將截斷添加到描述中。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.",
```

問題清單類型

您提供您的查找類型信息FindingProviderFields.Types。

Types應該與類型 ASFF 的類型分類。

如果需要，您可以指定一個自定義分類器（第三個命名空間）。

時間戳記

ASFF 格式包含幾個不同的時間戳。

CreatedAt 與 UpdatedAt

您必須提交CreatedAt和UpdatedAt每次調用BatchImportFindings對於每個發現。

這些值必須與 Python 3.8 中的 ISO8601 格式匹配。

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

FirstObservedAt 與 LastObservedAt

FirstObservedAt和LastObservedAt必須與系統觀察結果時匹配。如果您不記錄此信息，則不需要提交這些時間戳。

這些值與 Python 3.8 中的 ISO8601 格式相匹配。

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

Severity

您可以在FindingProviderFields.Severity對象，其中包含下列欄位。

Original

系統中的嚴重性值。Original可以是任何字符串，以適應您使用的系統。

Label

查找嚴重性所需的 Security Hub 指示符。允許的值為：

- INFORMATIONAL— 找不到任何問題。
- LOW— 問題不需要自身採取動作。

- MEDIUM問題必須解決，但不緊急。
- HIGH問題必須優先處理。
- CRITICAL— 問題必須立即修補以防止進一步的傷害。

符合要求的調查結果應始終具有Label設定為INFORMATIONAL。範例INFORMATIONAL調查結果是來自通過的安全檢查結果，AWS Firewall Manager調查結果被補救。

客户通常按其嚴重性對調查結果進行排序，以便為其安全運營團隊提供待辦事項列表。將查找嚴重性設置為HIGH或者CRITICAL。

您的集成文檔必須包含映射理由。

Remediation

Remediation有兩個元素。這些元素在 Security Hub 控制台上組合。

Remediation.Recommendation.Text顯示於修補部分的查找詳細信息。它是超鏈接到Remediation.Recommendation.Url。

目前，只有來自 Security Hub 標準、IAM 訪問分析器和 Firewall Manager 的調查結果顯示指向有關如何修復查找結果的文檔的超鏈接。

SourceUrl

僅使用SourceUrl如果您可以為該特定查找結果提供一個深度鏈接的 URL 到您的控制台。否則，請從映射中省略它。

Security Hub 不支持來自此字段的超鏈接，但它在 Security Hub 控制台上顯示。

Malware, Network, Process, ThreatIntelIndicators

在適用的情況下，使用Malware、Network、Process, 或ThreatIntelIndicators。這些對象中的每個都在 Security Hub 控制台中公開。在發送的查找結果的上下文中使用這些對象。

例如，如果您檢測到與已知命令和控制節點建立出站連接的惡意軟件，請在Resource.Details.AwsEc2Instance。提供相關Malware、Network，以及ThreatIntelIndicator對象。

Malware

Malware是一個列表，最多可接受五個惡意軟件信息數組。使惡意軟件條目與資源和查找結果相關。

每個項目都有下列欄位。

Name

惡意軟體名稱。值為最多 64 個字元的字串。

Name應該來自經過審查的威脅情報或研究人員來源。

Path

惡意軟體路徑。值為最多 512 個字元的字串。Path應該是 Linux 或 Windows 系統文件路徑，以下情況除外。

- 如果您根據 YARA 規則掃描 S3 存儲桶或 EFS 共享中的對象，則Path是 S3://或 HTTPS 對象路徑。
- 如果您掃描 Git 存儲庫中的文件，則Path是 Git URL 或克隆路徑。

State

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

在查找標題和描述中，確保您提供了惡意軟件發生的情況的上下文。

例如，如果Malware.State是REMOVED，則查找結果標題和描述應反映您的產品已刪除路徑上的惡意軟件。

如果Malware.State是OBSERVED，則查找結果標題和描述應反映您的商品在路徑上遇到此惡意軟件。

Type

指示惡意軟體類型。允許的值為ADWARE|BLENDED_THREAT|BOTNET_AGENT|COIN_MINER|EXPLOIT_KIT|KEYLOGGER|MACRO|POTENT

如果你需要一個額外的值Type，請聯繫 Security Hub 團隊。

Network

Network是單一物件。您不能添加多個與網絡相關的詳細信息。在映射欄位時，請使用下列準則。

目的地和源信息

目標和源易於映射 TCP 或 VPC 流日誌或 WAF 日誌。他們是更難以使用，當你正在描述網絡信息的發現有關攻擊.

通常，來源是攻擊的起源地，但它可能具有下面列出的其他來源。您應該在文檔中解釋來源，並在查找標題和描述中對其進行描述。

- 對於 EC2 實例的 DDoS 攻擊，源是攻擊者，儘管真正的 DDoS 攻擊可能會使用數百萬台主機。目標位置為 EC2 實例的公有 IPv4 地址。`Direction`是在。
- 對於觀察到從 EC2 實例到已知命令和控制節點通信的惡意軟件，源是 EC2 實例的 IPV4 地址。目標是命令和控制節點。`Direction`是`OUT`。您還可以提供`Malware`和`ThreatIntelIndicators`。

`Protocol`

`Protocol`始終映射到互聯網號碼分配機構 (IANA) 註冊名稱，除非您可以提供特定的協議。您應始終使用它並提供端口信息。

