集成集成集成集成集成集成集成

AWS Security Hub

AWS Security Hub: 集成集成集成集成集成集成集成

Table of Contents

第三方集成概述AWS Security Hub

本指南适用于AWS希望创建集成的合作伙伴网络 (APN) 合作伙伴AWS Security Hub.

作为 APN 合作伙伴，您可以通过以下一种或多个方式与 Security Hub 集成。

- 将结果发送到 Security Hub
- 使用来自 Security Hub 的结果
- 两者都向 Security Hub 发送调查结果并使用安全中心
- 使用 Security Hub 作为托管安全服务提供商 (MSSP) 产品的中心
- 咨询AWS客户了解如何部署和使用 Security Hub

本载入指南主要侧重于将结果发送到 Security Hub 的合作伙伴。

主题

为什么要集成AWS Security Hub?

AWS Security Hub提供 Security Hub 帐户中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 发送安全调查结果，以便让客户深入了解您生成的安全调查结果。

与 Security Hub 的集成可以通过以下方式增加价值。

- 满足已请求 Security Hub 集成的客户
- 为您的客户提供他们的单一视图AWS安全相关结果
- 允许新客户在寻找提供与特定类型安全事件相关的调查结果的合作伙伴时发现您的解决方案

在构建与 Security Hub 的集成之前，请检查集成的原因。如果您的客户希望将 Security Hub 与您的产品集成，则集成更有可能成功。您可以完全出于营销原因或获取新客户来构建集成。但是，如果您在没有任何当前客户意见的情况下构建集成并且不考虑客户的需求，则集成可能无法产生预期的结果。

准备将结果发送到AWS Security Hub

作为 APN 合作伙伴，在 Security Hub 团队让您成为寻找提供商之前，您无法为客户发送信息到 Security Hub。要启用为查找提供商，您必须完成以下载入步骤。这样可以确保为您和您的客户提供积极的体验 Security Hub。

完成入职步骤后，请务必遵循中的指导原则the section called “创建和更新调查结果的原则”、the section called “ASFF 映射准则”, 和the section called “的使用准则BatchImportFindingsAPI”.

1. 将你的安全发现映射到AWSSecurity Fin 格式 (ASFF)。
2. 构建集成架构，将发现推送到正确的区域 Security Hub 终端节点。要做到这一点，你可以定义是否要发送自己的调查结果AWS账户或来自客户的账户内。
3. 让你的客户订阅产品到他们的账户。要执行此操作，他们可以使用控制台或EnableImportFindingsForProductAPI 操作。请参阅管理产品集成中的AWS Security Hub 用户指南.

   你也可以为他们订阅产品。要执行此操作，您可使用跨账户角色访问EnableImportFindingsForProduct代表客户执行 API 操作。

   此步骤建立了接受该账户产品的调查结果所需的资源策略。

以下博客文章讨论了与 Security Hub 的一些现有合作伙伴集成。

- 宣布云托管人集成AWS Security Hub
- 使用AWS Fargate和 Powler 发送安全配置调查结果AWS向 Security Hub 提供的服务
- 如何导入AWS ConfigSecurity Hub 中的结果将规则评估结果

准备接收来自的调查结果AWS Security Hub

接收来自的调查结果AWS Security Hub中，请使用以下选项之一：

- 让你的客户自动将所有发现发送到CloudWatch事件。客户可以创建特定的CloudWatch将调查结果发送到特定目标（例如 SIEM 或 S3 存储桶）的事件规则。
- 让您的客户从 Security Hub 控制台中选择特定的调查结果或调查结果组，然后对其采取措施。

例如，您的客户可以将调查结果发送到 SIEM、票务系统、聊天平台或修复工作流程。这将是客户在 Security Hub 内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，CloudWatch事件是针对这些特定发现创建的。作为合作伙伴，你可以利用这种能力并构建CloudWatch供客户在自定义操作中使用的事件规则或目标。请注意，此功能不会自动将特定类型或类的所有发现发送到CloudWatch事件。此功能供用户对具体的调查结果采取行动。

以下博客文章概述了使用与 Security Hub 集成的解决方案，CloudWatch自定义操作的事件。

- 如何集成AWS Security Hub使用自定义操作PagerDuty
- 如何在中启用自定义操作AWS Security Hub
- 如何导入AWS ConfigSecurity Hub 中的结果将规则评估结果

用于了解有关的资源AWS Security Hub

以下材料可以帮助你更好地理解AWS Security Hub解决方案和如何AWS客户可以使用该服务。

- 简介AWS Security Hub视频
- Security Hub 用户指南
- Security Hub API 参考
- 载入网络研讨会

我们还鼓励您在其中一个中启用 Security HubAWS账户并获得该服务的实践经验。

合作伙伴的

在开始集成之前AWS Security Hub，您必须满足下列条件之一：

- 你是AWS选择等级合作伙伴或以上。
- 你已经加入了AWSISV 合作伙伴路径，并且您用于 Security Hub 集成的产品已完成AWS基础技术评论 (FTR). 然后，该产品被授予 “审核者”AWS“徽章。

您还必须与之签订相互保密协议AWS.

集成使用案例和所需的权限

AWS Security Hub允许AWS客户将获得 APN 合作伙伴的调查结果。合作伙伴的产品可能在客户的内部或外部运行AWSaccount. 客户账户中的权限配置因合作伙伴产品使用的型号而异。

在 Security Hub 中，客户始终控制哪些合作伙伴可以向客户的账户发送调查结果。客户可以随时撤销合作伙伴的权限。

为了使合作伙伴能够向其帐户发送安全调查结果，客户首先在 Security Hub 中订阅合作伙伴产品。订阅步骤对于下面概述的所有使用案例都是必要的。有关客户如何管理产品集成的详细信息，请参阅管理产品集成中的AWS Security Hub用户指南.

客户订阅合作伙伴产品后，Security Hub 会自动创建托管资源策略。该政策授予合作伙伴产品使用BatchImportFindings将结果发送到 Security Hub 的 API 操作，以获取客户账户。

以下是与 Security Hub 集成的合作伙伴产品的常见案例。信息包括每个使用案例所需的额外权限。

合作伙伴托管：从合作伙伴账户发送

本使用案例涵盖自己托管产品的合作伙伴AWSaccount. 要发送安全结果AWS客户，合作伙伴致电BatchImportFindings合作伙伴产品账户的 API 操作。

对于此使用案例，客户帐户只需要在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BatchImportFindingsAPI 操作必须具有相应的 IAM 策略，允许委托人调用BatchImportFindings.

使合作伙伴产品能够在 Security Hub 中向客户发送调查结果有两个步骤：

1. 客户在 Security Hub 中创建合作伙伴产品的订阅。
2. Security Hub 会在客户确认的情况下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结果，合作伙伴产品使用自己的凭据来调用BatchImportFindingsAPI 操作。

以下是一个 IAM 策略的示例，该策略向合作伙伴账户中的委托人授予必要的 Security Hub 权限。

```
{
```

```
    "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"
        }
    ]
}
```

合作伙伴托管：客户账户发送的调查结果

本使用案例涵盖自己托管产品的合作伙伴AWS账户，但是使用跨账户角色访问客户的账户。他们调用BatchImportFindings来自客户账户的 API 操作。

对于此使用案例，请调用BatchImportFindingsAPI 操作，合作伙伴账户在客户账户中承担客户托管的 IAM 角色。

这个电话来自客户的账户。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 托管资源策略授予合作伙伴产品帐户和合作伙伴产品 ARN 的权限。产品 ARN 是合作伙伴作为提供商的唯一标识符。由于呼叫不是来自合作伙伴产品帐户，因此客户必须明确授予合作伙伴产品向 Security Hub 发送调查结果的权限。

合作伙伴和客户账户之间的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。授予时，外部标识符提供了一个额外的安全层AWS合作伙伴的账户访问权限。唯一标识符可确保合作伙伴使用正确的客户账户。

通过四个步骤，使合作伙伴产品能够在 Security Hub 中以跨账户角色向客户发送调查结果：

1. 客户或使用代表客户工作的跨账户角色的合作伙伴，在 Security Hub 中开始订阅产品。
2. Security Hub 会在客户确认的情况下生成正确的托管资源策略。
3. 客户可以手动配置跨账户角色，也可以使用AWS CloudFormation. 有关跨账户角色的信息，请参阅提供访问权限AWS第三方拥有的账户中的IAM 用户指南.
4. 产品可以安全地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. 该产品称之为AWS Security Token Service(AWS STS) 承担客户角色。
2. 该产品称之为BatchImportFindings使用担任角色的临时证书在 Security Hub 上进行 API 操作。

以下是一个 IAM 策略的示例，该策略向合作伙伴的跨账户角色授予必要的 Security Hub 权限。

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

这些区域有：Resource策略的部分标识了特定的产品订阅。这可确保合作伙伴只能发送客户订阅的合作伙伴产品的调查结果。

客户托管：来自客户账户的调查结果

本使用案例涵盖了在客户的中部署了产品的合作伙伴AWSaccount. 这些区域有：BatchImportFindingsAPI 是从客户账户中运行的解决方案调用的。

对于此使用案例，必须向合作伙伴产品授予其他权限才能调用BatchImportFindingsAPI。授予此权限的方式取决于合作伙伴解决方案以及在客户账户中的配置方式。

这种方法的一个示例是在客户账户中的 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，该角色授予该实例调用BatchImportFindingsAPI 操作。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调查结果加载到他们所拥有的产品的帐户中的场景。

客户使合作伙伴产品能够在 Security Hub 中将客户账户中的调查结果发送给客户：

1. 客户将合作伙伴产品部署到他们的AWS手动使用账户AWS CloudFormation，或者另一种部署工具。

2. 客户定义了合作伙伴产品在向 Security Hub 发送调查结果时使用的必要 IAM 策略。
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，该产品可以将结果发送到 Security Hub：

1. 合作伙伴产品使用AWS开发工具包AWS CLI调用BatchImportFindingsSecurity Hub 的 API 操作。它从附加保单的客户账户中的组件拨打电话。
2. 在 API 调用期间，将生成必要的临时证书以允许BatchImportFindings调用成功。

以下是 IAM 策略的示例，该策略向客户账户中的合作伙伴产品授予必要的 Security Hub 权限。

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

合作伙伴启动过程

作为合作伙伴，作为入职流程的一部分，您可以期望完成几个高级步骤。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. 您启动了与 APN 合作伙伴团队或 Security Hub 团队的接触，并表示有兴趣成为 Security Hub 的合作伙伴。您可以确定要添加到 Security Hub 通信渠道的电子邮件地址。
2. AWS为您提供 Security Hub 合作伙伴入职资料。
3. 您被邀请加入 Security Hub 合作伙伴 Slack 频道，在那里你可以提出与集成相关的问题。
4. 您向 APN 合作伙伴联系人提供产品集成清单草稿以供审核。

   产品集成清单包含用于创建合作伙伴产品的信息亚马逊资源名称 (ARN) 以进行集成AWS Security Hub.

