aws

合作伙伴集成指南

AWS Security Hub

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Security Hub: 合作伙伴集成指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

第三方集成概述 AWS Security Hub 1
为什么要集成？ 1
准备发送调查发现 2
准备接收调查发现 2
Security Hub 信息资源 3
成为合作伙伴的前提条件 4
使用场景和权限 5
合作伙伴托管：从合作伙伴账户发送的调查发现 5
合作伙伴托管：从客户账户发送的调查发现 6
客户托管：从客户账户发送的调查发现 7
合作伙伴入驻流程 9
Go-to-market 活动 11
Security Hub 合作伙伴页面上的条目 11
新闻稿 11
AWS 合作伙伴网络 (APN) 博客 12
关于 APN 博客的重要信息 12
为什么要为 APN 博客撰稿？ 12
哪些类型的内容最适合 APN 博客？ 13
宣传单 13
白皮书或电子书 13
网络研讨会 13
演示视频 13
产品集成清单 14
使用案例和营销信息 15
寻找提供商和消费者使用案例 15
咨询合作伙伴（CP）使用案例 15
数据集 16
架构 16
配置 16
每位客户每天的平均调查发现数量 17
延迟 17
公司和产品描述 17
合作伙伴网站资产 17
合作伙伴徽标页面 18

Security Hub 的控制台徽标 18
调查发现类型 18
热线 19
心跳调查发现 19
Security Hub 控制台信息 19
公司信息 19
产品信息 20
准则和核对清单 30
控制台徽标准则 30
创建和更新调查发现的原则 33
ASFF 映射准则 34
识别信息 34
Title 以及 Description 34
调查发现类型 35
时间戳 35
Severity 35
Remediation 36
SourceUrl 36
Malware, Network, Process, ThreatIntelIndicators 36
Resources 39
ProductFields 40
合规 40
受限字段 40
BatchImportFindings API 的使用准则 40
产品准备清单 41
ASFF 映射 41
集成设置和功能 43
文档 45
产品卡片信息 46
营销信息 47
合作伙伴常见问题 49
文档历史记录 59
..... lxi

第三方集成概述 AWS Security Hub

本指南适用于想要与 AWS Security Hub之集成的 AWS 合作伙伴网络 (APN) 合作伙伴。

作为 APN 合作伙伴，您可通过以下一种或多种方式与 Security Hub 集成。

- 向 Security Hub 发送调查发现
- 使用来自 Security Hub 的调查发现
- 以上两者兼而有之
- 使用 Security Hub 作为托管安全服务提供商（MSSP）产品的中心
- 向 AWS 客户咨询如何部署和使用 Security Hub

本入门指南主要关注向 Security Hub 发送调查发现的合作伙伴。

主题

- 为什么要与 AWS Security Hub？
- 正在准备将调查结果发送至 AWS Security Hub
- 准备接收来自的调查结果 AWS Security Hub
- 用于学习的资源 AWS Security Hub

为什么要与 AWS Security Hub？

AWS Security Hub 提供所有 Security Hub 帐户的高优先级安全警报和安全状态的全面视图。Security Hub 允许像您这样的合作伙伴向 Security Hub 发送安全调查发现，让您的客户深入了解您生成的安全调查发现。

与 Security Hub 的集成可以通过以下方式实现增值。

- 满足您客户对 Security Hub 集成的需求
- 为您的客户提供与 AWS 安全相关的调查结果的单一视图
- 让新客户在寻找合作伙伴以获取与特定安全事件类型相关的调查发现时，发现您的解决方案

在与 Security Hub 建立集成之前，请仔细审查您的集成原因。如果您的客户希望您的产品与 Security Hub 集成，则集成的成功可能性更大。您可以纯粹出于营销或获取新客户的目的来建立集成。但是，

如果您建立集成时没有听取任何当前客户的意见，并且没有考虑您客户的需求，则集成可能无法产生预期的结果。

正在准备将调查结果发送至 AWS Security Hub

作为 APN 合作伙伴，在 Security Hub 团队允许您成为调查发现提供商之前，您无法为您的客户向 Security Hub 发送信息。要成为调查发现提供商，您必须完成以下入驻步骤。完成这些步骤可确保您和您的客户获得积极的 Security Hub 体验。

完成入驻步骤后，您务必遵守the section called “创建和更新调查发现的原则”、the section called “ASFF 映射准则” 和 the section called “`BatchImportFindings` API 的使用准则” 中的准则。

1. 将您的安全调查结果映射到 AWS 安全调查结果格式 (ASFF)。
2. 构建您的集成架构，以将调查发现推送到正确的 Security Hub 区域端点。为此，您需要定义是从自己的 AWS 账户还是从客户的账户中发送调查结果。
3. 让您客户用自己的账户订阅您的产品。为此，他们可以使用控制台或 `EnableImportFindingsForProduct` API 操作。请参阅《AWS Security Hub 用户指南》中的管理产品集成。

   您也可以为他们订阅产品。为此，您可以使用跨账户角色来代表客户访问 `EnableImportFindingsForProduct` API 操作。

   此步骤制定了接受该产品为该账户提供调查发现所需的资源策略。

以下博文讨论了合作伙伴与 Security Hub 的一些现有集成。

- 宣布与云托管人集成 AWS Security Hub
- 使用 AWS Fargate 和 Prowler 将有关 AWS 服务的安全配置结果发送到 Security Hub
- 如何将 AWS Config 规则评估作为调查发现导入 Security Hub

准备接收来自的调查结果 AWS Security Hub

要接收来自的调查结果 AWS Security Hub，请使用以下选项之一：

- 让您的客户自动将所有调查结果发送到 CloudWatch 活动。客户可以创建特定的 CloudWatch 事件规则，将调查结果发送到特定目标，例如 SIEM 或 S3 存储桶。
- 让您的客户在 Security Hub 控制台选择特定的调查发现或调查发现组，然后对其采取行动。

例如，您的客户可将调查发现发送到 SIEM、票务系统、聊天平台或修复工作流程。这将是客户在 Security Hub 中执行的警报分类工作流程的一部分。

这些操作称为自定义操作。当用户执行自定义操作时，会针对这些特定发现创建一个 CloudWatch 事件。作为合作伙伴，您可以利用此功能制定 CloudWatch 事件规则或目标，供客户在自定义操作中使用。请注意，此功能不会自动将特定类型或类别的所有发现结果发送到 Ev CloudWatch ents。此功能供用户对特定调查发现采取行动。

以下博客文章概述了使用与 Security Hub 和 Ev CloudWatch ents 的集成进行自定义操作的解决方案。

- 如何将 AWS Security Hub 自定义操作与 PagerDuty
- 如何在中启用自定义操作 AWS Security Hub
- 如何将 AWS Config 规则评估作为调查发现导入 Security Hub

用于学习的资源 AWS Security Hub

以下材料可以帮助您更好地了解 AWS Security Hub 解决方案以及 AWS 客户如何使用该服务。

- 介绍 AWS Security Hub 视频
- 《Security Hub 用户指南》
- “Security Hub API 参考”
- 入驻网络研讨会

我们还鼓励您在其中一个 AWS 账户中启用 Security Hub，并亲身体验该服务。

成为合作伙伴的前提条件

在开始与集成之前 AWS Security Hub，您必须满足以下条件之一：

- 您是 AWS 精选等级合作伙伴或更高级别的合作伙伴。
- 您已加入 AWS ISV 合作伙伴路径，并且用于 Security Hub 集成的产品已完成 AWS 基础技术审核（FTR）。然后，该产品将获得 “已审阅 AWS” 徽章。

您还必须与 AWS之签订相互保密协议。

集成使用案例和所需权限

AWS Security Hub 允许 AWS 客户接收来自 APN 合作伙伴的调查结果。合作伙伴的产品可能在客户的 AWS 账户内部或外部运行。客户账户中的权限配置因合作伙伴产品使用的模型而异。

在 Security Hub 中，客户始终有权控制哪些合作伙伴可向客户账户发送调查发现。客户可随时取消合作伙伴的权限。

为了使合作伙伴能够向其账户发送安全调查发现，客户首先应在 Security Hub 中订阅合作伙伴产品。以下概述的所有使用案例，都必须执行订阅步骤。有关客户如何管理产品集成的详细信息，请参阅《AWS Security Hub 用户指南》中的管理产品集成。

客户订阅合作伙伴产品后，Security Hub 会自动创建托管资源策略。该策略授予合作伙伴产品权限，允许其使用 `BatchImportFindings` API 操作向客户账户的 Security Hub 发送调查发现。

以下是合作伙伴产品与 Security Hub 集成的常见案例。这些信息包括各个使用案例所需的附加权限。

合作伙伴托管：从合作伙伴账户发送的调查发现

此用例涵盖使用自己的 AWS 账户托管产品的合作伙伴。要向 AWS 客户发送安全调查结果，合作伙伴需要从合作伙伴产品账户调用 `BatchImportFindings`API 操作。

在此使用案例中，客户账户只需要客户订阅合作伙伴产品时建立的权限。

在合作伙伴账户中，调用 `BatchImportFindings` API 操作的 IAM 主体必须具有允许主体调用 `BatchImportFindings` 的 IAM policy。

让合作伙伴产品能够在 Security Hub 中向客户发送调查发现需要两个步骤：

1. 客户在 Security Hub 中创建对合作伙伴产品的订阅。
2. 经客户确认，Security Hub 会生成正确的托管资源策略。

要发送与客户账户相关的安全调查发现，合作伙伴产品需使用自己的凭证调用 `BatchImportFindings` API 操作。

以下是 IAM policy 向合作伙伴账户中的主体授予 Security Hub 必要权限的示例。

```
{
```

```
    "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"
        }
    ]
}
```

合作伙伴托管：从客户账户发送的调查发现

此用例涵盖使用自己的 AWS 账户托管产品，但使用跨账户角色访问客户账户的合作伙伴。他们从客户账户调用 `BatchImportFindings` API 操作。

在此使用案例中，如要调用 `BatchImportFindings` API 操作，合作伙伴账户需要在客户账户中担任客户托管 IAM 角色。

此调用从客户账户发起。因此，托管资源策略必须允许在调用中使用合作伙伴产品账户的产品 ARN。Security Hub 托管资源策略为合作伙伴产品账户和合作伙伴产品 ARN 授予权限。产品 ARN 是合作伙伴作为提供商的唯一标识符。由于调用不是来自合作伙伴产品账户，因此客户必须明确授予合作伙伴产品向 Security Hub 发送调查发现的权限。

在合作伙伴账户和客户账户之间扮演跨账户角色的最佳做法是使用合作伙伴提供的外部标识符。此外部标识符是客户账户中跨账户策略定义的一部分。合作伙伴在担任角色时必须提供标识符。在向合作伙伴授予 AWS 账户访问权限时，外部标识符可提供额外的安全保护。唯一标识符可确保合作伙伴使用正确的客户账户。

允许合作伙伴产品以跨账户角色向 Security Hub 中的客户发送调查发现需要四个步骤：

1. 客户或代表客户使用跨账户角色的合作伙伴开始订阅 Security Hub 中的产品。
2. 经客户确认，Security Hub 会生成正确的托管资源策略。
3. 客户可以手动或使用配置跨账户角色。 AWS CloudFormation有关跨账户角色的信息，请参阅 IAM 用户指南中的向第三方拥有的 AWS 账户提供访问权限。
4. 该产品可安全存储客户角色和外部 ID。

接下来，该产品将结果发送到 Security Hub：

1. 产品调用 AWS Security Token Service (AWS STS) 来扮演客户角色。
2. 该产品使用所担任角色的临时证书在 Security Hub 上调用 BatchImportFindings API 操作。