`Protocol`獨立於源信息和目標信息。只有在有意義的情況下才提供它。

`Direction`

`Direction`始終相對於AWS網絡邊界。

- `IN`意味着它正在進入AWS（VPC、服務）。
- `OUT`意味着它正在退出AWS網絡邊界。

Process

`Process`是單一物件。您不能添加多個與進程相關的詳細信息。在映射欄位時，請使用下列準則。

`Name`

`Name`應該與可執行文件的名稱相匹配。它最多可接受 64 個字元。

`Path`

`Path`是進程可執行檔的文件系統路徑。它最多可接受 512 個字符。

`Pid`, **`ParentPid`**

`Pid`和`ParentPid`應該與 Linux 進程標識符 (PID) 或 Windows 事件 ID 匹配。若要區分開來，請使用 EC2 Amazon Machine Machine Image (AMI) 提供相關信息。客户可能會區分 Windows 和 Linux。

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

如果您無法可靠地檢索此信息，並且該信息不準確到毫秒，請不要提供它。

如果客户依賴時間戳進行取證調查，那麼沒有時間戳比使用錯誤的時間戳更好。

ThreatIntelIndicators

ThreatIntelIndicators接受最多五個威脅情報對象的陣列。

對於每個條目,Type是在具體威脅的背景下. 允許的值為DOMAIN|EMAIL_ADDRESS|HASH_MD5|HASH_SHA1|HASH_SHA256|HASH_SHA512|IPV4_ADDRESS|IPV6_A

下面是一些如何繪製威脅情報指標的示例：

- 你發現了一個你知道的過程與鈷罷工相關聯。你從FireEye的博客。

  將 Type 設為 PROCESS。同時創建Process對象。
- 您的郵件過濾器發現有人從已知惡意域發送一個眾所周知的哈希包。

  建立 2 個ThreatIntelIndicator物件。一個對象是DOMAIN。另一個用於HASH_SHA1。
- 你發現惡意軟件與亞拉規則（洛基，芬裏爾，AWS3VirusScan、BinaryAlert。

  建立 2 個ThreatIntelIndicator物件。一個是惡意軟件。另一個用於HASH_SHA1。

Resources

適用於Resources，請儘可能使用我們提供的資源類型和詳細信息字段。Security Hub 不斷向 ASFF 添加新資源。要接收 ASFF 更改的月度日誌，請聯繫<securityhub-partners@amazon.com>。

如果您無法適應模型化資源類型的詳細信息字段中的信息，請將剩餘詳細信息映射到Details.Other。

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

您也可以使用Other非資源類型AWS問題清單。

ProductFields

僅使用ProductFields如果您不能使用另一個策劃字段Resources或描述性對象，例如ThreatIntelIndicators、Network, 或Malware。

如果你確實使用ProductFields，您必須為此決定提供嚴格的理由。

合規

僅使用Compliance如果您的調查結果與合規性相關。

Security Hub 使用Compliance，瞭解它基於控件生成的調查結果。

Firewall Manager 使用Compliance，因為它們與遵守相關。

受限制的字段

這些字段旨在讓客户跟蹤他們對調查結果的調查。

請勿映射到這些字段或對象。

- Note
- UserDefinedFields
- VerificationState
- Workflow

對於這些字段，請映射到FindingProviderFields物件。請不要映射到頂層欄位。

- Confidence— 如果您的服務具有類似的功能，或者您的查找結果 100%，則僅包含置信度分數 (0-99)。
- Criticality— 重要度分數 (0-99) 用於表示與查找結果關聯的資源的重要性。
- RelatedFindings— 僅當您可以跟蹤與同一資源或查找類型相關的查找結果時才提供相關的查找結果。要標識相關查找結果，您必須參考已在 Security Hub 中的查找結果的查找標識符。

使用指導方針**BatchImportFindings**API

當您使用BatchImportFindingsAPI 操作將問題清單傳送到AWS Security Hub，請使用下列準則。

- 您必須調用BatchImportFindings使用與查找結果關聯的帳户。關聯帳户的標識符是AwsAccountId屬性來查找結果。
- 發送您可以的最大批次。Security Hub 每批最多可接受 100 個查找結果，每次查找最多可達 240 KB，每批最多可接受 6 MB 的查找結果。
- 節氣速率限制為每個區域每個賬户 10 TPS，突增 30 TPS。

- 如果存在限制或網絡問題，您必須實施一種機制來保留查找結果的狀態。您還需要查找狀態，以便您可以在查找結果進入和不合規時提交查找結果更新。
- 如需有關字串最大長度和其他限制的詳細資訊，請參見AWS安全問題清單格式 (ASFF)中的AWS Security Hub使用者指南。

產品準備情況清單

所以此AWS Security Hub和 APN 合作夥伴團隊使用此清單來驗證集成是否已準備好啟動。

ASFF 映射

這些問題與您的查找結果映射到AWS安全問題清單格式 (ASFF)。

合作夥伴的所有查找數據是否都映射到 ASFF 中？

以某種方式將您的所有調查結果映射到 ASFF。

使用精選字段，例如建模資源類型、Network、Malware, 或ThreatIntelIndicators。

將其他任何東西映射到Resource.Details.Other或者ProductFields視需要採取行動.

合作夥伴是否使用**Resource.Details**字段，例如**AwsEc2instance**、**AwsS3Bucket**，以及**Container**? 合作夥伴是否使用**Resource.Details.Other**來定義未在 ASFF 中建模的資源詳細信息？