   它为 Security Hub 团队提供了显示在 Security Hub 控制台的合作伙伴提供商页面上的信息。它还用于提出与集成相关的新托管见解，以添加到 Security Hub 洞察库中。

   此初始版本的产品集成清单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 团队为您的产品提供产品 ARN。您将结果发送到 Security Hub 将结果发送到 Security Hub。
6. 您构建集成以向 Security Hub 发送调查结果或从 Security Hub 接收调查结果。

   将调查结果映射到 ASFF

   要将调查结果发送到 Security Hub，您必须将调查结果映射到AWSSecurity Fend 格式 (ASFF)。

   ASFF 提供了一致的调查结果描述，可以在之间共享AWS安全服务、合作伙伴和客户安全系统。这减少了整合努力，鼓励使用共同语言，并为实施者提供了蓝图。

   ASFF 是将调查结果发送到所需的有线协议格式AWS Security Hub. 调查结果表示为遵循 ASFF JSON 模式和 RFC-7493 I-JSON 消息格式的 JSON 文档。有关 ASFF 架构的详细信息，请参阅AWSSecurity Finding 格式 (ASFF)中的AWS Security Hub用户指南.

   请参阅the section called “ASFF 映射准则”。

构建和测试集成

您可以使用AWS您拥有的账户。这样做可以让你完全了解发现在 Security Hub 中的显示方式。它还可以帮助您了解客户对安全调查结果的体验。

您将BatchImportFindings将新结果和更新结果发送到 Security Hub 的 API 操作。

在构建 Security Hub 集成的过程中，AWS鼓励您随时向 APN 合作伙伴联系人通报集成进度。您还可以向 APN 合作伙伴联系人寻求有关集成问题的帮助。

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

7. 你演示了与 Security Hub 产品团队的集成。必须使用 Security Hub 团队拥有的帐户来证明此集成。

   如果他们对集成感到满意，Security Hub 团队将批准继续将您列为提供商。
8. 你提供AWS附有最终清单供审查。
9. Security Hub 团队在 Security Hub 控制台中创建提供商集成。然后，客户可以发现并启用集成。
10. （可选）您参与额外的营销工作来促进 Security Hub 集成。请参阅Go-to-market活动。

    至少，Security Hub 建议您提供以下资产。
    - 工作集成的演示视频（最多 3 分钟）。该视频用于营销目的，并发布到AWS YouTubechannel。
    - 要添加到 Security Hub 首次调用幻灯片组的单幻灯片架构图。

Go-to-market活动

合作伙伴还可以参与可选的营销活动来帮助解释和推广他们的AWS Security Hub集成。

如果您想创建自己的与 Security Hub 相关的营销内容，请在发布内容之前向 APN 合作伙伴经理发送草稿以供审核和批准。这可以确保每个人都在消息上保持一致。

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) 计划创建广告活动并获得资金支持。有关这些计划的详细信息，请联系合作伙伴经理。

Security Hub 合作伙伴页面上的条目

获准成为 Security Hub 合作伙伴后，您的解决方案可以显示在AWS Security Hub合作伙伴页.

要在此页面上列出，请向 APN 合作伙伴联系人提供以下详细信息。这可能是您的合作伙伴开发经理 (PDM)、合作伙伴解决方案架构师 (PSA)，也可以是发送给<securityhub-pms@amazon.com>.

- 简要描述您的解决方案、它与 Security Hub 的集成以及与 Security Hub 的集成为客户提供的价值。此描述限制为 700 个字符，包括空格。
- 指向描述解决方案的页面的 URL。这个网站应该是特定于你的AWS集成，更具体地说是您的 Security Hub 集成。它应重点关注客户体验和客户在使用集成时获得的价值。
- 徽标的高分辨率副本，大小为 600 x 300 像素。有关此徽标要求的详细信息，请参阅the section called “合作伙伴徽标页面”.

新闻稿

作为获得批准的合作伙伴，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，必须将其提交至AWS供 APN 合作伙伴营销、Security Hub 领导层审核以及AWS外部安全服务（ESS）。新闻稿可以包括就业服务局副总裁的建议报价。

要启动此过程，请使用 PDM。我们有 10 个工作日的服务级别协议 (SLA) 来查看新闻稿。

AWS合作伙伴网络 (APN) 博客

我们还可以帮助你发布你创作到 APN 博客的博客条目。博客条目必须侧重于客户故事和使用案例。它不能仅仅围绕成为集成启动合作伙伴来定位。

如果你有兴趣，请联系你的 PDM 或 PSA 开始该过程。APN 博客可能需要 8 周或更长时间才能获得最终批准和发布。

关于 APN 博客的关键事情

创建博客文章时，请记住以下内容。

博客文章中有什么？

合作伙伴帖子应具有教育意义，并提供与以下相关主题的深入AWS顾客。

理想的长度不超过 1,500 个单词。读者重视深度的教育内容，可以教他们什么AWS.

内容应该是 APN 博客的原创内容。不要重新调整来自现有博客文章或白皮书等来源的内容的用途。

在 APN 博客上发布的其他限制是什么？

只有高级或高级级别合作伙伴才能发布到 APN 博客。对于具有 APN 计划名称（例如服务交付）的精选合作伙伴，有例外情况。

每个合作伙伴每年限于三个帖子。拥有成千上万的 APN 合作伙伴，AWS其覆盖范围必须是公平的.

每篇文章都必须有一位能够验证解决方案或使用案例的技术赞助商。

在发布博客文章之前编辑博客文章需要多长时间？

提交博客文章的第一份完整草稿后，编辑需要四到六周的时间。

为什么要为 APN 博客写？

APN 博客文章可以带来以下好处。

- 信誉— 对于 APN 合作伙伴，有故事发布AWS可以影响全球客户。
- Visibility— APN 博客是阅读量最多的博客之一AWS2019 年有 179 万个页面浏览量，包括受影响的流量。
- 业务— APN 合作伙伴帖子具有连接按钮，可以通过 APN 客户互动 (ACE) 计划生成潜在客户。

什么类型的内容最适合？

以下类型的内容最适合 APN 博客文章。

- 技术内容是最受欢迎的故事类型。这包括解决方案聚光灯和操作方法信息。超过 75% 的读者查看此技术内容。
- 客户重视 200 级或更高级别的故事，这些故事展示了某些东西AWS或者 APN 合作伙伴如何为客户解决业务问题。
- 迄今为止，技术专家或主题专家撰写的帖子表现最好。

光滑的表格或营销表

光滑的表格是一个单页的文档，它概述了您的产品、其集成架构和联合客户使用案例。

如果您为集成创建光滑的表格，请将副本发送给 Security Hub 团队。他们会将其添加到合作伙伴页面。

白皮书或电子书

如果您创建白皮书或电子书，概述产品、其集成架构和联合客户使用案例，请向 Security Hub 团队发送一份副本。他们会将其添加到 Security Hub 合作伙伴页面。

网络研讨会

如果您确实举办了有关集成的网络研讨会，请将网络研讨会的录像发送给 Security Hub 团队。团队将从合作伙伴页面链接到它。

该团队还可以提供 Security Hub 主题专家参加您的网络研讨会。

演示视频

出于营销目的，您可以制作有关工作集成的演示视频。在您的视频平台帐户上发布此类视频，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产品集成清单，为拟议的集成提供所需的详细信息。

Security Hub 团队通过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
- 将您的使用案例通知产品团队。

为了评估拟议集成的质量和所提供的信息，Security Hub 团队使用the section called “产品准备核对清”. 此清单确定您的集成是否已准备就绪，可以启动了。

您提供的所有技术信息也必须反映在您的文档中。

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，合作伙伴页面在中国（北京）和中国（宁夏）区域推出。

目录

- AWS Security Hub控制台信息
  - 公司信息
  - 产品信息

用例和营销信息

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用例

独立软件供应商 (ISV) 是必需的。

要描述与集成的用例AWS Security Hub，请回答以下问题。如果您不打算发送或接收调查结果，请注意本节中的内容，然后完成下一节。

以下信息必须反映在您的文档中。

- 你会发送调查结果、接收调查结果还是两者兼而有之？
- 如果您计划发送调查结果，您将发送哪些类型的调查结果？ 你会发送所有调查结果还是调查结果的特定子集？
- 如果你计划收到调查结果，你会如何处理这些发现？ 你会收到什么类型的发现？ 例如，您会收到所有调查结果、特定类型的调查结果，还是仅收到客户选择的特定调查结果？
- 你打算更新调查结果吗？ 如果是，你会更新哪些字段？ Security Hub 建议你更新调查结果，而不是总是创建新的发现。更新现有调查结果有助于减少客户的搜索噪音。