以下是 IAM policy 向合作伙伴跨账户角色授予必要的 Security Hub 权限的示例。

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

该策略的 Resource 部分确定了具体的产品订阅。这样确保了合作伙伴只能为客户订阅的合作伙伴产品发送调查发现。

客户托管：从客户账户发送的调查发现

此使用案例包括在客户 AWS 账户中部署产品的合作伙伴。在客户账户中运行的解决方案会调用 BatchImportFindings API。

对于此使用案例，必须向合作伙伴产品授予调用 BatchImportFindingsAPI 的附加权限。授予此权限的方式因合作伙伴解决方案及其在客户账户中的配置方式而异。

这种方法的一个例子是在客户账户中的 EC2 实例上运行的合作伙伴产品。此 EC2 实例必须附加一个 EC2 实例角色，以授予该实例调用 BatchImportFindingsAPI 操作的能力。这允许 EC2 实例向客户的账户发送安全调查结果。

此使用案例在功能上等同于客户将自有产品的调查发现加载到其账户中的场景。

客户允许合作伙伴产品在 Security Hub 中将客户账户中的调查发现发送给客户：

1. 客户使用或其他部署工具手动将合作伙伴产品部署到他们的 AWS 账户 AWS CloudFormation中。
2. 客户定义必要的 IAM policy，供合作伙伴产品在向 Security Hub 发送调查发现时使用。

3. 客户将策略附加到合作伙伴产品的必要组件，例如 EC2 实例、容器或 Lambda 函数。

现在，该产品可以将调查发现发送到 Security Hub：

1. 合作伙伴产品使用 AWS SDK 或在 Secur AWS CLI ity Hub 中调用 BatchImportFindingsAPI 操作。它从客户账户中附加有策略的组件发起调用。
2. 在 API 调用期间，将生成必要的临时凭证以使 BatchImportFindings 调用成功。

以下是 IAM policy 向客户账户中的合作伙伴产品授予 Security Hub 必要权限的示例。

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

合作伙伴入驻流程

作为合作伙伴，您可以期待在入驻流程中完成若干高级步骤。必须先完成这些步骤，然后才能将安全调查结果发送到 AWS Security Hub。

1. 您主动与 APN 合作伙伴团队或 Security Hub 团队联系，表示您有兴趣成为 Security Hub 的合作伙伴。您确定要添加到 Security Hub 通信渠道的电子邮件地址。
2. AWS 为您提供 Security Hub 合作伙伴入职材料。
3. 还会邀请您加入 Security Hub 合作伙伴 Slack 通道，您可在此提出与您集成相关的问题。
4. 您需向 APN 合作伙伴联系人提供一份产品集成清单草稿以供审核。

   产品集成清单包含用于创建与之集成的合作伙伴产品亚马逊资源名称 (ARN) 的信息。 AWS Security Hub

   它为 Security Hub 团队提供了要在 Security Hub 控制台的合作伙伴提供商页面上显示的信息。它还用于提出与集成相关的新托管见解，以便添加到 Security Hub 见解库中。

   产品集成清单的初始版本不必包含完整的详细信息。但它至少应该包含使用案例和数据集信息。

   有关清单和所需信息的详细信息，请参阅 产品集成清单。
5. Security Hub 团队会为您的产品提供产品 ARN。使用 ARN 将调查发现发送到 Security Hub。
6. 您可以构建集成，以将调查发现发送到 Security Hub 或接收来自 Security Hub 的调查发现。

   将调查发现映射到 ASFF

   要将调查结果发送到 Security Hub，您必须将发现的结果映射到 AWS 安全调查结果格式 (ASFF)。

   ASFF 对调查发现进行了一致的描述，可供 AWS 安全服务、合作伙伴和客户安全系统共享。这可减少集成工作，提倡使用通用语言，并为实施者提供蓝图。

   ASFF 是向 AWS Security Hub发送调查发现所需的通信协议格式。调查发现以符合 ASFF JSON 架构和 RFC-7493 The I-JSON Message Format 的 JSON 文档呈现。有关 ASFF 架构的详细信息，请参阅《AWS Security Hub 用户指南》中的 AWS 安全调查发现格式（ASFF）。

   请参阅the section called “ASFF 映射准则”。

构建和测试集成

您可以使用自己拥有的 AWS 账户完成所有集成测试。这样做可让您完全了解调查发现在 Security Hub 中的显示方式。这还可帮助您了解客户对您安全调查发现的体验情况。

您也可以使用 `BatchImportFindings` API 操作向 Security Hub 发送新的和更新的调查发现。

在构建 Security Hub 集成的整个过程中， AWS 鼓励您随时向 APN 合作伙伴联系人通报您的集成进度。您也可以就集成问题向 APN 合作伙伴联系人寻求帮助。

请参阅 the section called “`BatchImportFindings` API 的使用准则”。

7. 您需向 Security Hub 产品团队演示集成。必须使用 Security Hub 团队的账户来演示这一集成。

   如果 Security Hub 团队对集成感到满意，便会批准继续将您列为提供商。
8. 您 AWS 提供一份最终清单以供审核。
9. Security Hub 团队在 Security Hub 控制台中创建提供商集成。然后，客户就可以发现并启用集成。
10. （可选）您可参与额外的营销工作来推广您的 Security Hub 集成。请参阅 Go-to-market 活动。

    Security Hub 建议您至少提供以下资产。
    - 工作集成的演示视频（最长 3 分钟）。该视频用于营销目的，并发布到该 AWS YouTube 频道。
    - 一张单幻灯片架构图，可添加到 Security Hub 首次调用幻灯片中。

Go-to-market 活动

合作伙伴也可以参加各项可选的营销活动，以协助解释和推进其与 AWS Security Hub 的集成。

如果您想创建与 Security Hub 相关的独家营销内容，请在发布内容之前，将草稿发送给您的 APN 合作伙伴经理进行审批。这样便可确保能向所有人统一传递消息。

AWS 合作伙伴网络 (APN) 合作伙伴可以使用 APN 合作伙伴营销中心和市场开发基金 (MDF) 计划来创建活动并获得资金支持。有关这些计划的详细信息，请联系您的合作伙伴经理。

Security Hub 合作伙伴页面上的条目

在您经批准成为 Security Hub 合作伙伴后，您的解决方案方可显示在 AWS Security Hub 合作伙伴页面上。

要在此页面上列示您的解决方案，请向 您的合作伙伴发展经理（PDM）、合作伙伴解决方案架构师（PSA）等 APN 合作伙伴联系人，或向 <securityhub-pms@amazon.com> 发送电子邮件，提供以下详细信息。

- 简要描述您的解决方案及其与 Security Hub 的集成，并简要说明与 Security Hub 集成能为客户提供的价值。此描述限 700 个字符（包括空格）。
- 您的解决方案描述页面的 URL。该网站应针对您的 AWS 集成，更具体地说是您的 Security Hub 集成。该网站应侧重于客户体验和客户在使用集成时获得的价值。
- 您徽标的高分辨率副本（600 x 300 像素）。有关此徽标的详细要求，请参阅 the section called “合作伙伴徽标页面”

新闻稿

作为经批准的合作伙伴，您可以选择在自己的网站和公共关系渠道上发布新闻稿。新闻稿必须获得批准 AWS。

在发布新闻稿之前，您必须将其提交给 APN 合作伙伴营销部门、Security Hub 领导层和 AWS 外部安全服务 (ESS) 审核。 AWS 新闻稿还可包括 ESS 副总裁的拟议报价。

要启动此流程，请与您的 PDM 合作。我们的服务水平协议（SLA）要求在 10 个工作日内审核新闻稿。

AWS 合作伙伴网络 (APN) 博客

我们还可帮助您在 APN 博客上发布您撰写的博客文章。博文必须侧重于客户故事和使用案例。它的定位不能仅仅围绕着成为集成启动合作伙伴。

如果您对此感兴趣，请联系您的 PDM 或 PSA 以开始该流程。APN 博客可能需要 8 周或更长时间才能获得最终批准并发布。

关于 APN 博客的重要信息

在创作博文时，请记住以下事项。

博文内容是什么？

合作伙伴博文应具有教育意义，并针对与 AWS 客户相关的主题提供深厚的专业知识。

博文最好不要超过 1500 字。读者重视深刻的教育内容，这些内容可以教会他们什么是可能的 AWS。

APN 博客内容应为原创内容。请勿改编现有博文或白皮书等来源的内容。

APN 博客还有哪些发文限制？

只有高级或卓越级别的合作伙伴才能在 APN 博客上发文。拥有 APN 计划指定称号（例如服务交付）的精选合作伙伴除外。

每位合伙人每年仅限发布三篇博文。 AWS 拥有数以万计的 APN 合作伙伴，因此必须公平对待每一位合作伙伴。

每篇博文都必须拥有验证解决方案或使用案例的技术赞助商。

博文发布前需要编辑多长时间？

第一份完整的博文草稿提交后，需要四到六周的时间进行编辑。

为什么要为 APN 博客撰稿？

在 APN 博客发文可获得以下好处。

- 可信度 — 对于 APN 合作伙伴来说，发布故事 AWS 可以影响全球客户。
- 知名度 — APN 博客是阅读量最高的博客之一，2019 年页面浏览量为 179 万，其中包括受影响流量。 AWS

- 业务：APN 合作伙伴博文有连接按钮，可通过 AWS 合作伙伴网络客户参与计划（ACE）生成潜在客户。

哪些类型的内容最适合 APN 博客？

APN 博客文章最适合以下类型的内容。

- 技术内容是最受欢迎的故事类型。它包含解决方案亮点和操作方法信息。超过 75% 的读者会查看此类技术内容。
- 客户重视 200 级或以上的故事，这些故事展示了某产品/服务在 AWS 上的运行原理，或者 APN 合作伙伴是如何为客户解决业务问题的。
- 到目前为止，由技术专家或主题专家撰写的博文表现最好。

宣传单

宣传单是一页纸的文档，概述了您的产品及其集成架构，以及共同的客户使用案例。

如果您为您的集成制作了宣传单，请将副本发送给 Security Hub 团队。该团队会将其添加到合作伙伴页面。

白皮书或电子书

如果您制作了白皮书或电子书来简要介绍您的产品及其集成架构，以及共同的客户使用案例，请将副本发送给 Security Hub 团队。该团队会将其添加到 Security Hub 合作伙伴页面。

网络研讨会

如果您为您的集成举办了网络研讨会，请将网络研讨会的录像发送给 Security Hub 团队。该团队会将其链接到合作伙伴页面。

该团队还可以提供一名 Security Hub 主题专家来参加您的网络研讨会。

演示视频

您可以制作工作集成的演示视频来进行营销。在您的视频平台账户上发布此类视频，Security Hub 团队将从合作伙伴页面链接到该视频。

产品集成清单

每个 AWS Security Hub 集成合作伙伴都必须填写一份产品集成清单，其中包含建议的集成所需的详细信息。

Security Hub 团队以多种方式使用这些信息：

- 创建您的网站列表
- 为 Security Hub 控制台创建产品卡
- 让产品团队了解您的使用案例。

Security Hub 团队会使用 the section called “产品准备清单” 来评估拟议集成的质量和您提供的信息。此清单可确定您的集成是否准备就绪，可以启动。

您的文档必须涵盖您提供的所有技术信息。

您可以从 AWS Security Hub 合作伙伴页面的 “资源” 部分下载产品集成清单的 PDF 版本。请注意，在中国（北京）和中国（宁夏）区域不提供合作伙伴页面。

内容

- 使用案例和营销信息
  - 寻找提供商和消费者使用案例
  - 咨询合作伙伴（CP）使用案例
  - 数据集
  - 架构
  - 配置
  - 每位客户每天的平均调查发现数量
  - 延迟
  - 公司和产品描述
  - 合作伙伴网站资产
  - 合作伙伴徽标页面
  - Security Hub 的控制台徽标
  - 调查发现类型
  - 热线