請儘可能將提供的欄位用於您的調查結果中的 EC2 實例、S3 存儲桶和安全組等精選資源。

將與資源相關的其他信息映射到Resource.Details.Other只有在沒有直接匹配的情況下。

夥伴是否將值映射到**UserDefinedFields**?

請勿使用 UserDefinedFields。

考慮使用另一個策劃字段，例如Resource.Details.Other或者ProductFields。

合作夥伴是否將信息映射到**ProductFields**可以映射到其他 ASFF 字段中？

僅使用ProductFields，瞭解特定於產品的信息，例如版本控制信息、特定於產品的嚴重性查找結果或其他無法映射到精選字段的信息，或Resources.Details.Other。

合作夥伴是否導入自己的時間戳**FirstObservedAt**?

所以此FirstObservedAt時間戳用於記錄在產品中觀察到查找結果的時間。如果可能的話，映射此字段。

合作夥伴是否為每個查找標識符提供唯一值，但他們想要更新的查找結果除外？

Security Hub 中的所有查找結果都在查找標識符（Id屬性）。此值必須始終是唯一的，以確保不會意外更新查找結果。

您還應該維護查找結果標識符狀態，以便更新查找結果。

合作夥伴是否提供將查找結果映射到生成器 ID 的值？

GeneratorID不應該具有與查找 ID 相同的值。

GeneratorID應該能夠通過生成它們的內容邏輯鏈接發現。

這可以是產品中的子組件（產品 A-漏洞與產品 A-EDR）或類似的東西。

合作夥伴是否以與其產品相關的方式使用所需的查找類型命名空間？ 合作夥伴是否在其查找類型中使用推薦的查找類型類別或分類符？

查找結果類型分類應緊密映射到產品生成的結果。

第一級命名空間在AWS安全問題清單格式為必填項。

您可以將自定義值用於二級和三級命名空間（類別或分類符）。

合作夥伴是否捕獲網絡流信息**Network**字段，如果它們有網絡數據？

如果您的產品捕獲NetFlow信息，請將其映射到Network欄位。

夥伴捕獲進程 (PID) 信息是否在**Process**字段，如果它們有過程數據？

如果您的產品捕獲了流程信息，請將其映射到Process欄位。

合作夥伴是否捕獲**Malware**字段，如果它們有惡意軟件數據？

如果您的產品捕獲惡意軟件信息，請將其映射到Malware欄位。

合作夥伴是否捕獲威脅情報信息**ThreatIntelIndicators**字段，如果它們有威脅情報數據？

如果您的產品捕獲威脅情報信息，請將其映射到ThreatIntelIndicators欄位。

合作夥伴是否為調查結果提供信心評級？ 如果這樣做，是否提供了理由？

無論何時使用此字段，請在文檔和清單中提供理由。

合作夥伴是否使用規範 ID 或 ARN 作為查找結果中的資源 ID？

識別時AWS資源，最佳做法是使用 ARN。如果 ARN 不可用，請使用規範資源 ID。

集成設置和功能

這些問題與設置和day-to-day函數的集成。

合作夥伴是否提供infrastructure-as-code(iAC) 模板以部署與 Security Hub 的集成，例如 Terraform、AWS CloudFormation, 或AWS Cloud Development Kit (AWS CDK)?

對於將從客户帳户發送調查結果的集成或使用CloudWatch使用查找結果的事件，需要某種形式的 iAC 模板。

AWS CloudFormation是首選的，但AWS CDK也可以使用地形模型。

合作夥伴產品是否在控制台上進行一鍵式設置，以便與 Security Hub 集成？

某些合作夥伴產品在其產品中使用切換或類似機制來激活集成。這可能需要自動配置資源和權限。如果您從產品帳户發送查找結果，則首選方法是一鍵式設置。

合作夥伴是否只發送有價值的調查結果？

通常，您只應將具有安全價值的查找結果發送給 Security Hub 客户。

Security Hub 不是常規日誌管理工具。您不應將所有可能的日誌發送到 Security Hub。

合作夥伴是否對每位客户每天發送多少發現以及頻率（平均和突發頻率）提供了估計？

唯一查找結果的數量用於計算 Security Hub 上的負載。唯一查找結果定義為具有與其他查找結果不同的 ASFF 映射的查找結果。

例如，如果一個查找結果僅填充`ThreatIntelIndicators`和另一個僅填充`Resources.Details.AWSEc2Instance`，這些是兩個獨特的發現。

合作夥伴是否有處理 4xx 和 5xx 錯誤的優雅方式，以便它們不受限制，並且所有發現都可以在以後發送？

目前，在`BatchImportFindings`API 操作。如果返回 4xx 或 5xx 錯誤，則必須保留這些失敗的查找結果的狀態，以便以後可以全面重試它們。您可以通過死信隊列或其他AWS消息傳送服務，如 Amazon SNS 或 Amazon SQS。

合作夥伴是否維護其調查結果的狀態，以便他們知道存檔不再存在的調查結果？

如果計劃通過覆蓋原始查找結果 ID 來更新查找結果，則必須具有保留狀態的機制，以便更新正確的信息以獲得正確的查找結果。

如果您提供查找結果，請勿使用`BatchUpdateFindings`操作來更新查找結果。此操作應僅供客户使用。您只能使用`BatchUpdateFindings`當您調查問題並採取動作時。

合作夥伴是否以不影響先前發送的成功發現的方式處理重試？

您應該有一種機制來在出現錯誤的情況下保留原始查找 ID，以便您不會複製或覆蓋錯誤的成功查找結果。

合作夥伴是否通過調用**BatchImportFindings**操作與現有查找的查找 ID？

要更新查找結果，您必須通過提交相同的查找結果 ID 來覆蓋現有查找結果。

所以此BatchUpdateFindings操作應僅由客户使用。

合作夥伴是否使用**BatchUpdateFindings**API？

如果您對查找結果採取操作，則可以使用BatchUpdateFindings操作來更新特定字段。