  要更新查找结果，您发送的查找结果包含已分配给已发送的查找结果的查找结果 ID。

要尽早获得有关您的用例和数据集的反馈，请联系 APN 合作伙伴或 Security Hub 团队。

咨询合作伙伴 (CP) 用例

如果您是 Security Hub 咨询合作伙伴，则为必填项。

为你使用 Security Hub 提供两个客户用例。这些可以是私人用例。Security Hub 团队不会在任何地方为它们做广告。它们应描述以下一个或两个操作。

- 你如何帮助客户引导 Security Hub？ 例如，你有没有帮助客户使用专业服务、Terraform 模块或 AWS CloudFormation模板？

- 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补救模板、构建了自定义集成，或者使用商业智能工具设置了管理控制面板？

数据集

如果您将结果发送到 Security Hub 时必需。

对于您将发送到 Security Hub 的调查结果，请提供以下信息。

- 调查结果采用其原生格式，例如 JSON 或 XML
- 您如何将结果转换为 Security HindinAWS g (ASFF) 的示例

如果您需要更新 ASFF 以支持集成，请告知 Security Hub 团队。

架构

如果您向 Security Hub 发送调查结果或接收结果时必需。

描述您将如何与 Security Hub 集成。这些信息还必须反映在您的文档中。

您必须提供架构图。在准备您的架构图时，请注意以下事项：

- 您将使用哪些AWS服务、操作系统代理等？
- 如果您要向 Security Hub 发送调查结果，您会从客户AWS账户还是从您自己的AWS账户发送调查结果？
- 如果您将收到调查结果，您将如何使用 CloudWatch 活动集成？
- 你将如何将发现结果转换为 ASFF？
- 您将如何对发现结果进行批处理、跟踪查找状态并避免限制限制？

配置

如果您向 Security Hub 发送调查结果或接收结果时必需。

描述客户将如何配置您与 Security Hub 的集成。

您至少必须使用AWS CloudFormation模板或类似的基础架构，例如代码模板。一些合作伙伴提供了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集成提供配置指导。

每位客户每天的平均发现结果

如果您将结果发送到 Security Hub 时必需。

您预计每月向整个客户群的 Security Hub 发送多少查找更新（平均值和最大值）？ 数量级估计是可以接受的。

延迟

如果您将结果发送到 Security Hub 时必需。

您能以多快的速度将结果发送到 Security Hub？ 换句话说，从在您的产品中创建查找结果到将其发送到 Security Hub 的延迟是多少？

这些信息必须反映在您的产品文档中才能进行集成。这是客户的常见问题。

公司和产品描述

与 Security Hub 的所有集成都是必需的。

简要描述您的公司和产品，特别强调您的 Security Hub 集成的性质。我们在 Security Hub 合作伙伴页面上使用此功能。

如果您要将多个产品与 Security Hub 集成，则可以为每种产品提供单独的描述，但我们会将它们合并为合作伙伴页面上的单个条目。

每个描述不能超过 700 个字符，包含空格。

合作伙伴网站资产

与 Security Hub 的所有集成都是必需的。

您必须至少提供一个用于 Security Hub 合作伙伴页面上的 “了解更多” 超链接的 URL。它应该是一个营销登录页面，描述您的产品与SSecurity 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 建议此登录页面包含指向您的配置说明的链接。

您还可以提供其他资源的链接，例如博客、网络研讨会、演示视频或白皮书。Security Hub 还将链接到其合作伙伴页面上的链接。

合作伙伴徽标页面

所有 Security Hub 集成都是必需的。

提供要显示在 Security Hub 合作伙伴页面上的徽标的 URL。徽标必须满足以下条件：

- 尺寸：600 x 300 像素
- 裁剪：紧身，没有填充物
- 背景：透明
- 格式：PNG

Security Hub 控制台标

所有集成都是必需的。

提供要在 Security Hub 控制台上显示的浅色模式和深色模式徽标的 URL。

徽标必须满足以下条件：

- 格式：SVG
- 尺寸：175 x 40 像素。如果较大，则图像应使用该比例。
- 裁剪：紧身，无填充
- 背景：透明

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

查找类型

如果您将结果发送到 Security Hub 时必需。

提供一个表格，记录您使用的 ASFF 格式的查找结果类型以及它们如何与您的原生查找结果类型对齐。有关在 ASFF 中查找类型的详细信息，请参阅《AWS Security Hub用户指南》中的 ASFF 类型分类。

建议您还需要在产品文档中包含此信息。

热线

与 Security Hub 的所有集成都是必需的。

为技术联系人提供电子邮件地址和电话号码或寻呼机号码。Security Hub 将就任何技术问题（例如集成不再起作用时）与该联系人进行沟通。

还为高度严重的技术问题提供全天候联系人。

发现心跳

如果您将结果发送到 Security Hub，建议使用。

你能否每五分钟向 Security Hub 发送一次 “心跳信号”，表明你与 Security Hub 的集成正常运行？

如果可以，则使用查找类型来执行此操作`Heartbeat`。

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，并将您提议的托管见解包含在 Security Hub 洞察库中。

公司信息

公司信息提供有关贵公司的信息。示例如下：

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

公司信息包含以下字段：

字段	必填	描述
`id`	是	公司的唯一标识符。公司标识符在公司中必须唯一。 这可能与之相同或相似`name`。 类型：字符串 最小长度：5 个字符

字段	必填	描述
		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	将在 Security Hub 控制台上显示的提供商公司的名称。 类型：字符串 最大长度：16 个字符
description	是	提供商公司的描述将显示在 Security Hub 控制台上。 类型：字符串 最大长度：200 个字符

产品信息

本节提供有关您的产品的信息。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	必填	描述
IntegrationType	是	表明您的产品是向 Security Hub 发送调查结果，还是接收来自 Security Hub 的调查结果，还是同时发送和接收调查结果。 如果您是咨询合作伙伴，请将此字段留为空白。 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。它们在公司中必须唯一。它们不必在公司中唯一。这可能与... 相同或相似name。 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，在哪些区域，Security Hub 不应该在 Security Hub 控制台的合作伙伴页面上将你显示为选项？ 类型：字符串 仅提供区域代码。例如，us-west-1 。 有关区域列表，请参阅中的区域终端节点AWS一般参考。

字段	必填	描述
		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 （用于AWS GovCloud（美国东部））。 中国区域的区域代码是cn-north-1 （对于中国（北京））和cn-northwest-1 （对于中国（宁夏））。
commercialAccountNumber	是	该产品在各AWS地区的主要AWS账号。 如果您向 Security Hub 发送调查结果，则您提供的账户取决于您发送调查结果的来源。 • 来自您的AWS账户。在这种情况下，请提供您用来提交调查结果的账号。 • 来自客户的AWS账户。在这种情况下，Security Hub 建议您提供用于测试集成的主账户号。 理想情况下，您将为所有地区的所有产品使用同一个账户。如果不可能，请联系 Security Hub 团队。 如果您只收到来自 Security Hub 的调查结果，则不需要此帐号。 类型：字符串

字段	必填	描述
govcloudAccountNumber	否	AWS GovCloud (US)各地区产品的主要AWS账号（如果您的产品有售AWS GovCloud (US)）。 如果您向 Security Hub 发送调查结果，则您提供的账户取决于您发送调查结果的来源。 • 来自您的AWS账户。在这种情况下，请提供您用来提交调查结果的账号。 • 来自客户的AWS账户。在这种情况下，Security Hub 建议您提供用于测试集成的主账户号。 理想情况下，您对所有AWS GovCloud (US)地区的所有产品使用同一个账户。如果不可能，请联系 Security Hub 团队。 如果您只收到来自 Security Hub 的调查结果，则不需要此帐号。 类型：字符串

字段	必填	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）。 如果您向 Security Hub 发送调查结果，则您提供的账户取决于您发送调查结果的来源。 • 来自您的AWS账户。在这种情况下，请提供您用来提交调查结果的账号。 • 来自客户的AWS账户。在这种情况下，Security Hub 建议您提供用于测试产品集成的主要账户号码。 理想情况下，您在中国所有地区的所有产品都使用同一个账户。如果不可能，请联系 Security Hub 团队。 如果您只收到来自 Security Hub 的调查结果，则可以是您在中国地区拥有的任何账户。 类型：字符串
name	是	要在 Security Hub 控制台上显示的提供商产品的名称。 类型：字符串 最大长度：24 个字符
description	是	要在 Security Hub 控制台上显示的提供商产品的描述。 类型：字符串 最大长度：200 个字符

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

字段	必填	描述
category	是	定义您的产品的类别。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缺失，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	必填	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	必填	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	您的商品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 URL。 如果您没有AWS Marketplace清单，请将此字段留为空白。

字段	必填	描述
`configurationUrl`	是	您的产品文档的 URL，有关与 Security Hub 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） • 有关您的集成用例的信息 • 延迟 • ASFF 映射 • 发现结果类型包括 • 架构