- 心跳调查发现
- AWS Security Hub 控制台信息
  - 公司信息
  - 产品信息

使用案例和营销信息

以下用例可以帮助您 AWS Security Hub 针对不同的目的进行配置。

寻找提供商和消费者使用案例

对独立软件供应商（ISV）来说，该项为必填项。

要描述您与集成的用例 AWS Security Hub，请回答以下问题。如果您不打算发送或接收调查发现，请在本节中注明，然后完成下一节。

您的文档中必须涵盖以下信息。

- 您将发送调查发现、接收调查发现还是两者兼而有之？
- 如果您计划发送调查发现，您将发送哪些类型的调查发现？ 您会发送所有调查发现还是特定调查发现子集？
- 如果您计划接收调查发现，您会如何处理这些调查发现？ 您将接收什么类型的调查发现？ 例如，您将接收所有调查发现、特定类型的调查发现，还是仅接收客户选择的特定调查发现？
- 您打算更新调查发现吗？ 如果是，您将更新哪些字段？ Security Hub 建议您更新调查发现，而不要总是创建新的调查发现。更新现有调查发现有助于为客户减少调查发现噪音。

  如要更新调查发现，您需要发送带有调查发现 ID 的调查发现，该 ID 已分配给您已发送的调查发现。

如要提前获得您使用案例和数据集的相关反馈，请联系 APN 合作伙伴或 Security Hub 团队。

咨询合作伙伴（CP）使用案例

如果您是 Security Hub 咨询合作伙伴，该项为必填项。

提供您与 Security Hub 合作的两个客户使用案例。可以为私有使用案例。Security Hub 团队不会在任何地方为这些案例做广告。这些案例应描述以下一项或两项操作。

- 您如何帮助客户启动 Security Hub？ 例如，您是否帮助客户使用专业服务、Terraform 模块或模板？ AWS CloudFormation
- 您如何帮助客户运营和扩展 Security Hub？ 例如，您是否提供了响应或修复模板、构建了自定义集成或使用商业智能工具来设置执行控制面板？

数据集

如果您要向 Security Hub 发送调查发现，该项为必填项。

请为您将要发送到 Security Hub 的调查发现提供以下信息。

- 调查发现将采用 JSON 或 XML 等本机格式
- 如何将调查结果转换为 AWS 安全调查结果格式 (ASFF) 的示例

如果您需要更新 ASFF 来支持您的集成，请告知 Security Hub 团队。

架构

如果您要向 Security Hub 发送调查发现或从 Security Hub 接收调查发现，该项为必填项。

描述您将如何与 Security Hub 集成。您的文档中必须涵盖这些信息。

您必须提供架构图。在准备您的架构图时，请考虑以下事项：

- 您将使用哪些 AWS 服务、操作系统代理等？
- 如果您要将调查结果发送到 Security Hub，您会从客户 AWS 账户还是从自己的 AWS 账户发送调查结果？
- 如果你会收到调查结果，你将如何使用 CloudWatch 事件集成？
- 您将如何将调查发现转换为 ASFF？
- 您将如何批处理调查发现、跟踪调查发现状态以及避开节流限制？

配置

如果您要向 Security Hub 发送调查发现或从 Security Hub 接收调查发现，该项为必填项。

描述客户将如何配置您与 Security Hub 的集成。

您必须至少使用 AWS CloudFormation 模板或类似的基础架构，例如代码模板。一些合作伙伴还提供支持一键集成的用户界面。

配置时间不应超过 15 分钟。您的产品文档还必须为您的集成提供配置指导。

每位客户每天的平均调查发现数量

如果您要向 Security Hub 发送调查发现，该项为必填项。

您预计每月会在您的客户群中向 Security Hub 发送多少次调查发现更新（平均数量和最大数量）？ 可接受的数量级估值。

延迟

如果您要向 Security Hub 发送调查发现，该项为必填项。

您会以多快的速度批处理调查发现并将其发送到 Security Hub？ 换句话说，从在您的产品中创建调查发现到将其发送到 Security Hub 的延迟有多长时间？

您的集成产品文档中必须涵盖这些信息。这是客户的常见问题。

公司和产品描述

对于与 Security Hub 集成的所有项目，该项为必填项。

简要描述贵公司和产品，并特别说明贵公司的 Security Hub 集成性质。我们会在 Security Hub 合作伙伴页面使用该信息。

如果您要将多个产品与 Security Hub 集成，您可以为每个产品提供单独的描述，但我们会在合作伙伴页面将这些描述合并为一个条目。

每条描述不得超过 700 个字符，包括空格。

合作伙伴网站资产

对于与 Security Hub 集成的所有项目，该项为必填项。

您必须至少提供一个 URL 以用作 Security Hub 合作伙伴页面上的 “了解更多” 超链接。它应该是一个营销登录页面，描述您的产品与 Security Hub 之间的集成。

如果您将多个产品与 Security Hub 集成，则可以为它们设置一个登录页面。Security Hub 建议您在此登录页面中提供指向配置说明的链接。

您还可以提供指向其他资源的链接，例如博客、网络研讨会、演示视频或白皮书等。Security Hub 还将从其合作伙伴页面链接到这些资源。

合作伙伴徽标页面

对于所有 Security Hub 集成，该项为必填项。

提供徽标 URL，以便显示在 Security Hub 合作伙伴页面上。徽标必须符合以下标准：

- 尺寸：600 x 300 像素
- 裁剪：贴边，无内边框
- 背景：透明
- 格式：PNG

Security Hub 的控制台徽标

所有集成都必须填写该项。

提供 URLs 亮模式和深色模式徽标以显示在 Security Hub 控制台上。

徽标必须符合以下标准：

- 格式：SVG
- 尺寸：175 x 40 像素。如果徽标较大，则应使用此图像比例。
- 裁剪：贴边，无内边框
- 背景：透明

有关小徽标的详细指南，请参阅 the section called “控制台徽标准则”。

调查发现类型

如果您要向 Security Hub 发送调查发现，该项为必填项。

提供一个表格，记录您所用 ASFF 格式的调查发现类型以及它们如何与本机调查发现类型保持一致。有关 ASFF 调查发现类型的详细信息，请参阅《AWS Security Hub 用户指南》中的 ASFF 类型分类法。

建议您也在您的产品文档中提供此信息。

热线

对于与 Security Hub 集成的所有项目，该项为必填项。

提供技术联系人的电子邮件地址、电话号码或寻呼机号码。Security Hub 将与该联系人沟通所有技术问题，例如集成不起作用时。

还需为严重性程度高的技术问题提供全天候联系人。

心跳调查发现

如果您要将调查发现发送到 Security Hub，建议您填写该项。

您能否每五分钟向 Security Hub 发送一次“心跳”调查发现，表明您与 Security Hub 的集成已正常运行？

如果能，您应使用 `Heartbeat` 调查发现类型执行此操作。

AWS Security Hub 控制台信息

向 AWS Security Hub 团队提供包含以下信息的 JSON 文本。Security Hub 使用这些信息来创建您的产品 ARN，在控制台中显示提供商列表，并在 Security Hub 见解库中纳入您提出的托管见解。

公司信息

公司信息将提供贵公司的相关信息。示例如下：

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

公司信息包含以下信息：

字段	必需	描述
`id`	是	公司的唯一标识符。公司标识符在所有公司中必须是唯一的。

字段	必需	描述
		这可能与 name 相同或相似。 类型：字符串 最小长度：5 个字符 最大长度：24 个字符 允许使用的字符：小写字母、数字和连字符 必须以小写字母开头。必须以小写字母或数字结尾。
name	是	要在 Security Hub 控制台上显示的提供商公司名称。 类型：字符串 最大长度：16 个字符
description	是	将在 Security Hub 控制台上显示的提供商公司描述。 类型：字符串 最大长度：200 个字符

产品信息

本节提供您产品的相关信息。示例如下：

```
{
    "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"
}
```

产品信息包含以下字段。

字段	必需	描述
IntegrationType	是	指明您的产品是向 Security Hub 发送调查发现，还是从 Security Hub 接收调查发现，或两者兼而有之。 如果您是咨询合作伙伴，请将此字段留白。 类型：字符串数组 有效值：SEND_FINDINGS_TO_SECURITY_HUB | RECEIVE_FINDINGS_FROM_SECURITY_HUB
id	是	产品的唯一标识符。它们在公司内部必须是唯一的。它们在不同公司之间可以相同。这可能与 name 相同或相似。 类型：字符串 最小长度：5 个字符 最大长度：24 个字符 允许使用的字符：小写字母、数字和连字符 必须以小写字母开头。必须以小写字母或数字结尾。
regionsNotSupported	是	您不支持以下哪 AWS 个区域？ 换句话说，Security Hub 应在哪些区域将您排除 Security Hub 控制台的合作伙伴页面？

字段	必需	描述
		类型：字符串 仅提供地区代码。例如，us-west-1 。 有关区域的列表，请参阅 AWS 一般参考 中的区域端点。 的区域代码 AWS GovCloud (US) 是us-gov-west-1 （对于 AWS GovCloud （美国西部））和us-gov-east-1 （对于 AWS GovCloud （美国东部））。 中国区域的区域代码是 cn-north-1 [中国（北京）] 和 cn-northwest-1 [中国（宁夏）]。
commercialAccountNumber	是	各 AWS 地区产品的主要 AWS 账号。 如果您将调查发现发送到 Security Hub，则您提供的账户将取决于您发送调查发现的账户。 • 从你的 AWS 账户。在这种情况下，您应提供用来提交调查发现的账号。 • 来自客户的 AWS 账户。在这种情况下，Security Hub 建议您提供用于集成测试的主账号。 理想情况下，您将在所有区域为您所有产品使用同一账户。如果无法实现这一点，请联系 Security Hub 团队。 如果您只接收来自 Security Hub 的调查发现，则不需要此账号。 类型：字符串

字段	必需	描述
govcloudAccountNumber	否	AWS GovCloud (US) 地区产品的主要 AWS 账号（如果您的产品在中可用 AWS GovCloud (US)）。 如果您将调查发现发送到 Security Hub，则您提供的账户将取决于您发送调查发现的账户。 • 从你的 AWS 账户。在这种情况下，您应提供用来提交调查发现的账号。 • 来自客户的 AWS 账户。在这种情况下，Security Hub 建议您提供用于集成测试的主账号。 理想情况下，您将在整个 AWS GovCloud (US) 区域为您所有产品使用同一账户。如果无法实现这一点，请联系 Security Hub 团队。 如果您只接收来自 Security Hub 的调查发现，则不需要此账号。 类型：字符串

字段	必需	描述
chinaAccountNumber	否	中国地区产品的主要 AWS 账号（如果您的产品在中国地区有售）。 如果您将调查发现发送到 Security Hub，则您提供的账户将取决于您发送调查发现的账户。 • 从你的 AWS 账户。在这种情况下，您应提供用来提交调查发现的账号。 • 来自客户的 AWS 账户。在这种情况下，Security Hub 建议您提供用于产品集成测试的主账号。 理想情况下，您在中国所有区域为所有产品使用同一账户。如果无法实现这一点，请联系 Security Hub 团队。 如果您只接收来自 Security Hub 的调查发现，则可使用您在中国区域的任何账户。 类型：字符串
name	是	提供商要显示在 Security Hub 控制台上的产品名称。 类型：字符串 最大长度：24 个字符
description	是	提供商要在 Security Hub 控制台上显示的产品描述。 类型：字符串 最大长度：200 个字符