合作夥伴是否提供有關創建查找結果和從其產品發送到 Security Hub 之間的延遲量的信息？

您應該最大限度地減少延遲，以確保客户能夠儘快在 Security Hub 中看到調查結果。

此信息在清單中是必需的。

如果合作夥伴的體繫結構要將調查結果從客户帳户發送到 Security Hub，他們是否成功證明瞭這一點？

如果合作夥伴的體繫結構要從他們自己的帳户向 Security Hub 發送調查結果，他們是否成功證明瞭這一點？

在測試過程中，必須從您擁有的帳户中成功發送查找結果，該帳户與為產品 ARN 提供的帳户不同。

從產品 ARN 所有者的帳户發送查找結果可以繞過 API 操作中的某些錯誤異常。

合作夥伴是否向 Security Hub 提供檢測信號查找？

要顯示您的集成工作正常，您應該發送檢測信號查找。檢測信號查找每五分鐘發送一次，並使用查找類型`Heartbeat`。

如果您從產品帳户發送調查結果，這一點非常重要。

在測試過程中，合作夥伴是否與 Security Hub 產品團隊的帳户集成？

在生產前驗證期間，您應將查找示例發送到 Security Hub 產品團隊AWS帳户。這些示例表明發現的發送和映射正確。

文件

這些問題與您提供的集成文檔有關。

合作夥伴是否將其文檔託管在專用網站上？

文檔應作為靜態網頁、Wiki、閱讀文檔或其他專用格式託管在您的網站上。

託管文檔GitHub不符合專用網站要求。

合作夥伴文檔是否提供了有關如何設定 Security Hub 集成的說明？

您可以使用 iAC 模板或基於控制台的「一鍵式」集成來設置集成。

合作夥伴文檔是否提供了對其使用案例的描述？

您在清單中提供的用例也應在

合作夥伴文檔是否為他們發送的調查結果提供了理由？

您應該為您發送的查找結果類型提供理由。

例如，您的產品可能會對漏洞、惡意軟件和防病毒產生查找結果，但您只會向 Security Hub 發送漏洞和惡意軟件查找結果。在這種情況下，您必須提供不發送防病毒查找結果的理由。

合作夥伴文檔是否為合作夥伴如何將其調查結果映射到 ASFF 提供了理由？

您應該提供將產品的本機查找結果映射到 ASFF 的理由。買家想知道在哪裏查找特定商品信息。

合作夥伴文檔是否提供有關合作夥伴如何更新結果的指導，如果他們更新調查結果？

向客户提供有關如何保留狀態、確保冪等信息，並使用up-to-date資訊。

合作夥伴文檔是否描述瞭如何查找延遲？

最大限度地減少延遲，以確保客户在 Security Hub 中儘快看到調查結果。

此信息在清單中是必需的。

合作夥伴文檔是否描述了其嚴重性評分如何與 ASFF 嚴重性評分對應？

提供有關如何映射`Severity.Original`至`Severity.Label`。

例如，如果嚴重性值是字母等級（A、B、C），則應提供有關如何將字母等級映射到嚴重性標籤的信息。

合作夥伴文檔是否提供信心評級的理由？

如果您提供置信度分數，則應對這些分數進行排名。

如果使用靜態填充置信度分數或衍生於人工智能或機器學習的映射，則應提供其他上下文。

合作夥伴文檔是否註明合作夥伴支持和不支持哪些地區？

注意支持或不受支持的區域，以便客户知道在哪些地區不嘗試集成。

產品卡資訊

這些問題與顯示在整合頁面上的 Security Hub 控制台。

是否提供AWS賬户 ID 有效且包含 12 位數字？

賬户標識符長度為 12 位數字。如果賬户 ID 包含少於 12 位數字，則產品 ARN 將無效。

商品描述是否包含 200 個或更少的字符？

清單中 JSON 中提供的商品描述不應超過 200 個字符（包括空格）。

配置鏈接是否導致集成文檔？

配置鏈接應導向您的聯機文檔。它不應該導致您的主網站或營銷頁面。

購買鏈接（如果提供）是否導致AWS Marketplace商品的商品信息？

如果您提供購買鏈接，則該鏈接必須是AWS Marketplace項目。Security Hub 不接受不由AWS。

商品類別是否正確描述了商品？

在清單中，您最多可以提供三個商品類別。這些應該與 JSON 匹配，並且不能自定義。您提供的商品類別不能超過三個。

公司名稱和產品名稱是否有效和正確？

公司名稱必須為 16 個或更少的字符。

商品名稱必須少於 24 個字符。

產品卡 JSON 中的商品名稱必須與清單中的名稱匹配。

行銷資訊

這些問題與集成的營銷有關。

Security Hub 合作夥伴頁面的產品描述是否在 700 個字符內（包括空格）以內？

「Security Hub 合作夥伴」頁面僅接受最多 700 個字符（包括空格）。

團隊將編輯更長的描述。

Security Hub 合作夥伴頁面徽標是否大於 600 x 300 像素？

提供一個公開訪問的 URL，其中包含 PNG 或 JPG 的公司徽標，該網址不超過 600 x 300 像素。

Security Hub 合作夥伴頁面上的瞭解更多超鏈接是否會導致合作夥伴關於集成的專用網頁？

所以此進一步了解鏈接不應導致合作夥伴的主要網站或文檔信息。

此鏈接應始終轉到一個專門的網頁，其中包含有關集成的營銷信息。

合作夥伴是否提供演示或教學視頻瞭解如何使用他們的集成？

演示或集成演練視頻為選用操作，但建議您採用。

是一個AWS合作夥伴網絡博客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合作夥伴網絡博客文章應提前與合作夥伴開發經理或合作夥伴發展代表協調。

這些文章與您自己創建的任何博客文章分開。

允許 4 至 6 周的交貨時間。這項工作應在使用專用產品 ARN 測試完成後開始。

是否正在發佈合作夥伴主導的新聞稿？

您可以與合作夥伴開發經理或合作夥伴開發代表合作，獲取外部安全服務副總裁的報價。您可以在新聞稿中使用此報價。

是否正在發佈合作夥伴主導的博客文章？

您可以創建自己的博客文章，以展示AWS合作夥伴網絡博客。

是否正在發佈合作夥伴主導的網絡研討會？

您可以建立自己的網絡研討會以展示整合。

如果您需要 Security Hub 團隊的幫助，請在使用專用產品 ARN 完成測試後與產品團隊合作。

合作夥伴是否請求社交媒體支持AWS?

在您的版本後，您可以使用AWS安全營銷導致使用AWS官方社交媒體渠道，分享有關您的網絡研討會的詳細信息。

AWS Security Hub合作夥伴常見