准则和核对清单

当你为你准备所需的材料AWS Security Hub集成，请使用这些准则。

准备情况清单用于在 Security Hub 向 Security Hub 客户提供集成之前对集成进行最终审查。

主题

将徽标显示在AWS Security Hub控制台

要显示在AWS Security Hub控制台，请遵循以下准则。

光明和黑暗模式

您必须同时提供灯光模式和黑暗模式的徽标版本。

格式

SVG 文件格式

Background color

Transparent

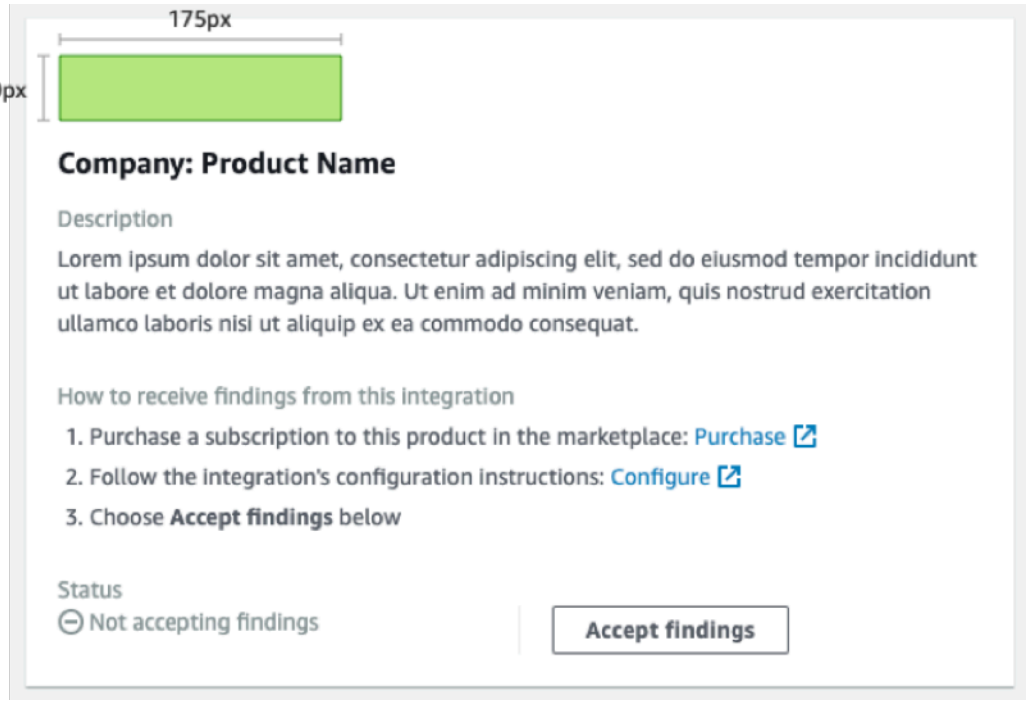
Size

理想的比例为 175 像素宽 x 40 像素高。

最小高度为 40 px。

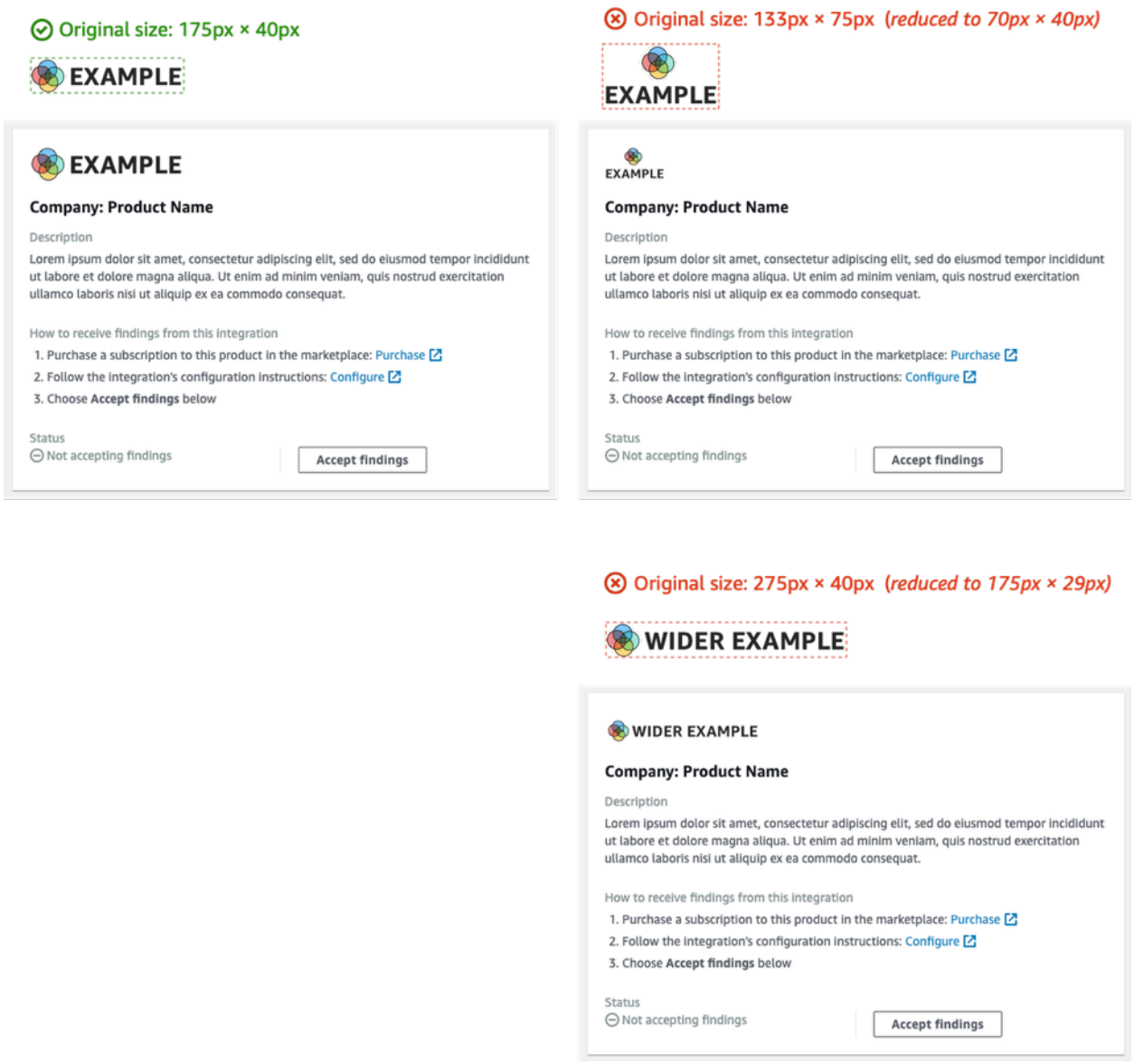
矩形徽标效果最好。

下图显示 Security Hub 控制台上如何显示理想徽标。



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 px，最大宽度为 175 px。这会影响徽标在 Security Hub 控制台上的显示方式。

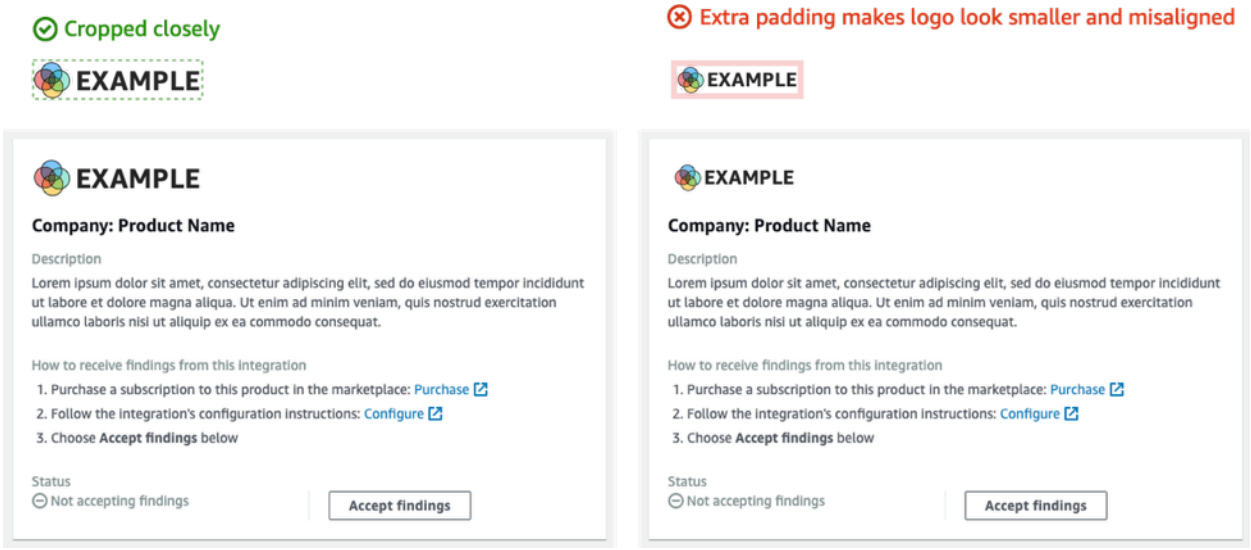
下图将使用理想尺寸的徽标的显示与更宽或更高的徽标进行了比较。



裁剪

尽可能靠近裁剪徽标图像。不要提供额外的填充物。

下图显示了紧密裁剪的徽标与具有额外填充的徽标之间的区别。



创建和更新调查结果的原则

在计划如何在中创建和更新结果时AWS Security Hub，请注意以下原则：

使结果具体化，以便客户可以轻松对其采取相应措施。

客户希望自动执行响应和补救措施，并将调查结果与其他发现相关联。为了支持这一点，结果应具有以下特征：

- 他们通常应该处理单个资源或主要资源。
- 他们应该有一种查找类型。
- 他们应该处理单个安全事件。

当调查结果包含多个安全事件的数据时，客户就更难对该调查结果采取行动。

将所有查找字段映射到AWSSecurity Found 格式 (ASFF)。允许客户依靠 Security Hub 作为真相的来源。

客户预计，Security Hub ASFF 中也会显示您原生查找格式的每个字段。

客户希望所有数据都出现在该调查结果的 Security Hub 版本中。缺少数据会导致他们对作为安全信息的核心来源的 Security Hub 失去信任。

尽量减少发现的冗余。不要因寻找数量而压倒客户。

Security Hub 不是一个通用的日志管理工具。您应该向 Security Hub 发送高度可操作的调查结果，客户可以直接响应、补救或与其他调查结果相关联。

当查找结果只有微小变化时，请更新查找结果，而不是创建新的查找结果。

当调查结果（例如严重性分数或资源标识符）发生重大变化时，请创建一个新的查找结果。

例如，实时为单个端口扫描创建查找结果并不具有高度可操作性。由于端口扫描可以持续进行，因此会产生大量的发现。更具吸引力和精确的做法是简单地更新上次扫描时间并在 TOR 节点上对 MongoDB 端口进行端口扫描的单个发现进行扫描。

允许客户自定义他们的发现，使其更有意义。

客户希望能够调整某些查找字段，使其与其环境或要求更相关。

例如，客户希望能够根据账户类型或查找结果关联的资源类型添加备注、标签和调整严重性分数。

将调查结果映射到AWSSecurity Finding 格式 (ASFF)

使用以下准则将您的结果映射到 ASFF。有关每个 ASFF 字段和对象的详细说明，请参阅AWSSecurity Finding 格式 (ASFF)中的AWS Security Hub用户指南.