字段	必需	描述
importType	是	合作伙伴的资源策略类型。 在合作伙伴入驻过程中，您可以指定以下资源策略之一，也可以指定 NEITHER。 • 使用 BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT ，您只能从您产品 ARN 中列出的账户向 Security Hub 发送调查发现。 • 使用 BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT ，您只能从订阅您的客户账户发送调查发现。 类型：字符串 有效值： BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT | BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT | NEITHER

字段	必需	描述
category	是	定义您的产品类别。您的选择将显示在 Security Hub 控制台上。 最多选择三个类别。 不允许自定义选择。如果您认为您的类别丢失，请联系 Security Hub 团队。 类型：数组 可用类别： • 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

字段	必需	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

字段	必需	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	您的产品 AWS Marketplace 目的地的 URL。URL 显示在 Security Hub 控制台中。 类型：字符串 这必须是一个 AWS Marketplace 网址。 如果您没有 AWS Marketplace 房源，请将此字段留空。

字段	必需	描述
`configurationUrl`	是	您产品文档的 URL，该文档介绍您与 Security Hub 的集成。这些内容托管在您的网站或您管理的网页（例如 GitHub 页面）上。 类型：字符串 您的文档应包含以下信息： • 配置说明 • AWS CloudFormation 模板链接（如有必要） • 您的集成使用案例的相关信息 • 延迟 • ASFF 映射 • 所含调查发现的类型 • 架构

准则和核对清单

在准备 AWS Security Hub 集成所需的材料时，请使用以下指南。

在 Security Hub 向 Security Hub 客户提供集成之前，准备清单用于对集成进行最终审查。

主题

- 在 AWS Security Hub 控制台上显示徽标的准则
- 创建和更新调查发现的原则
- 将调查结果映射到 AWS 安全调查结果格式 (ASFF) 的指南
- BatchImportFindings API 的使用准则
- 产品准备清单

在 AWS Security Hub 控制台上显示徽标的准则

要在 AWS Security Hub 主机上显示徽标，请遵循以下指南。

浅色和深色模式

您必须同时提供浅色模式和深色模式的徽标版本。

格式

SVG 文件格式

背景颜色

透明度

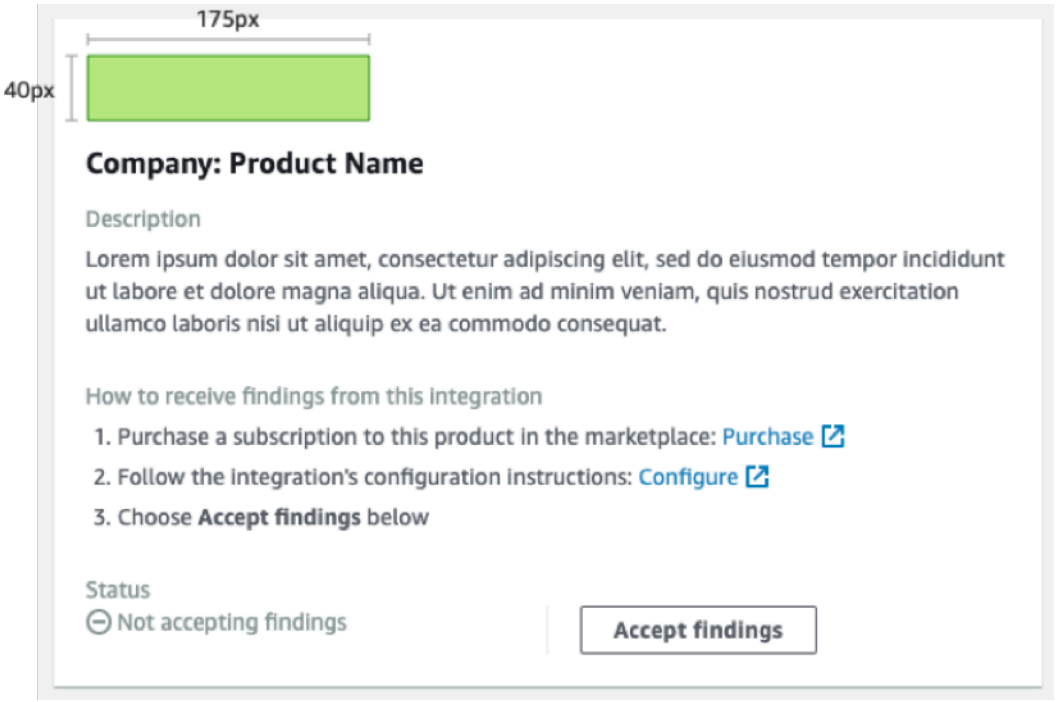
尺寸

理想比例是宽 175 像素，高 40 像素。

最小高度为 40 像素。

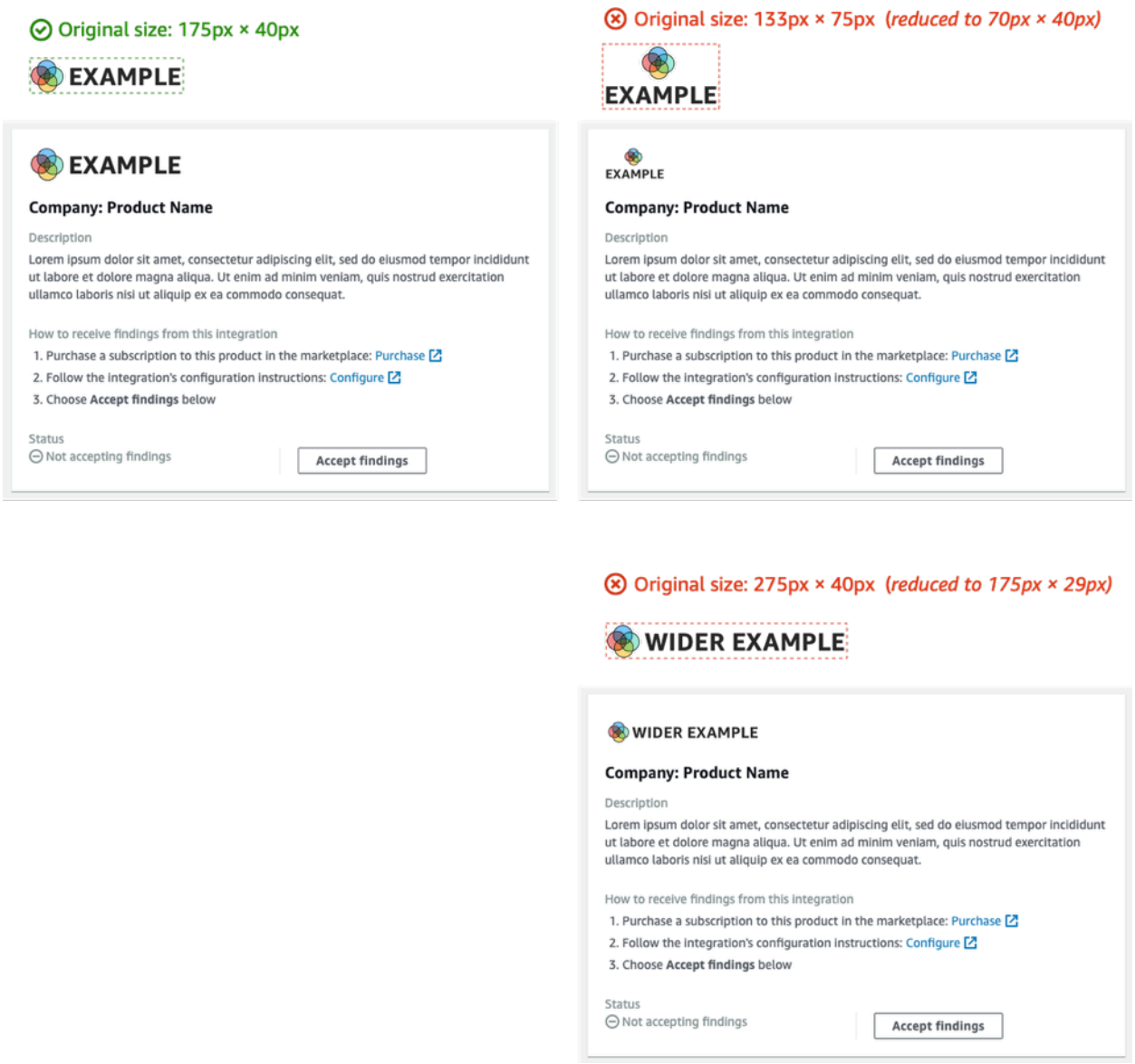
矩形徽标效果最好。

下图说明了理想徽标在 Security Hub 控制台上的显示方式。



如果您的徽标与这些尺寸不匹配，Security Hub 会将尺寸缩小到最大高度为 40 像素，最大宽度为 175 像素。这会影响徽标在 Security Hub 控制台上的显示方式。

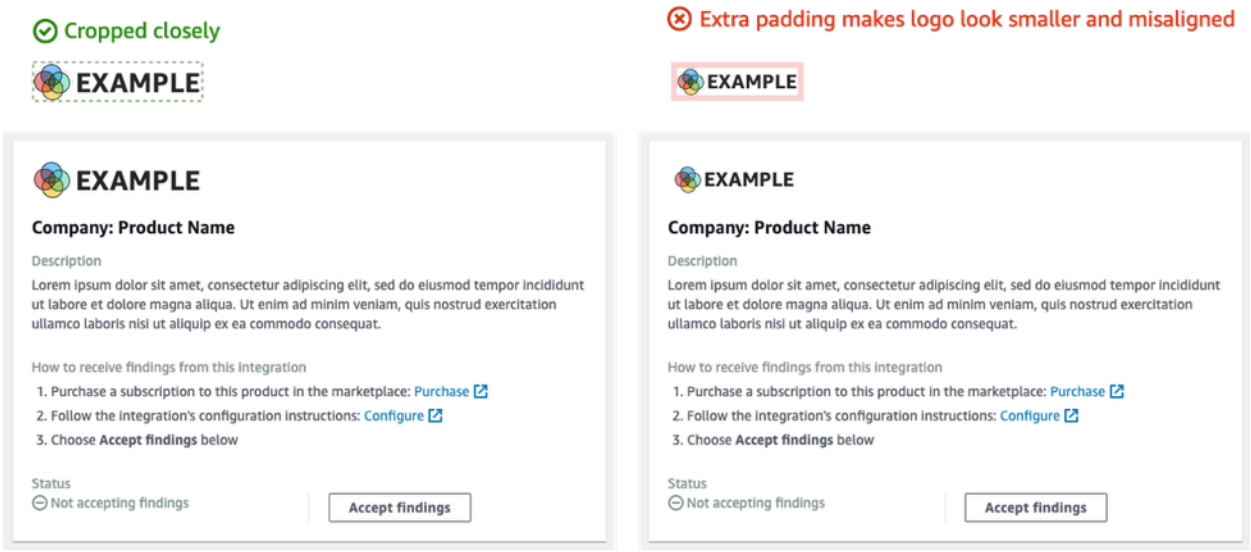
下图比较了理想尺寸徽标与较宽或较高徽标的显示情况。



裁剪

尽可能贴边裁剪徽标图像。不要留下额外的内边框。

下图显示了尽可能贴边裁剪的徽标和带有额外内边框的徽标之间的区别。



创建和更新调查发现的原则

在计划如何在中创建和更新发现结果 AWS Security Hub时，请记住以下原则。

详细地描述调查发现，以便客户可以轻松地对其采取行动。

客户希望自动执行响应和修复措施，并将调查发现与其他调查发现关联起来。为支持这一点，调查发现应具有以下特征：

- 它们通常应处理单一资源或主要资源。
- 它们应该只有一种调查发现类型。
- 它们应该处理单一的安全事件。

调查发现包含多个安全事件的数据时，客户就更难对调查发现采取行动。

将所有查找字段映射到 AWS 安全调查结果格式 (ASFF)。允许客户依赖 Security Hub 作为事实来源。

客户希望本机调查发现格式的每个字段也能在 Security Hub ASFF 中得到体现。

客户希望所有数据都出现在 Security Hub 版本的调查发现中。数据丢失会导致他们对作为安全信息来源中心的 Security Hub 失去信任。

尽量减少调查发现中的冗余。不要用海量调查发现让客户不知所措。

Security Hub 不是一个通用的日志管理工具。您应该向 Security Hub 发送具有高度可操作性、客户可以直接响应、修复或与其他调查发现相关联的调查发现。