以下是有關設置和維護與AWS Security Hub。

1. Security Hub 整合有哪些優點？
   - 顧客滿意度— 與 Security Hub 集成的首要原因是您有客户要求這樣做。

     Security Hub 是AWS客户。它被設計為第一站，其中AWS安全性和法規遵從性專業人員每天都會瞭解他們的安全性和合規性狀態。

     傾聽客户的意見。他們會告訴您他們是否希望在 Security Hub 查看您的發現。
   - 探索機會— 我們在 Security Hub 控制台中推廣具有認證集成的合作夥伴，包括指向其AWS Marketplace清單。這是客户發現新安全產品的好方法。
   - 市場推廣機會— 具有批準集成的供應商可以參加網絡研討會，發佈新聞稿，創建光滑的表格，並演示他們與AWS客户。
2. 有哪些類型的合作夥伴？
   - 將問題清單傳送到 Security Hub
   - 接收 Security Hub 問題清單的合作夥伴
   - 發送和接收調查結果的合作夥伴
   - 幫助客户在其環境中設置、自定義和使用 Security Hub 的諮詢合作夥伴
3. 合作夥伴與 Security Hub 的集成如何在高級別工作？

   您可以從客户帳户或自己的帳户中收集調查結果AWS帳户，並將調查結果的格式轉換為AWS安全問題清單格式 (ASFF)。然後，您將這些查找結果推送到相應的 Security Hub 區域終端節點。

   您也可以使用CloudWatch從 Security Hub 接收問題清單的事件。
4. 完成與 Security Hub 集成的基本步驟是什麼？
   a. 提交合作夥伴清單資訊。
   b. 如果要將查找結果發送到 Security Hub，則接收要與 Security Hub 一起使用的產品 ARN。
   c. 將您的調查結果映射到 ASFF。請參閱the section called “ASFF 映射指導方針”。
   d. 定義您的體繫結構，以便向 Security Hub 發送查找結果並從安全中心接收 遵循the section called “創建和更新調查結果的原則”。
   e. 為客户創建部署框架。例如：AWS CloudFormation腳本可以達到這個目的。
   f. 記錄您的設置併為客户提供配置説明。

g. 定義客戶可用於您的產品的任何自定義見解（關聯規則）。

h. 向 Security Hub 團隊演示您的集成。

i. 提交營銷信息以供批準（網站語言、新聞稿、體繫結構幻燈片、視頻、光滑表格）。

5. 提交合作夥伴清單的流程是什麼？ 而對於AWS服務將問題清單傳送到 Security Hub？

   要將清單信息提交給 Security Hub 團隊，請使用<securityhub-partners@amazon.com>。

   您將在七個日歷日內獲得產品 ARN 頒發。

6. 我應該向 Security Hub 發送哪些類型的調查結果？

   Security Hub 定價部分取決於攝入的問題清單數目。因此，您應避免發送無法為客户提供價值的調查結果。

   例如，某些漏洞管理供應商僅發送通用漏洞評分系統 (CVSS) 評分為 3 或以上的可能 10 分的調查結果。

7. 如何將問題清單傳送到 Security Hub，有哪些不同的方法？

   以下是主要方法：

   - 您可以從他們自己指定的AWS帳户使用BatchImportFindingsoperation.
   - 您可以從客户帳户中使用BatchImportFindingsoperation. 您可以使用保證角色方法，但這些方法不是必需的。

   有關使用BatchImportFindings，請參the section called “使用指導方針BatchImportFindingsAPI”。

8. 如何收集我的發現並將其推送到 Security Hub 區域終端節點？

   合作夥伴對此採用了不同的方法，因為它高度依賴於您的解決方案的體繫結構。

   例如，一些合作夥伴構建了一個 Python 應用程序，該應用程序可以部署為AWS CloudFormation指令碼。該腳本從客户環境中收集合作夥伴的調查結果，將其轉換為 ASFF，並將其發送到 Security Hub 區域終端節點。

   其他合作夥伴構建了一個完整的嚮導，為客户提供一次單擊體驗，將調查結果推送到 Security Hub。

9. 如何知道何時開始向 Security Hub 發送問題清單？

   Security Hub 支持部分批處理授權BatchImportFindingsAPI 操作，以便您可以將所有發現發現發送到所有客户的 Security Hub。

如果您的某些客户尚未訂閱 Security Hub，則 Security Hub 不會收集這些調查結果。它僅接收批處理中的授權查找結果。

10.我需要完成哪些步驟才能將調查結果發送到客户的 Security Hub 實例？

a. 確保採用正確的 IAM 策略。

b. 為帳户啟用產品訂閱（資源策略）。使用EnableImportFindingsForProductAPI 操作或整合(憑證已建立！) 頁面上的名稱有些許差異。客户可以執行此操作，也可以使用跨賬户角色代表客户行事。

c. 確保ProductArn是您產品的公共 ARN。

d. 確保AwsAccountId是客户的賬户 ID。

e. 確保您的調查結果沒有任何格式錯誤的數據根據AWS安全問題清單格式 (ASFF)。例如，填充必填字段，並且沒有無效值。

f. 將查找結果批量發送到正確的區域終端節點。

11.我必須具備哪些 IAM 權限才能發送調查結果？

必須為調用BatchImportFindings或其他 API 調用。

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

可以使用 IAM 策略配置同一賬户中的資源，而無需資源策略。

要排除來自BatchImportFindings中，設置呼叫者的 IAM 策略，如下所示：

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

請務必檢查是否沒有Deny策略。使用該策略後，您可以將策略限製為以下內容：