识别信息

`SchemaVersion` 始终为 `2018-10-08`。

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

`Id`是 Security Hub 用来索引发现的值。查找结果标识符必须是唯一的，以确保其他调查结果不会被覆盖。要更新调查结果，请使用相同标识符重新提交查找结果。

`GeneratorId`可以是一样的`Id`或者可以参考离散的逻辑单元，例如亚马逊GuardDuty探测器 ID，AWS Config记录器 ID 或 IAM 访问分析器 ID。

Title 和 Description

`Title`应包含有关受影响资源的一些信息。`Title`包括空格在内的长度限制为 256 个字符。

将更长的详细信息添加到`Description`.`Description`包括空格在内的长度限制为 1024 个字符。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.",
```

查找类型

您在中提供了查找类型信息FindingProviderFields.Types.

Types应该匹配ASFF 的类型分类.

如果需要，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

你必须提交CreatedAt和UpdatedAt每次打电话BatchImportFindings对于每个发现。

这些值必须与 Python 3.8 中的 ISO8601 格式匹配。

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

FirstObservedAt 和 LastObservedAt

FirstObservedAt和LastObservedAt系统观察到发现的时候必须匹配。如果您不记录此信息，则无需提交这些时间戳。

这些值与 Python 3.8 中的 ISO8601 格式匹配。

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

Severity

您可以在FindingProviderFields.Severity对象，其中包含以下字段。

Original

系统中的严重性值。Original可以是任意字符串，以容纳你使用的系统。

`Label`

查找严重性的所需 Security Hub 指示器。允许的值如下所示。

- `INFORMATIONAL`— 未发现任何问题。
- `LOW`— 问题不需要单独采取任何措施。
- `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，以防止进一步的伤害。

合规的调查结果应始终具有`Label`设置为`INFORMATIONAL`. 示例`INFORMATIONAL`调查结果是通过安全检查的结果和AWS Firewall Manager得到补救的调查结果。

客户经常按严重程度对发现进行排序，以便为安全运营团队提供待办事项清单。将查找严重性设置为时要保守`HIGH`要么`CRITICAL`.

您的集成文档必须包括映射的理由。

Remediation

`Remediation`有两个元素。这些元素组合在 Security Hub 控制台上。

`Remediation.Recommendation.Text`显示在补救措施查找细节的部分。它与的价值超链接`Remediation.Recommendation.Url`.

目前，只有来自 Security Hub 标准、IAM 访问分析器和 Firewall Manager 的调查结果显示有关如何修复发现的文档的超链接。

SourceUrl

只能使用`SourceUrl`是否可以为该特定发现提供一个深度链接的 URL 到控制台。否则，请从映射中省略它。

Security Hub 不支持来自此字段的超链接，但它显示在 Security Hub 控制台上。

Malware, Network, Process, ThreatIntelIndicators

如果适用，请使用`Malware`、`Network`、`Process`，或者`ThreatIntelIndicators`. 这些对象中的每个都在 Security Hub 控制台中公开。在您发送的查找结果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 EC2 实例的详细信息`Resource.Details.AwsEc2Instance`. 提供相关的`Malware`、`Network`, 和`ThreatIntelIndicator`EC2 实例的对象。

Malware

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

每个条目都包含以下字段。

`Name`

恶意软件的名称。值是最多 64 个字符的字符串。

`Name`应该来自经过审查的威胁情报或研究人员来源。

`Path`

通向恶意软件的路径。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，那么`Path`是 S3://或 HTTPS 对象路径。
- 如果你扫描 Git 存储库中的文件，那么`Path`是 Git URL 或克隆路径。

`State`

恶意软件的状态。允许的值为`OBSERVED| REMOVAL_FAILED|REMOVED`.

在查找标题和描述中，确保提供恶意软件发生的情况的上下文。

例如，如果`Malware.State`是`REMOVED`，那么查找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`，那么查找标题和描述应反映出您的产品遇到了位于路径上的此恶意软件。

`Type`

指示恶意软件的类型。允许的值为`ADWARE|BLENDED_THREAT|BOTNET_AGENT|COIN_MINER|EXPLOIT_KIT|KEYLOGGER|MACRO|POTENT`

如果你需要额外的价值`Type`，请联系 Security Hub 团队。

Network

Network是单个对象。不能添加多个与网络相关的详细信息 在映射字段时，请使用以下准则。

目的地和来源信息

目标和源很容易映射 TCP 或 VPC 流日志或 WAF 日志。当你描述网络信息以获得攻击的发现时，它们更难以使用。

通常，来源是攻击的起源，但它可能有下面列出的其他来源。你应该在文档中解释来源，并在查找标题和描述中对其进行描述。

- 对于 EC2 实例的 DDoS 攻击，来源是攻击者，尽管真正的 DDoS 攻击可能会使用数百万台主机。目标是 EC2 实例的公有 IPv4 地址。Direction在。
- 对于观察到从 EC2 实例与已知命令和控制节点进行通信的恶意软件，源是 EC2 实例的 IPV4 地址。目的地是命令和控制节点。Direction是OUT. 你还会提供Malware和ThreatIntelIndicators.

Protocol

Protocol除非您可以提供特定协议，否则始终映射到互联网号码分配机构 (IANA) 的注册名称。你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。只有在有意义的时候才提供它。

Direction

Direction总是相对于AWS网络边界。

- IN意味着它正在进入AWS（VPC、服务）。
- OUT意味着它正在退出AWS网络边界。

Process

Process是单个对象。不能添加多个与流程相关的详细信息 在映射字段时，请使用以下准则。

Name

Name应与可执行文件的名称匹配。最多可接受 64 个字符。

Path

Path是进程可执行文件的文件系统路径。它最多可接受 512 个字符。

Pid, **ParentPid**

Pid和ParentPid应与 Linux 进程标识符 (PID) 或 Windows 事件 ID 匹配。要区分，请使用 EC2 Amazon 系统映像 (AMI) 提供信息。客户可能可以区分 Windows 和 Linux。

时间戳 (**LaunchedAt**和**TerminatedAt**)

如果您无法可靠地检索此信息，并且不准确到毫秒，请不要提供它。

如果客户依赖时间戳进行取证调查，那么没有时间戳比具有错误的时间戳更好。

ThreatIntelIndicators

ThreatIntelIndicators接受最多包含 5 个威胁情报对象的数组。

对于每个条目，Type是在具体威胁的背景下。允许的值为DOMAIN|EMAIL_ADDRESS|HASH_MD5|HASH_SHA1|HASH_SHA256|HASH_SHA512|IPV4_ADDRESS|IPV6_A

以下是一些如何映射威胁情报指标的示例：

- 你发现了一个你知道与 Cobalt Strike 有关的过程。你从中学到了FireEye的博客。

  将 Type 设置为 PROCESS。还可以创建Process该进程的对象。
- 您的邮件过滤器发现有人从已知恶意域发送了众所周知的哈希包。

  创建两个ThreatIntelIndicator对象。一个对象是用于DOMAIN. 另一个是用于HASH_SHA1.
- 你发现了带有 Yara 规则的恶意软件（洛基、Fenrir、Ass3VirusScan、BinaryAlert)。

  创建两个ThreatIntelIndicator对象。其中一个是恶意软件。另一个是用于HASH_SHA1.

Resources

适用于Resources，尽可能使用我们提供的资源类型和详细信息字段。Security Hub 不断向 ASFF 添加新资源。要获取 ASFF 变更的月度日志，请联系<securityhub-partners@amazon.com>.

如果您不能适合模型化资源类型的详细信息字段中的信息，请将其余详细信息映射到Details.Other.

对于 ASFF 中未建模的资源，请设置Type到Other. 有关详细信息，请使用Details.Other.

您也可以使用Other非-的资源类型AWS结果。

ProductFields

只能使用ProductFields如果你不能使用另一个策划的字段Resources或描述性对象，例如ThreatIntelIndicators、Network，或者Malware.

如果你确实使用ProductFields，你必须为此决定提供严格的理由。

Compliance

只能使用Compliance如果你的调查结果与合规性有关。

Security Hub 使用Compliance因为它根据控件生成的调查结果。

Firewall Manager 使用Compliance因为它们与合规性有关。

受限的字段

这些字段旨在让客户跟踪他们对调查结果的调查。

不要映射到这些字段或对象。

- Note
- UserDefinedFields
- VerificationState
- Workflow

对于这些字段，请映射到位于FindingProviderFields对象。请勿映射到顶级字段。

- Confidence— 如果您的服务具有类似的功能，或者如果您 100% 支持自己的发现，则仅包括信心评分（0-99）。
- Criticality— 重要程度分数（0-99）旨在表达与调查结果相关的资源的重要性。
- RelatedFindings— 只有在可以跟踪与同一资源或查找类型相关的调查结果时才提供相关的调查结果。要识别相关查找结果，您必须参考 Security Hub 中已存在的查找结果的查找标识符。