在调查发现的变化很小时，应更新调查发现而不是创建新的调查发现。

在调查发现发生重大变化（例如严重性分数或资源标识符）时，应创建新的调查发现。

例如，实时为单个端口扫描创建调查发现不太可行。由于端口扫描可以持续进行，因此会产生大量调查发现。从 TOR 节点对 MongoDB 端口进行端口扫描时，只需对单个调查发现更新上次扫描时间和扫描次数，这样做更有说服力，也更精确。

允许客户自定义调查发现，使其更有意义。

客户希望能够调整某些调查发现字段，使其更契合他们的环境或要求。

例如，客户希望能够添加注释、标签，并根据与调查发现相关联的账户类型或资源类型调整严重性分数。

将调查结果映射到 AWS 安全调查结果格式 (ASFF) 的指南

使用以下准则将您的调查发现映射到 ASFF。有关每个 ASFF 字段和对象的详细描述，请参阅《AWS Security Hub 用户指南》中的 AWS 安全调查发现格式（ASFF）。

识别信息

`SchemaVersion` 始终为 `2018-10-08`。

`ProductArn`是 AWS Security Hub 分配给你的 ARN。

`Id` 是 Security Hub 用来为调查发现编制索引的值。调查发现标识符必须是唯一的，以确保其他调查发现不会被覆盖。如要更新调查发现，应使用相同的标识符重新提交调查发现。

`GeneratorId`可以与离散的逻辑单元相同`Id`或可以指代离散的逻辑单元，例如 Amazon GuardDuty 探测器 ID、 AWS Config 录制器 ID 或 IAM Access Analyzer ID。

Title 以及 Description

`Title` 应包含受影响资源的一些相关信息。`Title` 限 256 个字符，包括空格。

在 `Description` 中添加更多详细信息。`Description` 限 1024 个字符，包括空格。你可以考虑在描述中添加截断。示例如下：

```
"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.",
```

调查发现类型

您可在 FindingProviderFields.Types 中提供您的调查发现类型信息。

Types 应符合 ASFF 的类型分类法。

如有需要，您可以指定自定义分类器（第三个命名空间）。

时间戳

ASFF 格式包括几个不同的时间戳。

CreatedAt 和 UpdatedAt

每次为各项调查发现调用 BatchImportFindings 时，您必须提交 CreatedAt 和 UpdatedAt。

这些值必须与 Python 3.8 中的 ISO86 01 格式相匹配。

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

FirstObservedAt 和 LastObservedAt

您系统观察到调查发现时，FirstObservedAt 和 LastObservedAt 必须匹配。如果您未记录此信息，则无需提交这些时间戳。

这些值与 Python 3.8 中的 ISO86 01 格式相匹配。

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

Severity

您可在 FindingProviderFields.Severity 对象中提供严重性信息，其应包含以下字段。

Original

来自您系统的严重性值。Original 可是任何字符串，以便适应您使用的系统。

Label

必需的 Security Hub 指标，可表示调查发现的严重性。允许的值如下：

- INFORMATIONAL：未发现任何问题。
- LOW：无需针对问题执行任何操作。
- MEDIUM：必须解决问题，但不是紧急的。
- HIGH：必须优先解决问题。
- CRITICAL：必须立即纠正问题,防止造成进一步的伤害。

合规的调查发现应始终将 Label 设置为 INFORMATIONAL。INFORMATIONAL发现的示例包括通过安全检查的 AWS Firewall Manager 结果和经过补救的结果。

客户通常按严重性对调查发现进行排序，以便为其安全运营团队提供待办事项清单。将调查发现的严重性设置为 HIGH 或 CRITICAL 时,应保持谨慎。

您的集成文档必须包含您的映射原理。

Remediation

Remediation 有两个要素。这两个元素在 Security Hub 控制台上以组合的形式出现。

Remediation.Recommendation.Text 出现在调查发现详细信息的“修复”部分。它已超链接到的 Remediation.Recommendation.Url 值。

目前，只有来自 Security Hub 标准、IAM Access Analyzer 和 Firewall Manager 的调查发现才会显示指向如何修复调查发现的文档超链接。

SourceUrl

仅在您可以为特定调查发现提供指向您控制台的深度链接 URL 时，才使用 SourceUrl。否则，将其从映射中省略。

Security Hub 不支持来自此字段的超链接，但它已在 Security Hub 控制台上公开。

Malware, Network, Process, ThreatIntelIndicators

适用时，可使用Malware、Network、Process 或 ThreatIntelIndicators。这些对象中均公开显示在 Security Hub 控制台中。在您发送的调查发现的上下文中使用这些对象。

例如，如果您检测到与已知命令和控制节点建立出站连接的恶意软件，请在中提供该 EC2 实例的详细信息Resource.Details.AwsEc2Instance。为该 EC2实例提供相关的MalwareNetwork、和ThreatIntelIndicator对象。

Malware

Malware 是一个最多可接受五组恶意软件信息的列表。让恶意软件条目与资源和调查发现相关。

每个条目都包含以下字段。

Name

恶意软件的名称。该值是最多 64 个字符的字符串。

Name 应来自经过审查的威胁情报或研究人员来源。

Path

该恶意软件的路径。该值是最多 512 个字符的字符串。Path 应该是 Linux 或 Windows 系统文件路径，但以下情况除外。

- 如果您根据 YARA 规则扫描 S3 存储桶或 EFS 共享中的对象，则Path 为 S3:// 或 HTTPS 对象路径。
- 如果您扫描 Git 存储库中的文件，则 Path 为 Git URL 或克隆路径。

State

恶意软件的状态。容许值为 OBSERVED | REMOVAL_FAILED | REMOVED。

务必在调查发现标题和描述中提供恶意软件发生事件的背景信息。

例如，如果 Malware.State 是 REMOVED，则调查发现的标题和描述应反映出您的产品删除了路径上的恶意软件。

如果 Malware.State 是 OBSERVED，则调查发现的标题和描述应反映出您的产品在路径上遇到了该恶意软件。

Type

指明恶意软件的类型。容许值为 ADWARE | BLENDED_THREAT | BOTNET_AGENT | COIN_MINER | EXPLOIT_KIT | KEYLOGGER | MACRO | POTENTIALLY_UNWANTED | SPYWARE | RANSOMWARE | REMOTE_ACCESS | ROOTKIT | TROJAN | VIRUS | WORM。

如果您需要其他 Type 值，请联系 Security Hub 团队。

Network

Network 是一个单一对象。您不能添加多个与网络相关的详细信息。映射字段时，应使用以下准则。

目的地和来源信息

目的地和来源很容易映射 TCP 或 VPC 流日志或 WAF 日志。在您描述有关攻击调查发现的网络信息时，这些信息用起来就更加困难。

通常，来源是攻击发起的地方，但也可能是如下所示的其他来源。您应在您的文档中解释来源，还应在调查发现的标题和描述中对其进行说明。

- 对于 EC2 实例的 DDo S 攻击，来源是攻击者，尽管真正的 DDo S 攻击可能会使用数百万台主机。目的地是 EC2 实例的公共 IPv4 地址。 `Direction`已进入。
- 对于观察到的从 EC2 实例与已知命令和控制节点通信的恶意软件，来源是该 EC2 实例 IPV4 的地址。目的地是命令和控制节点。`Direction` 为 `OUT`。您还需要提供 `Malware` 和 `ThreatIntelIndicators`。

`Protocol`

除非您可以提供特定的协议，否则 `Protocol` 始终映射到互联网编号分配机构（IANA）的注册名称。您应该始终使用它并提供端口信息。

`Protocol` 独立于来源和目的地信息。只在有意义的时候才提供它。

`Direction`

`Direction`始终相对于 AWS 网络边界。

- `IN`表示正在进入 AWS （VPC、服务）。
- `OUT`表示它正在退出 AWS 网络边界。

Process

`Process` 是一个单一对象。您不能添加多个与流程相关的详细信息。映射字段时，应使用以下准则。

`Name`

`Name` 应与可执行文件的名称相匹配。最多可接受 64 个字符。

`Path`

`Path` 是可执行进程的文件路径。最多可接受 512 个字符。

`Pid`, **`ParentPid`**

`Pid` 和 `ParentPid` 应与 Linux 进程标识符（PID）或 Windows 事件 ID 一致。为了区分差异，请使用 EC2 亚马逊系统映像 (AMI) 来提供信息。客户或许可以区分 Windows 和 Linux。

时间戳（**LaunchedAt** 和 **TerminatedAt**）

如果您无法可靠地检索此信息，并且该信息不能精确到毫秒级，请不要提供该信息。

如果客户依赖时间戳进行取证调查，那么没有时间戳比使用错误的时间戳要好。

ThreatIntelIndicators

`ThreatIntelIndicators` 接受最多五个威胁情报对象的数组。

每个条目的 `Type` 都根据特定威胁的情况而定。容许值为 `DOMAIN` | `EMAIL_ADDRESS` | `HASH_MD5` | `HASH_SHA1` | `HASH_SHA256` | `HASH_SHA512` | `IPV4_ADDRESS` | `IPV6_ADDRESS` | `MUTEX` | `PROCESS` | `URL`。

下面是一些如何映射威胁情报指标的示例：

- 您找到了一个与 Cobalt Strike 相关的进程。您知道该进程，这是你从 FireEye的博客中学到的。

  将 `Type` 设置为 `PROCESS`。还要为进程创建一个 `Process` 对象。
- 您的邮件过滤器发现有人从已知恶意域发送了一个经过散列计算的著名数据包。

  创建两个 `ThreatIntelIndicator` 对象。一个对象用于 `DOMAIN`。另一个是用于 `HASH_SHA1`。
- 你发现了带有 Yara 规则的恶意软件（Loki、Fenrir、Awss3、）。VirusScan BinaryAlert

  创建两个 `ThreatIntelIndicator` 对象。一个是针对恶意软件。另一个是用于 `HASH_SHA1`。

Resources

`Resources` 应尽可能使用我们提供的资源类型和详细信息字段。Security Hub 会不断向 ASFF 添加新资源。如需获取 ASFF 的每月变动日志，请联系 `<securityhub-partners@amazon.com>`。

如果建模资源类型的详细信息字段中无法容纳信息，您可将其余详细信息映射到 `Details.Other`。

对于未在 ASFF 中建模的资源，可将 `Type` 设置为 `Other`。有关详细信息，请使用 `Details.Other`。

您也可以将`Other`资源类型用于非AWS 调查结果。

ProductFields

仅在您无法为 Resources 使用其他辅助字段或描述性对象（例如ThreatIntelIndicators、Network 或 Malware）时才使用 ProductFields。

如果您使用了 ProductFields，则必须为此决定提供严谨的理由。

合规

仅在您的调查发现与合规性有关时，才使用 Compliance。

Security Hub 将 Compliance 用于基于控制生成的调查发现。

Firewall Manager 将 Compliance 用于其调查发现，这是因为它们与合规性相关。

受限字段

这些字段旨在让客户跟踪他们对调查发现的调查。

切勿映射到这些字段或对象。

- Note
- UserDefinedFields
- VerificationState
- Workflow

可将这些字段映射到 FindingProviderFields 对象中的字段。切勿映射到顶级字段。

- Confidence：仅在您的服务具有类似功能，或您百分百相信您的调查发现时，才包括置信度分数（0-99）。
- Criticality：关键性分数（0-99）旨在表示调查发现相关资源的重要性。
- RelatedFindings：仅在您可以跟踪与同一资源或调查发现类型相关的调查发现时，才提供相关的调查发现。如欲识别相关的调查发现，您必须参考 Security Hub 中已有调查发现的调查发现标识符。