```
{
    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？

要接收來自特定合作夥伴產品的調查結果，客戶（或具有代表客戶工作的跨賬戶角色的合作夥伴）必須建立產品訂閱。若要從主控台執行此操作，他們使用整合(憑證已建立！) 頁面上的名稱有些許差異。要從 API 執行此操作，他們使用EnableImportFindingsForProductAPI 操作。

產品訂閱創建一個資源策略，授權客戶接收或發送來自合作夥伴的查找結果。如需詳細資訊，請參閱 使用案例及許可。

Security Hub 具有適用於合作夥伴的以下類型的資源策略：

- BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT
- BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT

在合作夥伴入職過程中，您可以請求一種或兩種類型的策略。

搭配BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT，您只能從產品 ARN 中列出的帳戶將查找結果發送到 Security Hub。

搭配BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT，您只能從訂閱您的客戶帳戶發送調查結果。

13.假設客戶創建了一個管理員帳戶並添加了幾個成員帳戶。客戶是否需要為我訂閱每個會員帳戶？ 或者客戶是否只從管理員帳戶訂閱，然後我可以針對所有成員帳戶中的資源發送調查結果？

此問題詢問是否基於管理員帳戶註冊為所有成員帳戶創建權限。

客戶必須為每個帳戶提供產品訂閱。他們可以通過 API 以編程方式執行此操作。

14.什麼是我的產品 ARN？

您的產品 ARN 是 Security Hub 為您生成並用於提交調查結果的唯一標識符。您會收到與 Security Hub 集成的每個產品的產品 ARN。正確的產品 ARN 必須是您發送到 Security Hub 的每個查找結果的一部分。沒有產品 ARN 的調查結果將被刪除。產品 ARN 採用下列格式：

`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`

每個部署 Security Hub 的區域都會為您提供一個產品 ARN。賬戶 ID、公司和產品名稱由您的合作夥伴清單提交決定。除區域代碼外，您絕不會更改與產品 ARN 關聯的任何信息。區域代碼必須與您為其提交調查結果的地區匹配。

一個常見的錯誤是更改賬戶 ID 以匹配您當前使用的賬戶。賬戶 ID 不會更改。作為提交清單的一部分，您提交「家庭」賬戶 ID。此帳戶 ID 已鎖定到您的產品 ARN 中。

當 Security Hub 在新區域啟動時，它會自動使用標準區域代碼為這些區域生成產品 ARN。

每個帳戶還會自動配置一個私有產品 ARN。在收到官方公共產品 ARN 之前，您可以使用此 ARN 在您自己的開發帳戶中測試導入結果。

15.應使用何種格式將問題清單傳送到 Security Hub？

問題清單必須在AWS安全問題清單格式 (ASFF)。如需詳細資訊，請參閱AWS安全問題清單格式 (ASFF)中的AWS Security Hub使用者指南。

預期您的本機調查結果中的所有信息都完全反映在 ASFF 中。自訂欄位，例如`ProductFields`和`Resource.Details.Other`允許您映射不適合預定義字段的數據。

16.要使用的區域終端節點是什麼？

您必須將查找結果發送到與客戶帳戶關聯的 Security Hub 區域終端節點。

17.哪裏可以找到區域終端清單？

請參Security Hub 終端列表。

18.我可以提交跨區域的調查結果嗎？

Security Hub 尚不支持跨區域提交本機AWS服務，例如亞馬遜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地區的調查結果。