的使用准则**BatchImportFindings**API

使用BatchImportFindings将结果发送到的 API 操作AWS Security Hub，请遵守以下准则。

- 你必须打电话BatchImportFindings使用与调查结果关联的账户。关联账户的标识符是AwsAccountId查找结果的属性。
- 发送你可以的最大批次。Security Hub 每批最多可接受 100 个查找结果，每个查找结果最多可接受 240 KB，每批最多可接受 6 MB。
- 限制费率限制为每个区域每个账户 10 TPS，突发率为 30 TPS。
- 如果存在限制或网络问题，则必须实施一种机制来保持发现状态。您还需要查找状态，以便在调查结果进入和退出合规性时提交查找更新。
- 有关字符串的最大长度和其他限制的信息，请参阅AWSSecurity Finding 格式 (ASFF)中的AWS Security Hub用户指南.

产品准备核对清

这些区域有：AWS Security HubAPN 合作伙伴团队使用此清单验证集成是否已准备好启动。

ASFF 映射

这些问题与将你的发现映射到AWSSecurity Found 格式 (ASFF)。

合作伙伴的所有发现数据是否都映射到 ASFF 中？

以某种方式将你的所有发现映射到 ASFF。

使用策划字段，例如模型化的资源类型，Network、Malware，或者ThreatIntelIndicators.

将任何东西映射到Resource.Details.Other要么ProductFields根据需要执行。

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**定义 ASFF 中未建模的资源详细信息？

如果可能，请在结果中使用针对策划资源（如 EC2 实例、S3 存储桶和安全组）的所提供字段。

将与资源相关的其他信息映射到Resource.Details.Other只有在没有直接匹配的情况下才能。

合作伙伴是否将值映射到**UserDefinedFields**?

请勿使用 UserDefinedFields。

考虑使用另一个精心策划的领域，例如Resource.Details.Other要么ProductFields.

合作伙伴是否将信息映射到**ProductFields**那可以映射到其他 ASFF 字段？

只能使用ProductFields获取特定于产品的信息，例如版本控制信息、特定于产品的严重性调查结果或其他无法映射到精选字段的信息，或Resources.Details.Other.

合作伙伴是否导入自己的时间戳**FirstObservedAt**?

这些区域有：FirstObservedAt时间戳旨在记录商品中观察到发现的时间。如果可能的话，映射此字段。

合作伙伴是否提供为每个查找结果标识符生成的唯一值，但他们想要更新的调查结果除外？

Security Hub 中的所有发现都在查找结果标识符上编制索引（Id属性)。此值必须始终是唯一的，以确保不会意外更新调查结果。

为了更新调查结果，您还应保持查找结果标识符状态。

合作伙伴是否提供了将发现映射到生成器 ID 的值？

GeneratorID不应该与查找 ID 具有相同的值。

GeneratorID应该能够通过产生这些结果的原因在逻辑上链接发现。

这可以是产品中的子组件（产品 A-漏洞与产品 A-EDR）或类似的东西。

合作伙伴是否以与其产品相关的方式使用所需的查找类型命名空间？ 合作伙伴在其查找类型中是否使用推荐的查找类型类别或分类器？

查找类型分类应与产品生成的调查结果密切相对应。

中概述的第一级命名空间AWS需要使用 Security F功能格式。

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。

合作伙伴是否在**Network**字段，如果他们有网络数据？

如果您的产品捕获NetFlow信息，将其映射到Network字段中返回的子位置类型。

合作伙伴捕获过程 (PID) 信息是否在**Process**字段，如果他们有过程数据？

如果您的产品捕获过程信息，请将其映射到Process字段中返回的子位置类型。

合作伙伴是否在**Malware**字段，如果他们有恶意软件数据？

如果您的产品捕获了恶意软件信息，请将其映射到Malware字段中返回的子位置类型。

合作伙伴是否在**ThreatIntelIndicators**字段，如果他们有威胁情报数据？

如果您的产品捕获威胁情报信息，请将其映射到ThreatIntelIndicators字段中返回的子位置类型。

合作伙伴是否为调查结果提供信心评级？ 如果他们这样做，是否提供了理由？

无论何时使用此字段，都可以在文档和清单中提供理由。

合作伙伴是否在调查结果中使用规范 ID 或 ARN 作为资源 ID？

识别时AWS资源，最佳做法是使用 ARN。如果 ARN 不可用，请使用规范资源 ID。

集成设置和功能

这些问题与设置和day-to-day集成的功能。

合作伙伴是否提供infrastructure-as-code部署与 Security Hub 的集成的 (iAC) 模板，例如 Terraform，AWS CloudFormation，或者AWS Cloud Development Kit (AWS CDK)?

对于将从客户帐户发送调查结果或使用CloudWatch使用调查结果的事件，需要某种形式的 iAC 模板。

AWS CloudFormation最好使用，但AWS CDK或者 Terraform 也可以使用。

合作伙伴产品是否在控制台上安装了一键式设置，以便与 Security Hub 集成？

一些合作伙伴产品在其产品中使用切换或类似的机制来激活集成。这可能需要自动配置资源和权限。如果您从产品帐户发送调查结果，则首选一键设置方法是首选方法。

合作伙伴只发送有价值的调查结果吗？

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

Security Hub 不是一个通用的日志管理工具。你不应该将所有可能的日志发送到 Security Hub。

合作伙伴是否对每位客户每天发送多少调查结果以及发送频率（平均和突发频率）提供了估计数？

独特发现的数量用于计算 Security Hub 上的负载。唯一的发现被定义为具有与另一个发现不同 ASFF 映射的查找结果。

例如，如果只填充了一个查找结果ThreatIntelndicators另一个只有人口Resources.Details.AWSEc2Instance，这是两个独特的发现。

合作伙伴是否有一种优雅的方法来处理 4xx 和 5xx 错误，以免它们受到限制，所有发现都可以在以后发送？

目前在上面有 30—50 TPS 的突发率BatchImportFindingsAPI 操作。如果返回 4xx 或 5xx 错误，则必须保留这些失败的查找结果的状态，以便稍后可以重试它们。你可以通过死信队列或其他队列来做到这一点AWS消息传递服务，例如 Amazon SNS 或 Amazon SQS。

合作伙伴是否保持调查结果的状态，以便他们知道存档不再存在的调查结果？

如果您计划通过覆盖原始查找结果 ID 来更新调查结果，则必须有保留状态的机制，以便更新正确的信息以获得正确的查找结果。

如果您提供了调查结果，请勿使用BatchUpdateFindings操作来更新调查结果。此操作只能由客户使用。你只能使用BatchUpdateFindings当您调查结果并对结果采取相应措施时。

合作伙伴是否以不影响先前发送的成功调查结果的方式处理重试？

您应该有一种机制来在出错时保留原始查找 ID，这样您就不会错误地复制或覆盖成功的查找结果。

合作伙伴是否通过调用**BatchImportFindings**使用现有调查结果的发现 ID 进行操作？

要更新查找结果，必须通过提交相同的查找结果 ID 覆盖现有查找结果。

这些区域有：BatchUpdateFindings操作只能由客户使用。

合作伙伴是否使用**BatchUpdateFindings**API？

如果你对调查结果采取行动，你可以使用BatchUpdateFindings操作来更新特定字段。

合作伙伴是否提供有关创建查找结果到发现结果从其产品发送到 Security Hub 之间的延迟量的信息？

您应该最大限度地减少延迟，以确保客户尽快在 Security Hub 中看到发现结果。

清单中必须提供此信息。

如果合作伙伴的体系结构是要从客户帐户向 Security Hub 发送调查结果，他们是否成功地证明了这一点？ 如果合作伙伴的体系结构要从自己的账户向 Security Hub 发送调查结果，他们是否成功地证明了这一点？

在测试过程中，必须从您拥有的账户成功发送调查结果，该账户与为产品 ARN 提供的账户不同。

从产品 ARN 所有者账户发送调查结果可以绕过 API 操作中的某些错误例外。

合作伙伴是否向 Security Hub 提供心跳发现？

为了表明您的集成工作正常，你应该发送心跳发现。心跳查找结果每五分钟发送一次，并使用查找类型`Heartbeat`.

如果您从产品账户发送调查结果，这很重要。

在测试过程中，合作伙伴是否与 Security Hub 产品团队的帐户集成了？

在生产前验证期间，您应该向 Security Hub 产品团队发送查找示例AWSaccount. 这些示例表明，发现已正确发送和映射。

文档

这些问题与您提供的集成文档有关。

合作伙伴是否在专用网站上托管他们的文档？

文档应作为静态网页、Wiki、阅读文档或其他专用格式托管在您的网站上。

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他们的使用案例的描述？

还应在文档中描述您在清单中提供的用例

合作伙伴文档是否为他们发送的调查结果提供了理由？

你应该提供你发送的调查结果类型的理由。

例如，您的产品可能会生成漏洞、恶意软件和防病毒软件的发现，但您只能将漏洞和恶意软件发现发送到 Security Hub。在这种情况下，您必须提供为什么不发送防病毒检测结果的理由。

合作伙伴文档是否提供了合作伙伴如何将其调查结果与 ASFF 相对应的理由？

您应该提供将产品的原生发现映射到 ASFF 的理由。买家想知道在哪里查找具体的商品信息。

如果合作伙伴更新调查结果，合作伙伴文档是否就如何更新调查结果提供指导？

向客户提供有关如何保持状态、确保幂等以及覆盖调查结果的信息up-to-date信息。

合作伙伴文档是否描述了发现延迟？

最大限度地减少延迟，以确保客户尽快在 Security Hub 中看到发现结果。

清单中必须提供此信息。

合作伙伴文档是否描述了他们的严重程度评分与 ASFF 严重性评分相对应？

提供有关如何映射的信息`Severity.Original`到`Severity.Label`.

例如，如果严重性值是字母等级（A、B、C），则应提供有关如何将字母成绩映射到严重性标签的信息。

合作伙伴文档是否提供了信心评级的理由？

如果您提供置信度分数，则应对这些分数进行排名。

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，则应提供其他上下文。

合作伙伴文档是否注明合作伙伴支持哪些地区和不支持哪些地区？

注意支持或不受支持的区域，以便客户知道在哪些地区不尝试集成。

产品卡信息

这些问题与显示在集成Security Hub 控制台的页面。