BatchImportFindings API 的使用准则

使用 BatchImportFindingsAPI 操作将调查结果发送到时 AWS Security Hub，请遵循以下准则。

- 您必须使用与调查发现相关的账户来调用 BatchImportFindings。相关账户的标识符是调查发现的 AwsAccountId 属性值。
- 尽您所能发送最大批量。Security Hub 每批最多接受 100 个调查发现，每个调查发现最大为 240 KB，每批次最大为 6 MB。
- 每个区域每个账户的节流速率限制为 10 TPS，突增速率为 30 TPS。
- 如果存在节流或网络问题，您必须实施一种机制来保持调查发现的状态。您还需要了解调查发现状态，以便您可以在调查发现符合或不符合合规性要求提交调查发现更新。
- 有关字符串的最大长度和其他限制信息，请参阅《AWS Security Hub 用户指南》中的 AWS 安全调查发现格式（ASFF）。

产品准备清单

AWS Security Hub 和 APN 合作伙伴团队使用此清单来验证集成是否已准备就绪，可以启动。

ASFF 映射

这些问题与您的发现与 AWS 安全调查结果格式 (ASFF) 的映射有关。

合作伙伴的所有调查发现数据是否都已映射到 ASFF？

将您所有调查发现都以某种方式映射到 ASFF。

使用辅助字段，例如建模资源类型、Network、Malware 或 ThreatIntelIndicators。

酌情将其他任何内容映射到 Resource.Details.Other 或 ProductFields。

合作伙伴是否使用 **Resource.Details** 字段，例如 **AwsEc2instance**、**AwsS3Bucket** 和 **Container**？ 合作伙伴是否使用 **Resource.Details.Other** 来定义未在 ASFF 中建模的资源详细信息？

只要有可能，请在调查结果中使用提供的精选资源（例如 EC2 实例、S3 存储桶和安全组）字段。

仅在没有直接匹配项时，才将与资源相关的其他信息映射到 Resource.Details.Other。

合作伙伴是否将值映射到 **UserDefinedFields**？

切勿使用 UserDefinedFields。

考虑使用其他辅助字段，例如 Resource.Details.Other 或 ProductFields。

合作伙伴是否将信息映射到 **ProductFields**（该字段可映射到其他 ASFF 字段）？

仅将 ProductFields 用于特定产品信息，例如版本控制信息、特定产品的严重性调查发现以及其他无法映射到辅助字段的信息或 Resources.Details.Other。

合作伙伴是否已为 **FirstObservedAt** 导入自己的时间戳？

FirstObservedAt 时间戳旨在记录在产品中观察到调查发现的时间。如有可能，应映射此字段。

除了想要更新的调查发现外，合作伙伴是否提供为每个调查发现标识符生成的唯一值？

Security Hub 中的所有搜索调查发现都以调查发现标识符（Id 属性）为索引。此值必须始终是唯一的，以避免意外更新调查发现。

您还应保持调查发现标识符状态，以便更新调查发现。

合作伙伴是否提供可将调查发现映射到生成器 ID 的值？

GeneratorID 不应与调查发现 ID 具有相同的值。

GeneratorID 应能够根据调查发现的生成原因，将调查发现有逻辑地联系起来。

这可以是产品中的子组件（产品 A - 漏洞与产品 A - EDR）或类似物品。

合作伙伴是否以与其产品相关的方式使用所需的调查发现类型命名空间？ 合作伙伴是否在其调查发现类型中使用推荐的调查发现类型类别或分类器？

调查发现类型分类法应与产品生成的调查发现紧密对应。

AWS 安全调查结果格式中列出的第一级命名空间是必填的。

您可以为二级和三级命名空间（类别或分类器）使用自定义值。

如果合作伙伴有网络数据，他们是否会在 **Network** 字段捕获网络流量信息？

如果您的产品捕获了 NetFlow 信息，请将其映射到现Network场。

如果合作伙伴有进程（PID）数据，他们是否会在 **Process** 字段中捕获进程信息？

如果您的产品捕获到进程信息，则将其映射到 Process 字段。

如果合作伙伴有恶意软件数据，他们是否会在 **Malware** 字段捕获恶意软件信息？

如果您的产品捕获到恶意软件信息，则将其映射到 Malware 字段。

如果合作伙伴有威胁情报数据，他们是否会在 **ThreatIntelIndicators** 字段捕获威胁情报信息？

如果您的产品捕获到威胁情报信息，则将其映射到 ThreatIntelIndicators 字段。

合作伙伴是否为调查发现提供置信度评级？ 如果有，他们是否提供了理由？

每次使用此字段，您都要在文档和清单中说明理由。

合作伙伴是否在调查发现中将规范 ID 或 ARN 用作资源 ID？

识别 AWS 资源时，最佳做法是使用 ARN。如果 ARN 不可用，则应使用规范资源 ID。

集成设置和功能

这些问题与集成的设置和 day-to-day功能有关。

合作伙伴是否提供 infrastructure-as-code (IaC) 模板来部署与 Security Hub 的集成，例如 Terraform、AWS CloudFormation或？ AWS Cloud Development Kit (AWS CDK)

对于将从客户账户发送调查结果或使用 CloudWatch 事件来使用调查结果的集成，需要某种形式的 IaC 模板。

AWS CloudFormation 是首选，但 AWS CDK 也可以使用 Terraform。

合作伙伴产品的控制台上是否有与 Security Hub 集成的一键设置？

一些合作伙伴产品在其产品中使用开关或类似机制来激活集成。这可能需要自动配置资源和权限。如果您要从产品帐户发送调查发现，首选方法当属一键设置。

合作伙伴是否只发送有价值的调查发现？

通常，您应该只向 Security Hub 客户发送具有安全价值的调查发现。

Security Hub 不是一个通用的日志管理工具。您不应将所有可能的日志都发送到 Security Hub。

合作伙伴是否提供了他们每天将向每位客户发送多少个调查发现以及发送频率（平均和突发）的估计值？

唯一调查发现的数量用于计算 Security Hub 的负载。唯一调查发现的定义是与另一个调查发现具有不同 ASFF 映射的调查发现。

例如，如果一个调查发现仅填充 `ThreatIntelIndicators`，另一个仅填充 `Resources.Details.AWSEc2Instance`，则这两个均为唯一调查发现。

合作伙伴是否有妥善处理 4xx 和 5xx 错误的方法，让其不会受到节流，并在稍后时间发送所有调查发现？

目前，BatchImportFindings API 操作的突发速率为 30 - 50 TPS。如果返回 4xx 或 5xx 错误，您必须保留这些失败的调查发现状态，以便稍后可以全部重试。您可以通过死信队列或其他 AWS 消息服务（例如 Amazon SNS 或 Amazon SQS）来执行此操作。

合作伙伴是否会保留其调查发现的状态，以便他们知道是否该归档不再存在的调查发现？

如果您计划通过覆盖原始调查发现 ID 来更新调查发现，则必须使用一种机制来保留状态，以便为正确的调查发现更新正确的信息。

如果您提供调查发现，切勿使用 BatchUpdateFindings 操作来更新调查发现。此操作只能由客户使用。您只有在对调查发现进行调查并采取行动时，才能使用 BatchUpdateFindings。

合作伙伴处理重试的方式是否会影响先前发送的成功调查发现？

您应该有一种机制，可以在出现错误时保留原始调查 IDs 结果，这样您就不会错误地重复或覆盖成功的搜索结果。

合作伙伴是否使用现有调查发现的调查发现 ID 来调用 **BatchImportFindings** 操作，从而更新调查发现？

如要更新调查发现，您必须提交相同的调查发现 ID 来覆盖现有调查发现。

该 BatchUpdateFindings 操作只能由客户使用。

合作伙伴是否使用 **BatchUpdateFindings** API 来更新调查发现？

如果您要对调查发现采取行动，则可以使用 BatchUpdateFindings 操作来更新特定字段。

合作伙伴是否提供有关从创建调查发现到将其从产品发送到 Security Hub 之间的延迟时间信息？

您应尽量减少延迟，确保客户尽快在 Security Hub 中看到调查发现。

清单中必须提供此信息。

如果合作伙伴的架构是将调查发现从客户账户发送到 Security Hub，那么他们是否成功地证明了这一点？ 如果合作伙伴的架构是通过自己的账户向 Security Hub 发送调查发现，他们是否成功示范了这一点？

在测试期间，必须从您拥有的账户成功发送调查发现，该账户不同于为产品 ARN 提供的账户。

从产品 ARN 所有者的账户发送调查发现可以绕过 API 操作中的某些错误异常。

合作伙伴是否向 Security Hub 提供了心跳调查发现？

要证明您的集成运行正常，您应该发送心跳调查发现。每五分钟发送一次心跳调查发现，并使用 `Heartbeat` 调查发现类型。

如果您从产品账户发送调查发现，这一点便很重要。

测试期间，合作伙伴是否与 Security Hub 产品团队的账户进行了集成？

在预制作验证期间，您应将发现示例发送到 Security Hub 产品团队的 AWS 账户。这些示例证明，调查发现的发送和映射都是正确的。

文档

这些问题与您提供的集成文档有关。

合作伙伴是否将其文档托管在专门的网站上？

文档应以静态网页、wiki、Read the Docs 或其他专用格式托管在您的网站上。

在上托管文档 GitHub 不符合专用网站的要求。

合作伙伴文档是否提供有关如何设置 Security Hub 集成的说明？

您可以使用 IaC 模板或基于控制台的“一键式”集成来设置集成。

合作伙伴文档是否提供了其使用案例的描述？

您在清单中提供的使用案例也应在文档中加以描述

合作伙伴文档是否说明了其所发送调查发现的依据？

您应为所发送调查发现类型提供依据。

例如，您的产品可能会生成漏洞、恶意软件和防病毒的调查发现，但您只能将漏洞和恶意软件调查发现发送到 Security Hub。在这种情况下，您必须提供不发送防病毒调查发现的依据。