在這個意義上，您可以從任何位置調用區域終端節點，並且 ASFF 的資源信息不必與終端節點的區域匹配。但是,`ProductArn`必須與終端節點的區域匹配。

19.發送批量調查結果的規則和準則是什麼？

您可以批處理多達 100 個發現或 240 KB 的單個調用BatchImportFindings。排隊並批處理儘可能多的查找結果，直到此限制。

您可以批處理來自不同帳户的一組查找結果。但是，如果批處理中的任何帳户未訂閱 Security Hub，則整個批處理將失敗。這是 API Gateway 基準授權模型的限制。

請參閱the section called “使用指導方針BatchImportFindingsAPI”。

20.我可以向創建的調查結果發送更新嗎？

是的，如果您使用相同的產品 ARN 和相同的查找結果 ID 提交查找結果，它會覆蓋該查找結果的先前數據。請注意，所有數據都被覆蓋，因此您應提交完整的查找結果。

根據新的調查結果和查找更新對客户進行計費和計費。

21.我可以向其他人創建的調查結果發送更新嗎？

是的，如果客户授予您訪問BatchUpdateFindingsAPI 操作，您可以使用該操作更新某些字段。此操作旨在供客户、SIEMS、票證系統和安協調、自動化和響應 (SOAR) 平台使用。

22.調查結果如何老化？

Security Hub 會在上次更新日期後 90 天過期。在此時間之後，將從 Security Hub 清除老化的查找結果OpenSearch叢集。

如果您更新具有相同查找 ID 的查找結果，並且該查找結果已過期，則會在 Security Hub 中創建一個新的查找結果。

客户可以使用CloudWatch將查找結果移出 Security Hub 的事件。這樣做可以將所有調查結果發送到客户選擇的目標。

通常，Security Hub 建議您每 90 天創建一次新的查找結果，並且不要永遠更新查找結果。

23.Security Hub 設置了哪些限制？

Security Hub 節流GetFindingsAPI 調用，因為建議的訪問查找結果的方法是使用CloudWatch事件

除了 API Gateway 和 Lambda 調用強制實施的限制之外，Security Hub 不會對內部服務、合作夥伴或客户實施任何其他限制。

24.從源服務發送到 Security Hub 的調查結果的及時性或延遲 SLA 或期望是多少？

目的是儘可能接近實時地提供初步調查結果和調查結果的最新情況。您應在創建查找結果後五分鐘內將其發送到 Security Hub。

25如何接收 Security Hub 的問題清單？

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發送到CloudWatch事件 客户可以創建特定的CloudWatch將查找結果發送到特定目標（如 SIEM 或 S3 存儲桶）的事件規則。此功能取代了舊版`GetFindings`API 操作。
- 使用CloudWatch自訂動作的事件。Security Hub 允許客户從控制台中選擇特定的查找結果或查找結果組，並對其採取措施。例如，他們可以將查找結果發送到 SIEM、票證系統、聊天平台或修正工作流。這將是客户在 Security Hub 內執行的警報分類工作流的一部分。這些都稱為自訂動作。

  當用户選擇自定義操作時，CloudWatch事件為這些特定的查找結果創建。您可以利用此功能並構建CloudWatch事件規則和目標，供客户用作自定義操作的一部分。請注意，此功能不用於自動將特定類型或類的所有查找結果發送到CloudWatch事件 用户可以對特定的調查結果採取行動。

  您可以使用自定義操作 API 操作，例如`CreateActionTarget`，為您的商品自動創建可用操作（例如使用AWS CloudFormation）。您還可以使用CloudWatch事件規則 API 操作來創建相應的CloudWatch與自定義操作關聯的事件規則。使用AWS CloudFormation模板，您還可以創建CloudWatch事件規則自動從 Security Hub 接收具有特定特徵的所有查找結果或所有查找結果。

26託管安全服務提供商 (MSSP) 成為 Security Hub 合作夥伴的要求是什麼？

您必須演示如何將 Security Hub 用作向客户提供服務的一部分。

您應該有解釋您使用 Security Hub 的用户文檔。

如果 MSSP 是查找提供程序，他們必須演示將查找結果發送到 Security Hub。

如果 MSSP 只接收來自 Security Hub 的查找結果，他們必須至少具有AWS CloudFormation模板設定適當的CloudWatch事件規則。

27非 MSSP APN 諮詢合作夥伴成為 Security Hub 合作夥伴的要求是什麼？

如果您是 APN 諮詢合作夥伴，您可以成為 Security Hub 合作夥伴。您應提交兩個私人案例研究，說明您如何幫助特定客户完成以下操作。

- 使用客户所需的 IAM 權限設置 Security Hub。
- 使用控制台中合作夥伴頁面上的配置説明，幫助將已集成的獨立軟件供應商 (ISV) 解決方案連接到 Security Hub。
- 幫助客户進行定製產品集成。

- 構建與客戶需求和數據集相關的自定義見解。
- 構建自定義操作。
- 構建補救行動手冊。
- 構建符合 Security Hub 合規性標準的快速入門。這些必須由 Security Hub 團隊驗證。

案例研究不需要公開分享。

28.如何與客戶部署與 Security Hub 的集成有哪些要求？

Security Hub 和合作夥伴產品之間的集成體繫結構因合作夥伴解決方案的運營方式而異。您應確保集成的設置過程不超過 15 分鐘。

如果要將集成軟件部署到客戶的AWS環境中，您應該利用AWS CloudFormation模板來簡化集成。一些合作夥伴已經創建了一鍵式集成，我們非常鼓勵這樣做。

29.我的文檔要求是什麼？

您必須提供一個指向描述產品與 Security Hub 之間的集成和設置過程的文檔鏈接，包括您使用AWS CloudFormationTemplate。

該文檔還應包括有關您使用 ASFF 的信息。具體而言，這應該列出您用於不同查找結果的 ASFF 查找類型。如果您有任何默認的智能分析定義，我們建議您也在此處包含它們。