提供了吗AWS账户 ID 有效且包含 12 位数字？

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

商品描述是否包含 200 个或更少的字符？

清单中 JSON 中提供的产品描述不应超过 200 个字符，包括空格。

配置链接是否导致了集成的文档？

配置链接应该导向您的在线文档。它不应该导致你的主网站或营销页面。

购买链接（如果提供）是否会导致AWS Marketplace商品上架？

如果您提供购买链接，则必须用于AWS Marketplace条目。Security Hub 不接受未托管的购买链接 AWS.

商品类别描述商品是否正确？

在清单中，您最多可以提供三个产品类别。这些应该与 JSON 匹配，不能自定义。您提供的商品分类不能超过三个。

公司和产品名称是否有效且正确？

公司名称必须为 16 个或更少的字符。

商品名称必须为 24 个或更少的字符。

产品卡片 JSON 中的产品名称必须与清单中的名称匹配。

营销信息

这些问题与集成的营销有关。

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

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

团队将向下编辑更长的描述。

Security Hub 合作伙伴页面徽标不超过 600 x 300 像素吗？

提供一个公开可访问的 URL，其中包含 PNG 或 JPG 的公司徽标，不超过 600 x 300 像素。

Security Hub 合作伙伴页面上的了解更多超链接是否可以指向合作伙伴关于集成的专用网页？

这些区域有：了解更多链接不应导致合作伙伴的主网站或文档信息。

此链接应始终转到专用网页，其中包含有关于集成的营销信息。

合作伙伴是否提供演示或教学视频，了解如何使用他们的集成？

您可以自由选择，但我们建议您使用演示视频或集成演

是AWS合作伙伴网络博客文章是与合作伙伴及其合作伙伴开发经理或合作伙伴开发代表一起

AWS合作伙伴网络博客文章应提前与合作伙伴开发经理或合作伙伴开发代表进行协调。

这些与你自己创建的任何博客文章是分开的。

允许 4-6 周的交货时间。这项工作应该在私有产品 ARN 测试完成后开始。

合作伙伴主导的新闻稿是否正在发布？

您可以与合作伙伴开发经理或合作伙伴开发代表合作，从外部安全服务副总裁那里获取报价。你可以在新闻稿中使用此报价。

合作伙伴主导的博客文章是否正在发布？

你可以创建自己的博客文章来展示AWS合作伙伴网络博客。

合作伙伴主导的网络研讨会正在发布吗？

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。

合作伙伴请求社交媒体支持吗？AWS?

发布后，您可以使用AWS安全营销导致使用AWS官方社交媒体渠道，分享有关网络研讨会的详细信息。

AWS Security Hub常见问题

以下是有关设置和维护与集成的常见问题AWS Security Hub.

1. Security Hub 集成有哪些优势？
   - 客户满意度— 与 Security Hub 集成的首要原因是您有客户要求这样做。

     Security Hub 是安全与合规中心AWS客户。它被设计为第一站AWS安全和合规性专业人员每天都会了解他们的安全性和合规状态。

     听你的客户的意见。他们会告诉你他们是否想在 Security Hub 中看到你的发现。
   - 发现机会— 我们在 Security Hub 控制台内推广具有认证集成的合作伙伴，包括指向他们的链接AWS Marketplace列表。这是客户发现新安全产品的好方法。
   - 营销机会— 获得批准集成的供应商可以参加网络研讨会、发布新闻稿、创建光滑的表格，并展示他们的集成AWS客户。
2. 那里有哪些类型的合作伙伴？
   - 向 Security Hub 发送结果的合作伙伴
   - 收来自 Security Hub 的结果的合作伙伴
   - 发送和接收调查结果的合作伙伴
   - 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. 合作伙伴与 Security Hub 的集成如何在高层次上运作？

   您可以从客户账户内或自己的账户中收集调查结果AWS账户并将调查结果的格式转换为AWSSecurity Find 格式 (ASFF)。然后，您将这些发现推送到适当的 Security Hub 区域终端节点。

   您还可以使用CloudWatch接收来自 Security Hub 的结果的活动。
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. 如果要向 Security Hub 发送调查结果，请接收产品 ARN 以与 Security Hub 一起使用。
   c. 将你的发现映射到 ASFF。请参阅the section called “ASFF 映射准则”。
   d. 定义用于向 Security Hub 发送调查结果和接收调查结果的架构。遵循中概述的原则the section called “创建和更新调查结果的原则”.
   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. 定义客户可以用于您的产品的任何自定义见解（关联规则）。

h. 展示你与 Security Hub 团队的集成。

i. 提交营销信息以供批准（网站语言、新闻稿、架构幻灯片、视频、光滑表）。

5. 提交合作伙伴清单的流程是什么？ 而且对于AWS要将结果发送到 Security Hub 的服务？

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

   在七个日历日内向您发放商品 ARN。

6. 我应该向 Security Hub 发送哪些类型的发现？

   Security Hub 定价部分基于所收到的结果的数量。因此，您应避免发送不给客户带来价值的调查结果。

   例如，一些漏洞管理供应商发送的调查结果在可能的 10 分中只有 3 分或以上的普通漏洞评分系统 (CVSS) 得分。

7. 将结果发送到 Security Hub 有哪些不同的方法？

   这些是主要的方法：

   - 你发送自己指定的调查结果AWS账户使用BatchImportFindingsoperation.
   - 您可以使用从客户账户中发送调查结果BatchImportFindingsoperation. 你可以使用假设角色方法，但这些方法不是必需的。

   有关使用的总体指南BatchImportFindings，请参阅the section called “的使用准则BatchImportFindingsAPI”.

8. 如何收集我的发现并将其推送到 Security Hub 区域终端节点？

   合作伙伴为此使用了不同的方法，因为它高度依赖于您的解决方案的体系结构。

   例如，一些合作伙伴构建了一个 Python 应用程序，该应用程序可以作为AWS CloudFormation脚本。该脚本从客户环境中收集合作伙伴的调查结果，将其转换为 ASFF，然后将其发送到 Security Hub 区域终端节点。

   其他合作伙伴构建了一个完整的向导，为客户提供一键式体验，将发现推送到 Security Hub。

9. 如何知道何时开始将结果发送到 Security Hub？

   Security Hub 支持部分批量授权BatchImportFindingsAPI 操作，以便您可以将所有调查结果发送到所有客户的 Security Hub。

如果您的一些客户尚未订阅 Security Hub，Security Hub 将不会收录这些发现。它只提取批处理中的授权调查结果。

10.我需要完成哪些步骤才能将结果发送到客户的 Security Hub 实例？

a. 确保制定了正确的 IAM 策略。

b. 为账户启用产品订阅（资源策略）。使用EnableImportFindingsForProductAPI 操作或集成页. 客户可以这样做，也可以使用跨账户角色代表客户行事。

c. 确保ProductArn的发现是你产品的公开 ARN。

d. 确保AwsAccountId的结果是客户的账户 ID。

e. 确保你的发现没有任何格式错误的数据，根据AWSSecurity Find 格式 (ASFF)。例如，填充必填字段，并且没有无效值。

f. 将调查结果批量发送到正确的区域终端节点。

11.我必须有哪些 IAM 权限才能发送调查结果？

必须为调用的 IAM 用户或角色配置 IAM 策略BatchImportFindings或者其他 API 调用。

最简单的测试是从管理员帐户执行此操作。你可以将这些限制为action: 'securityhub:BatchImportFindings'和resource: *<productArn and/or productSubscriptionArn>*.

可以使用 IAM 策略配置同一账户中的资源，而无需资源策略。

排除来自调用者的 IAM 策略问题BatchImportFindings中，按如下方式为调用者设置 IAM 策略：

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

一定要检查没有Deny调用方的策略。使用它之后，您可以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结果，客户（或代表客户工作的跨账户角色的合作伙伴）必须建立产品订阅。要通过控制台完成这一操作，他们需要使用集成页. 为了从 API 执行此操作，他们使用EnableImportFindingsForProductAPI 操作。

产品订阅将创建资源策略，授权客户接收或发送合作伙伴的调查结果。有关详细信息，请参阅 使用案例和权限。

Security Hub 为合作伙伴提供以下类型的资源策略：

- BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT
- BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT

在合作伙伴入职过程中，您可以请求一种或两种类型的策略。

与BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT，您只能从产品 ARN 中列出的账户向 Security Hub 发送调查结果。

与BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT，您只能从订阅您的客户账户中发送调查结果。

13.假设客户创建了管理员帐户并添加了一些成员帐户。客户是否需要向我订阅每个会员账户？ 还是客户只从管理员帐户订阅，然后我可以根据所有成员账户中的资源发送调查结果？

此问题询问是否根据管理员帐户注册为所有成员帐户创建权限。

客户必须为每个账户进行产品订阅。他们可以通过 API 以编程方式完成此操作。

14.我的产品 ARN 是什么？

您的产品 ARN 是 Security Hub 为您生成的、用于提交调查结果的唯一标识符。对于与 Security Hub 集成的每个产品，您都会收到一个产品 ARN。正确的产品 ARN 必须是您发送给 Security Hub 的每个发现结果的一部分。没有产品 ARN 的发现将被删除。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
```