合作伙伴文档是否说明了合作伙伴如何将其调查发现映射到 ASFF 的原理？

您应该提供将产品的本机调查发现映射到 ASFF 的原理。客户希望知道在哪里可以找到具体的商品信息。

如果合作伙伴更新了调查发现，合作伙伴文档是否就其如何更新调查发现提供了指导？

向客户提供有关您如何保留状态的信息，确保偶然性，并用信息覆盖调查结果。 up-to-date

合作伙伴文档是否描述了调查发现延迟？

尽量减少延迟，确保客户尽快在 Security Hub 中看到调查发现。

清单中必须提供此信息。

合作伙伴文档是否描述了其严重性评分与 ASFF 严重性评分的对应关系？

提供有关您如何将 `Severity.Original` 映射到 `Severity.Label` 的信息。

例如，如果您的严重性值为字母等级（A、B、C），您应提供有关如何将字母等级映射到严重性标签的信息。

合作伙伴文档是否提供了置信度评级依据？

如果您提供置信度分数，则应对这些分数进行排序。

如果您使用静态填充的置信度分数或源自人工智能或机器学习的映射，则应提供其他背景信息。

合作伙伴文档是否记录了合作伙伴支持和不支持哪些区域？

您应记录支持或不支持的区域，以便客户知道不应在哪些区域尝试集成。

产品卡片信息

这些问题与 Security Hub 控制台“集成”页面上显示的产品卡片有关。

提供的 AWS 账户 ID 是否有效且包含 12 位数字？

账户标识符的长度为 12 位数。如果账户 ID 包含的数字少于 12 位，则产品 ARN 将无效。

商品描述中是否包含 200 个或更少的字符？

清单中 JSON 部分的产品描述不应超过 200 个字符（包括空格）。

配置链接是否指向集成文档？

配置链接应指向您的在线文档。它不应指向您的主网站或营销页面。

购买链接（如果提供）是否会指向该 AWS Marketplace 商品的上架信息？

如果您提供购买链接，则该链接必须用于 AWS Marketplace 参赛作品。Security Hub 不接受非AWS托管的购买链接。

产品类别对产品的描述是否正确？

在清单中，您最多可以提供三个产品类别。它们应与 JSON 相匹配，不能自定义。您提供的产品类别不能超过三个。

公司名称和产品名称是否正确有效？

公司名称长度必须等于或少于 16 个字符。

产品名称长度必须等于或少于 24 个字符。

产品卡片 JSON 中的产品名称必须与清单中的名称相同。

营销信息

这些问题与集成营销有关。

Security Hub 合作伙伴页面的产品描述是否在 700 个字符以内（包括空格）？

Security Hub 合作伙伴页面最多只能接受 700 个字符，包括空格。

团队会删减较长的描述。

Security Hub 合作伙伴页面徽标是否不大于 600 x 300 像素？

提供一个可公开访问的 URL，并附上不大于 600 x 300 像素的公司徽标（PNG 或 JPG 格式）。

Security Hub 合作伙伴页面上的“了解更多”超链接是否指向合作伙伴的集成专用网页？

“了解更多”链接不应指向合作伙伴的主网站或文档信息。

此链接应始终指向提供集成营销信息的专用网页。

合作伙伴是否提供演示或教学视频，说明如何使用其集成？

演示或集成演练视频不是强制要求，但建议提供。

AWS 合作伙伴网络博客文章是否与合作伙伴及其合作伙伴发展经理或合作伙伴发展代表一起发布？

AWS Partner Network 的博客文章应事先与合作伙伴发展经理或合作伙伴发展代表进行协调。

这些内容独立于您自己撰写的任何博文。

您应留出 4 - 6 周的准备时间。这项工作应在私有产品 ARN 测试完成后开始。

是否会发布合作伙伴主导的新闻稿？

您可以与您的合作伙伴开发经理或合作伙伴发展代表合作，从外部安全服务副总裁处获得报价。您可在新闻稿中使用此报价。

是否会发布合作伙伴主导的博文？

您可以创建自己的博客文章，在 AWS 合作伙伴网络博客之外展示您的集成。

是否发布合作伙伴主导的网络研讨会？

您可以创建自己的网络研讨会来展示集成。

如果您需要 Security Hub 团队的帮助，请在使用私有产品 ARN 完成测试后与产品团队合作。

合作伙伴是否向其请求社交媒体支持 AWS？

发布后，您可以与 AWS 安全营销主管合作，使用 AWS 官方社交媒体渠道分享有关您的网络研讨会的详细信息。

AWS Security Hub 合作伙伴常见问题解答

以下是与 AWS Security Hub集成相关的设置和维护常见问题。

1. Security Hub 集成有哪些好处？
   - 客户满意度：与 Security Hub 集成的首要原因是您的客户有此方面的需求。

     Security Hub 是 AWS 客户的安全与合规中心。它被设计为 AWS 安全和合规专业人员每天前往的第一站，以了解他们的安全与合规状态。

     倾听您客户的意见。他们会告诉您是否想在 Security Hub 看到您的调查发现。
   - 发现机会：我们在 Security Hub 控制台内推广进行过认证集成的合作伙伴（包括其 AWS Marketplace 列表链接）。这是客户发现新安全产品的好方法。
   - 营销机会 — 集成获得批准的供应商可以参加网络研讨会、发布新闻稿、创建精美表格，并向客户展示其集成。 AWS
2. 合作伙伴分为哪几类？
   - 向 Security Hub 发送调查发现的合作伙伴
   - 从 Security Hub 接收调查发现的合作伙伴
   - 既发送也接收调查发现的合作伙伴
   - 帮助客户在其环境中设置、自定义和使用 Security Hub 的咨询合作伙伴
3. 合作伙伴如何与 Security Hub 进行高层次集成？

   您可以从客户账户或自己的 AWS 账户中收集调查结果，然后将调查结果的格式转换为 AWS 安全调查结果格式 (ASFF)。然后，您可将这些调查发现推送到相应的 Security Hub 区域端点。

   您还可以使用 CloudWatch 事件来接收来自 Security Hub 的调查结果。
4. 完成与 Security Hub 集成的基本步骤是什么？
   a. 提交您的合作伙伴清单信息。
   b. 如果您 ARNs 要向 Security Hub 发送调查结果，请接收产品以与 Security Hub 配合使用。
   c. 将您的调查发现映射到 ASFF。请参阅the section called “ASFF 映射准则”。
   d. 定义一个架构，将其用于向 Security Hub 发送调查发现和从 Security Hub 接收调查发现。遵循the section called “创建和更新调查发现的原则”中概述的原则。
   e. 为客户创建部署框架。例如， AWS CloudFormation 脚本可以达到这个目的。
   f. 记录您的设置并为客户提供配置说明。

g. 定义客户可在您的产品中使用的任何自定义见解（关联规则）。

h. 向 Security Hub 团队演示您的集成。

i. 提交营销信息（网站语言、新闻稿、架构幻灯片、视频、宣传单）以供批准。

5. 提交合作伙伴清单的流程是什么？ AWS 服务如何向 Security Hub 发送调查发现？

   请使用 <securityhub-partners@amazon.com> 向 Security Hub 团队提交清单信息。

   您 ARNs 将在七个日历日内收到商品。

6. 我应该向 Security Hub 发送哪些类型的调查发现？

   Security Hub 定价一定程度上基于所接收的调查发现数量。因此，您应避免发送无法为客户带来价值的调查发现。

   例如，一些漏洞管理供应商只发送通用漏洞评分系统（CVSS）评分达 3 分或以上分数（满分 10 分）的调查发现。

7. 有哪些方法可以将调查发现发送到 Security Hub？

   主要方法如下：

   - 您可以使用该BatchImportFindings操作从他们自己的指定 AWS 账户发送调查结果。
   - 您可以使用 BatchImportFindings 操作从客户账户内发送调查发现。您可以使用代入角色的方法，但这些方法并不是必需的。

   有关使用 BatchImportFindings 的综合指南，请参阅 the section called “BatchImportFindings API 的使用准则”。

8. 如何收集我的调查发现并将其推送到 Security Hub 区域端点？

   由于这高度依赖于您的解决方案架构，为此，合作伙伴使用了不同的方法。

   例如，一些合作伙伴构建了一个可以作为 AWS CloudFormation 脚本部署的 Python 应用程序。该脚本从客户环境中收集合作伙伴的调查发现，将其转换为 ASFF，然后将其发送到 Security Hub 区域端点。

   其他合作伙伴构建了一个完整的向导，可让客户一键将调查发现推送到 Security Hub。

9. 怎么知道何时开始向 Security Hub 发送调查发现？

   Security Hub 支持对 BatchImportFindings API 操作进行部分批量授权，因此您可以将所有调查发现发送到 Security Hub，供所有客户使用。

如果您的某些客户尚未订阅 Security Hub，则 Security Hub 不会接收这些调查发现。它只会接收批次中经过授权的调查发现。

10.需要完成哪些步骤才能将调查发现发送到客户的 Security Hub 实例？

a. 确保采用正确的 IAM policy。

b. 为账户启用产品订阅（资源策略）。使用 `EnableImportFindingsForProduct` API 操作或集成页面。客户可以执行此操作，您也可以使用跨账户角色代表客户行事。

c. 确保调查发现的 `ProductArn` 是您产品的公有 ARN。

d. 确保调查发现的 `AwsAccountId` 是客户的账户 ID。

e. 根据 AWS 安全调查结果格式 (ASFF)，确保您的发现没有任何格式错误的数据。例如，必填字段均已填写，并且没有无效值。

f. 将调查发现分批发送到正确的区域端点。

11.我必须拥有哪些 IAM 权限才能发送调查发现？

必须为调用 `BatchImportFindings` 其他 API 调用的 IAM 用户或角色配置 IAM policy。

最简单的测试方法是使用管理员帐户执行此操作。您可以将其限制为 `action: 'securityhub:BatchImportFindings'` 和 `resource: <productArn and/or productSubscriptionArn>`。

同一账户中的资源可以使用 IAM policy 进行配置，而无需资源策略。

要排除调用方的 IAM policy 问题 `BatchImportFindings`，请按如下方式为调用方设置 IAM policy：

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

请务必检查有无针对调用方的 `Deny` 策略。在您使用它之后，便可将策略限制为以下内容：

```
{
    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'
}
```

12.什么是产品订阅？

要接收特定合作伙伴产品的调查发现，客户（或代表客户工作的具有跨账户角色的合作伙伴）必须订阅产品。要通过控制台执行此操作，客户需要使用集成 页面。要通过 API 执行此操作，则客户使用 EnableImportFindingsForProduct API 操作。

产品订阅会创建资源策略，授权客户接收或发送来自合作伙伴的调查发现。有关详细信息，请参阅使用场景和权限。

Security Hub 为合作伙伴制定了以下类型的资源策略：

- BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT
- BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT

在合作伙伴入驻过程中，您可以申请一种或两种类型的策略。

使用 BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT，您只能从您产品 ARN 中列出的账户向 Security Hub 发送调查发现。

使用 BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT，您只能从订阅您的客户账户发送调查发现。

13.假设客户创建了一个管理员帐户并添加了几个成员帐户。客户需要向我订阅每个成员账户吗？ 还是客户只需从管理员账户订阅，然后我就可以针对所有成员账户中的资源发送调查发现？

此问题问的是能否根据管理员账户的注册情况为所有成员账户创建权限。

客户必须为每个账户订阅产品。他们可以通过 API 以编程方式执行此操作。

14.我的产品 ARN 是什么？

您的产品 ARN 是 Security Hub 为您生成的唯一标识符，供您提交调查发现。每与 Security Hub 集成一款产品，您都会收到一个产品 ARN。您发送给 Security Hub 的每份调查发现都必须包含正确的产品 ARN。不包含产品 ARN 的调查发现将被删除。产品 ARN 使用以下格式：

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

示例如下：

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

对于部署了 Security Hub 的每个区域，您都会获得一个产品 ARN。账户 ID、公司和产品名称由您提交的合作伙伴清单决定。除了区域代码外，您绝不会更改与您产品 ARN 相关的任何信息。区域代码必须与您提交调查发现的区域相匹配。

一个常见错误是更改账户 ID，以匹配您当前使用的账户。账户 ID 不会改变。您提交含有“家庭”账户 ID 的清单。此账户 ID 已锁定在您的产品 ARN 中。

当 Security Hub 在新区域启动时，它会自动使用标准区域代码 ARNs 为这些区域生成您的产品。

每个账户还会自动配置私有产品 ARN。在收到官方公有产品 ARN 之前，您可以使用此 ARN 在自己的开发账户中测试导入调查发现。

15.向 Security Hub 发送调查发现应使用何种格式？

必须以 AWS 安全调查结果格式 (ASFF) 提供调查结果。有关详情，请参阅《AWS Security Hub 用户指南》中的 AWS 安全调查发现格式（ASFF）。

我们期望，您本机调查发现中的所有信息都能完全反映在 ASFF 中。自定义字段（例如 `ProductFields` 和 `Resource.Details.Other` ）允许您映射不完全适合预定义字段的数据。