考慮包括其他潛在信息：

- 與 Security Hub 集成的使用案例
- 發送的調查結果的平均數量
- 您的整合架構
- 您支持和不支持的區域
- 查找結果創建與發送到 Security Hub 之間的延遲
- 是否更新查找結果

30.什麼是自定義見解？

我們鼓勵您為調查結果定義自定義見解。見解是輕量級關聯規則，可幫助客戶優先考慮哪些調查結果和資源最需要注意和採取行動。

Security Hub 具有`CreateInsight`API 操作。您可以在客戶帳戶中創建自定義見解，作為AWS CloudFormationTemplate。這些見解顯示在客戶控制台上。

31.我可以提交儀錶板小部件嗎？

不，這個時候不行 您只能創建受管洞見。

32.您的定價模式是什麼？

請參Security Hub 價格信息。

33.如何將調查結果提交到 Security Hub 模擬賬户，作為我集成的最終審批流程的一部分？

使用您提供的產品 ARN 將調查結果發送到 Security Hub 模擬賬户，使用us-west-2作為區域. 調查結果應包含模擬賬號在AwsAccountId領域。要獲取模擬賬號，請聯繫 Security Hub 團隊。

請勿向我們發送任何敏感數據或個人身份信息。此數據用於公共演示。當您向我們發送此數據時，您授權我們在演示中使用這些數據。

34.什麼錯誤或成功消息**BatchImportFindings**提供？

Security Hub 提供授權響應和響應BatchImportFindings。更清晰的成功、失敗和錯誤消息正在開發中。

35.源服務負責哪些錯誤處理？

源服務負責所有錯誤處理。他們必須處理錯誤消息、重試、限制和警報。他們還必須處理通過 Security Hub 反饋機制發送的反饋或錯誤消息。

36.常見問題有哪些解決方案？

同時AuthorizerConfigurationException是由格式錯誤導致的AwsAccountId或者ProductArn。

故障排除時，請注意下列事項：

- AwsAccountId必須準確為 12 位數字。
- ProductArn必須採用下列格式：arn: AW: Security Hub:*<us-west-2 or us-east-1>*：*<accountId>*：Products*<company-id>*/*<product-id>*

  帳户 ID 與 Security Hub 團隊提供給您的產品 ARN 中包含的帳户 ID 不會更改。

AccessDeniedException是在發送到錯誤帳户或從錯誤帳户發送查找結果時引起的，或者當該帳户沒有ProductSubscription。錯誤消息將包含一個 ARN，其資源類型為product或者product-subscription。此錯誤僅在跨賬户調用期間發生。如果您調用BatchImportFindings使用您自己的帳户為同一帳户AwsAccountId和ProductArn，操作使用 IAM 策略，與無關ProductSubscriptions。

請確保您使用的客戶帳戶和產品帳戶是實際註冊帳戶。某些合作夥伴使用了產品 ARN 中產品的帳號，但嘗試使用完全不同的帳戶來調用BatchImportFindings。在其他情況下，他們創建ProductSubscriptions用於其他客戶帳戶，甚至為他們自己的產品帳戶。他們沒有創建ProductSubscriptions用於他們嘗試導入問題清單的客戶帳戶。

37.我在哪裏發送問題、評論和錯誤？

<securityhub-partners@amazon.com>

38.我要向哪個地區發送與全局相關的項目的調查結果AWS服務？ 例如，我應在哪裏發送與 IAM 相關的調查結果？

將查找結果發送到檢測到查找結果的同一區域。對於 IAM 等服務，您的解決方案可能會在多個地區發現相同的 IAM 問題。在這種情況下，查找結果被發送到檢測到問題的每個區域。

如果客戶在三個區域運行 Security Hub，並且在所有三個區域都檢測到相同的 IAM 問題，則將查找結果發送到所有三個區域。

問題解決後，將更新發送到查找結果到您發送原始查找結果的所有區域。

合作夥伴整合指南的文件歷史紀錄

下表說明此指南的說明文件。

變更	描述	日期
主機標誌的更新需求	已更新合作夥伴資訊清單和標誌準則，指出合作夥伴必須同時提供標誌的淺色模式和深色模式版本，才能在 Security Hub 主控台上顯示。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AWSISV 合作夥伴路徑，以及使用已完成AWS基礎技術審查（FTR）。過去，所有整合合作夥伴都必須AWS選取等級合作夥伴。	2021 年 4 月 29 日
全新FindingProviderFields ASFF 中的物件	已更新將發現項目對應至 ASFF 的資訊。對於Confidence 、Criticality 、RelatedFindings 、Severity，以及Types，合作夥伴將其值映射到中的字段FindingProviderFields 。	2021 年 3 月 18 日
建立和更新發現項目的新原則	已新增一組新的準則，以便在 Security Hub 中建立新的發現項目，以及更新現有發現項目。	2020 年 12 月 4 日
本指南的初始版本	這合作夥伴整合指南提供AWS提供有關如何與之建立整合的	2020 年 6 月 23 日

資訊的合作夥伴AWS Security Hub。

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。