16.哪个应使用的区域端点是正确的？

您必须将调查发现发送到关联了客户账户的 Security Hub 区域端点。

17.在哪里可以找到区域端点列表？

请参阅 Security Hub 端点列表。

18.我能否提交跨区域调查发现？

Security Hub 尚不支持跨区域提交原生 AWS 服务（例如亚马逊 GuardDuty、亚马逊 Macie 和 Amazon Inspector）的调查结果。如果您的客户允许，Security Hub 不会阻止您从不同区域提交调查发现。

从这个意义上讲，您可以从任何地方调用区域端点，而且 ASFF 的资源信息不必与端点区域相匹配。但是，`ProductArn` 必须与端点区域相匹配。

19.批量发送调查发现的规则和指导方针是什么？

在 `BatchImportFindings` 的单次调用中，您可以批处理多达 100 个或 240KB 的调查发现。排队并批量处理尽可能多的调查发现，但不超过此限制。

您可以批量分析来自不同账户的一组调查发现。但是，如果批次中有任何账户未订阅 Security Hub，则整个批次都将失败。这是 API Gateway 基准授权模型的局限性。

请参阅 the section called “BatchImportFindings API 的使用准则”。

20.我能否向我创建的调查发现发送更新？

可以，如果您提交具有相同产品 ARN 和相同调查发现 ID 的调查发现，它会覆盖该调查发现的先前数据。请注意，所有数据都将被覆盖，因此您应该提交完整的调查发现。

新调查发现和调查发现更新都会对客户进行计量和计费。

21.我能否向其他人创建的调查发现发送更新？

可以，如果客户授予您访问 `BatchUpdateFindings` API 操作的权限，则您可以使用该操作更新某些字段。此操作旨在供客户、 SIEMs票务系统以及安全编排、自动化和响应 (SOAR) 平台使用。

22.调查发现的过时机制是怎样的？

Security Hub 会将上次更新日期在 90 天前的调查发现视为已过时。此后，将从 Security Hub 集群中清除已过期的搜索结果。 OpenSearch

如果您使用相同的调查发现 ID 更新调查发现，而该调查发现已过时，则会在 Security Hub 中创建新的调查发现。

客户可以使用 CloudWatch 事件将发现结果移出 Security Hub。这样做可以将所有调查发现发送给客户选择的目标。

通常，Security Hub 建议您每 90 天创建一次新的调查发现，并且不要永远更新调查发现。

23.Security Hub 设置了哪些节流措施？

Security Hub 会限制 `GetFindings` API 调用，因为访问结果的推荐方法是使用 CloudWatch 事件。

除了 API Gateway 和 Lambda 调用强制执行的节流措施之外，Security Hub 不会对内部服务、合作伙伴或客户实施任何其他节流措施。

24.从源服务发送到 Security Hub 的调查结果的及时性、延迟时间 SLAs 或期望值如何？

我们的目标是尽可能实时地获取初步调查发现和最新调查发现。您应在创建调查发现后五分钟内将其发送到 Security Hub。

25.如何接收来自 Security Hub 的调查发现？

请使用以下任意一种方法接收调查发现。

- 所有发现的结果都会自动发送到 CloudWatch 活动。客户可以创建特定的 CloudWatch 事件规则，将调查结果发送到特定目标，例如 SIEM 或 S3 存储桶。此功能取代了传统的 `GetFindings` API 操作。
- 使用 CloudWatch 事件进行自定义操作。Security Hub 允许客户从控制台选择特定的调查发现或调查发现组并对其采取行动。例如，他们可以将调查发现发送到 SIEM、票务系统、聊天平台或修复工作流程。这将是客户在 Security Hub 中执行的警报分类工作流程的一部分。这些操作称为自定义操作。

  当用户选择自定义操作时，将针对这些特定发现创建一个 CloudWatch 事件。您可以利用此功能构建 CloudWatch 事件规则和目标，供客户在自定义操作中使用。请注意，此功能不用于将特定类型或类别的所有发现结果自动发送到 Ev CloudWatch ents。用户可以根据具体的调查发现采取行动。

  您可以使用自定义操作 API 操作（例如）自动为您的产品创建可用操作（例如使用 AWS CloudFormation 模板）。`CreateActionTarget`您还可以使用 CloudWatch 事件规则 API 操作来创建与自定义操作关联的相应 CloudWatch 事件规则。使用 AWS CloudFormation 模板，您还可以创建 CloudWatch 事件规则，自动从 Security Hub 获取所有发现或具有特定特征的所有发现。

26.托管安全服务提供商（MSSP）成为 Security Hub 合作伙伴的要求是什么？

您必须演示如何在向客户交付服务的过程中使用 Security Hub。

您应该准备用户文档来阐述您如何使用 Security Hub。

如果 MSSP 是调查发现提供商，则他们必须证明已将调查发现发送到 Security Hub。

如果 MSSP 只收到来自 Security Hub 的调查结果，则他们必须至少有一个 AWS CloudFormation 模板来设置相应 CloudWatch 的事件规则。

27.非 MSSP APN 咨询合作伙伴要成为 Security Hub 合作伙伴需要满足哪些条件？

如果您是 APN 咨询合作伙伴，您可以成为 Security Hub 合作伙伴。您应该提交两份私人案例研究，说明您如何帮助特定客户完成以下工作。

- 使用客户所需的 IAM 权限设置 Security Hub。
- 使用控制台合作伙伴页面上的配置说明，帮助将已经集成的独立软件供应商（ISV）解决方案连接到 Security Hub。
- 帮助客户进行定制产品集成。
- 生成与客户需求和数据集相关的自定义见解。
- 创建自定义操作。
- 制作修复行动手册。
- 构建符合 Security Hub 合规标准的快速入门程序。这些必须经过 Security Hub 团队的验证。

案例研究无需公开分享。

28.向客户部署我与 Security Hub 的集成有哪些要求？

Security Hub 与合作伙伴产品之间的集成架构因合作伙伴解决方案的运作方式而异。您应确保集成的设置过程不超过 15 分钟。

如果您要将集成软件部署到客户的 AWS 环境中，则应利用 AWS CloudFormation 模板来简化集成。一些合作伙伴创建了一键集成，这是我们强烈推荐的做法。

29.我的文档要求是什么？

您必须提供文档链接，说明您的产品与 Security Hub 之间的集成和设置过程，包括 AWS CloudFormation 模板的使用。

该文档还应包括您使用 ASFF 的相关信息。具体而言，您应在文档中列出不同调查发现所使用的 ASFF 调查发现类型。如果您拥有任何默认的见解定义，我们建议您也将其纳入文档中。

考虑纳入其他可能的信息：

- 您与 Security Hub 集成的使用案例
- 所发送调查发现的平均数量
- 您的集成架构
- 您支持和不支持的区域
- 从创建调查发现到将其发送到 Security Hub 之间的延迟
- 是否更新调查发现

30.什么是自定义见解？

我们鼓励您为自己的调查发现定义自定义见解。见解是一种轻量级关联规则，可帮助客户优先考虑哪些调查发现和资源最需要关注和采取行动。

Security Hub 拥有 `CreateInsight` API 操作。作为 AWS CloudFormation 模板的一部分，您可以在客户账户中创建自定义见解。这些见解将显示在客户的控制台上。

31.我可以提交控制面板小部件吗？

目前不可以。您只能创建托管见解。

32.您的定价模式是什么？

查看 Security Hub 的定价信息。

33.在集成的最终批准流程中，我应如何向 Security Hub 模拟账户提交调查发现？

使用您提供的产品 ARN 将调查发现发送到 Security Hub 模拟账户，并将 `us-west-2` 用作区域。调查发现应包括 ASFF `AwsAccountId` 字段中的模拟账户号码。要获取模拟账号，请联系 Security Hub 团队。

请勿向我们发送任何敏感数据或个人身份信息。此数据用于公开演示。您向我们发送这些数据，即表示您授权我们在演示中使用这些数据。

34.**`BatchImportFindings`** 提供了哪些错误或成功消息？

Security Hub 提供授权响应和 `BatchImportFindings` 响应。我们还在开发更多条理清晰的成功、失败和错误消息。

35.源服务负责处理哪些错误？

源服务负责处理所有错误。他们必须处理错误消息、重试、节流和警报。他们还必须处理通过 Security Hub 反馈机制发送的反馈或错误消息。

36.常见问题有哪些解决方法？

`AuthorizerConfigurationException` 是由格式错误的 `AwsAccountId` 或 `ProductArn` 造成的。

在问题排查期间，请注意以下要求：

- `AwsAccountId` 必须精确为 12 位数字。
- `ProductArn`必须采用以下格式：arn: aws: securityHub::: product//*<us-west-2 or us-east-1><accountId><company-id><product-id>*

  账户 ID 与 Security Hub 团队在提供给您的产品 ARNs 中包含的账号 ID 没有变化。

造成 AccessDeniedException 的原因是调查发现发送给或来自错误的账户，或者该账户没有 ProductSubscription。错误消息将包含资源类型为 product 或 product-subscription 的 ARN。此错误仅在跨账户调用期间出现。如果您在 AwsAccountId 和 ProductArn 中使用自己的账户为同一账户调用 BatchImportFindings，则该操作将使用 IAM policy 且与 ProductSubscriptions 无关。

请确保您使用的客户账户和产品账户是实际注册的账户。一些合作伙伴使用了产品 ARN 中的产品账号，但会尝试使用完全不同的账户调用 BatchImportFindings。在其他情况下，他们为其他客户账户甚至是为自己的产品账户创建 ProductSubscriptions。他们不为试图导入调查发现的客户账户创建 ProductSubscriptions。

37. 我应该向哪里发送问题、评论和错误？

<securityhub-partners@amazon.com>

38. 有关全球 AWS 服务的项目，我应该向哪个地区发送调查发现？ 例如，我应将与 IAM 相关的调查发现发送到哪里？

您应将调查发现发送到检测出调查发现的区域。对于 IAM 这类的服务，您的解决方案可能会在多个区域发现相同的 IAM 问题。在这种情况下，您应将调查发现发送到检测出问题的各个区域。

如果客户在三个区域运行 Security Hub，并在所有三个区域都检测出相同的 IAM 问题，您应将调查发现发送到所有三个区域。

问题解决后，您还应将调查发现的更新信息发送到您发送了原始调查发现的所有区域。

合作伙伴集成指南的文档历史记录

下表介绍了此指南的文档更新信息。

变更	说明	日期
更新了控制台徽标要求	更新了合作伙伴清单和徽标指南，指出合作伙伴必须同时提供浅色模式和深色模式的徽标版本，才能在 Security Hub 控制台上显示徽标。徽标必须是 SVG 格式。	2021 年 5 月 10 日
更新了成为新集成合作伙伴的前提条件	Security Hub 现在还允许已加入 AWS ISV 合作伙伴路径的合作伙伴，以及使用已完成 AWS 基础技术审查 (FTR) 的集成产品的合作伙伴。以前，所有整合合作伙伴都必须是 AWS 精选级别合作伙伴。	2021 年 4 月 29 日
ASFF 中的新 FindingProviderFields 对象	更新了有关将调查发现映射为 ASFF 的信息。对于 Confidence 、Criticality 、RelatedFindings 、Severity 以及 Types，合作伙伴将其值映射到 FindingProviderFields 中的字段。	2021 年 3 月 18 日
创建和更新调查发现的新原则	添加了一套用于在 Security Hub 中创建新调查发现和更新现有调查发现的新指南。	2020 年 12 月 4 日
此指南的初始版本	本《合作伙伴集成指南》为 AWS 合作伙伴提供了有关如	2020 年 6 月 23 日

何与之建立集成的信息 AWS Security Hub。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。