您将获得针对部署 Security Hub 的每个区域的产品 ARN。账户 ID、公司和产品名称由您的合作伙伴提交的清单决定。除区域代码外，您永远不会更改与商品 ARN 关联的任何信息。区域代码必须与您提交调查结果的地区匹配。

一个常见的错误是更改账户 ID 以与您当前工作的账户匹配。账户 ID 不会更改。作为提交清单的一部分，您提交 “家庭” 账户 ID。此账户 ID 已锁定在您的产品 ARN 中。

当 Security Hub 在新区域中启动时，它会自动使用标准区域代码为这些区域生成产品 ARN。

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

15.向 Security Hub 发送结果应该使用哪种格式？

必须在中提供结果AWSSecurity Find 格式 (ASFF)。有关详细信息，请参阅。AWSSecurity Finding 格式 (ASFF)中的AWS Security Hub用户指南.

我们的期望是，你原生发现中的所有信息都充分反映在 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.要使用的正确区域终端节点是什么？

您必须将调查结果发送到与客户账户关联的 Security Hub 区域终端节点。

17.在哪里可以找到区域终端节点列表？

请参阅Security Hub 终端节点列表.

18.我可以提交跨区域调查结果吗？

Security Hub 尚不支持为本地人提交跨区域的调查结果AWS服务，例如亚马逊GuardDuty、Amazon Macie 和亚 Amazon Inspector。如果您的客户允许，Security Hub 不会阻止您提交来自不同地区的调查结果。

从这个意义上说，您可以从任何地方调用区域终端节点，而 ASFF 的资源信息不必与终端节点的区域匹配。但是，`ProductArn`必须与终端节点的区域匹配。

19.发送批量调查结果的规则和指导方针是什么？

一次调用最多可以批量 100 个发现或 240 KB`BatchImportFindings`. 排队并批量尽可能多的发现，直到此限制。

您可以批处理来自不同账户的一组调查结果。但是，如果批处理中的任何账户未订阅 Security Hub，则整个批次将失败。这是 API Gateway 基准授权模型的限制。

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

20.我可以对我创建的调查结果发送更新吗？

是的，如果您提交的调查结果具有相同的商品 ARN 和相同的查找结果 ID，它将覆盖该调查结果的先前数据。请注意，所有数据都被覆盖，因此您应该提交完整的调查结果。

对新发现和查找更新的客户进行计费和计费。

21.我可以发送其他人创建的调查结果的更新信息吗？

是的，如果客户授予您访问`BatchUpdateFindings`API 操作，您可以使用该操作更新某些字段。此操作旨在供客户、SIEM、票证系统以及安全编制、自动化和响应 (SOAR) 平台使用。

22.调查结果如何过时？

Security Hub 在上次更新日期后 90 天将结果过期。在此之后，已过时的调查结果将从 Security Hub 中清除OpenSearch集群。

如果您使用相同的查找结果 ID 更新查找结果并且该查找结果已过期，则会在 Security Hub 中创建一个新的查找结果。

客户可以使用CloudWatch将调查结果移出 Security Hub 的活动。这样做可以将所有调查结果发送给客户选择的目标。

一般来说，Security Hub 建议您每 90 天创建一次新的调查结果，而不要永远更新调查结果。

23.Security Hub 设置了什么限制？

Security Hub 限制`GetFindings`API 调用，因为推荐的访问结果方法正在使用CloudWatch事件。

除了 API Gateway 和 Lambda 调用强制实施的限制外，Security Hub 不会对内部服务、合作伙伴或客户实施任何其他限制。

24.从源服务发送到 Security Hub 的调查结果的时效性或延迟 SLA 或对发现的期望是什么？

目的是尽可能接近实时的初步调查结果和调查结果的更新。您应该在创建调查结果后的五分钟内将其发送到 Security Hub。

25如何接收来自 Security Hub 的结果？

要接收结果，请使用以下方法之一。

- 所有调查结果都会自动发送到CloudWatch事件。客户可以创建特定的CloudWatch将调查结果发送到特定目标（例如 SIEM 或 S3 存储桶）的事件规则。此功能取代了传统`GetFindings`API 操作。
- 使用CloudWatch自定义操作的事件。Security Hub 允许客户从控制台中选择特定的调查结果或调查结果组并对其采取措施。例如，他们可以将调查结果发送到 SIEM、票务系统、聊天平台或修复工作流程。这将是客户在 Security Hub 内执行的警报分类工作流程的一部分。这些被称为自定义操作。

  当用户选择自定义操作时，CloudWatch事件是针对这些特定发现创建的。你可以利用这个功能然后进行构建CloudWatch供客户用作自定义操作一部分的事件规则和目标。请注意，此功能不会自动将特定类型或类的所有结果发送到CloudWatch事件。用户应该对具体的调查结果采取行动。

  您可以使用自定义操作 API 操作，例如`CreateActionTarget`，以便为您的商品自动创建可用操作（例如使用AWS CloudFormation）。你还可以使用CloudWatch事件规则 API 操作来创建相应CloudWatch与自定义操作关联的事件规则。使用AWS CloudFormation模板，你也可以创建CloudWatch事件规则可自动从 Security Hub 提取所有发现或具有特定特征的所有发现结果。

26托管安全服务提供商 (MSSP) 成为 Security Hub 合作伙伴有什么要求？

您必须演示如何使用 Security Hub 作为向客户交付服务的一部分。

你应该有解释你使用 Security Hub 的用户文档。

如果 MSSP 是查找提供商，他们必须展示向 Security Hub 发送调查结果。

如果 MSSP 只收到来自 Security Hub 的调查结果，他们至少必须有AWS CloudFormation用于设置适当的模板CloudWatch活动规则。

27非 MSSP APN 咨询合作伙伴成为 Security Hub 合作伙伴有什么要求？

如果您是 APN 咨询合作伙伴，则可以成为 Security Hub 合作伙伴。您应该提交两份私人案例研究，说明如何帮助特定客户执行以下操作。

- 使用客户需要的 IAM 权限设置 Security Hub。

- 使用控制台中合作伙伴页面上的配置说明，帮助将已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。
- 建立与客户需求和数据集相关的自定义见解。
- 构建自定义操作。
- 构建补救行动手册。
- 构建符合 Security Hub 合规性标准的快速入门。这些必须由 Security Hub 团队验证。

不需要可公开分享案例研究。

28.围绕如何与客户部署与 Security Hub 的集成有什么要求？

Security Hub 和合作伙伴产品之间的集成体系结构因合作伙伴的解决方案的运营方式而异。您应确保集成的设置过程不超过 15 分钟。

如果您将集成软件部署到客户的AWS环境中，你应该利用AWS CloudFormation用于简化集成的模板。一些合作伙伴创建了一键式集成，这受到了高度鼓励。

29.我的文件要求是什么？

您必须提供一个指向描述产品与 Security Hub 之间的集成和设置过程的文档的链接，包括使用AWS CloudFormationTemplate

该文档还应包括有关你使用 ASFF 的信息。具体来说，这应该列出您用于不同调查结果的 ASFF 查找类型。如果您有任何默认的洞察定义，建议您还要将这些定义包括在这里。

考虑包括其他潜在信息：

- 与 Security Hub 集成的使用案例
- 发送的调查结果的平均量
- 您的集成架构
- 你支持和不支持的地区
- 创建查找结果到发送到 Security Hub 之间的延迟
- 是否更新调查结果

30.什么是自定义见解？

我们鼓励你为自己的发现定义自定义见解。见解是轻量级关联规则，可帮助客户优先考虑哪些发现和资源最需要关注和采取行动。

Security Hub 有`CreateInsight`API 操作。您可以在客户账户中创建自定义见解作为您的一部分 AWS CloudFormationTemplate 这些见解显示在客户的控制台上。

31.我可以提交仪表板小部件吗？

目前不可以。您只能创建托管见解。

32.你的定价模式是什么？

请参阅Security Hub 定价信息.

33.作为集成的最终批准流程的一部分，如何向 Security Hub 模拟账户提交调查结果？

使用您提供的产品 ARN 将调查结果发送到 Security Hub 模拟账户，使用`us-west-2`作为该地区。调查结果应包括模拟账户号码`AwsAccountId`ASFF 领域。要获取模拟账户号码，请联系 Security Hub 团队。

不要向我们发送任何敏感数据或个人身份信息。这些数据用于公开演示。当您向我们发送此数据时，您授权我们在演示中使用这些数据。

34.错误或成功消息的作用是什么**`BatchImportFindings`**提供？

Security Hub 提供授权响应和响应`BatchImportFindings`. 正在开发更清晰的成功、失败和错误信息。

35.源服务负责哪些错误处理？

源服务负责所有错误处理。他们必须处理错误消息、重试次数、限制和警报。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.对于常见问题有哪些解决办法？

网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping
的`AuthorizerConfigurationException`是由格式错误引起的`AwsAccountId`要么`ProductArn`.

在排除故障时，请注意以下内容

- `AwsAccountId`必须准确为 12 位数。
- `ProductArn`必须采用以下格式：arn: AWS: Security Hub:*<us-west-2 or us-east-1>*：*<accountId>*: 产品/*<company-id>*/*<product-id>*

  账户 ID 与 Security Hub 团队提供给您的产品 ARN 中包含的账户 ID 不会更改。

AccessDeniedException是由于发送到错误的账户或从错误的账户发送了发现，或者当账户没有ProductSubscription. 错误消息将包含资源类型为product要么product-subscription. 此错误仅在跨账户调用期间发生。如果你打电话BatchImportFindings使用自己的账户为同一账户AwsAccountId和ProductArn，该操作使用 IAM 策略，与无关ProductSubscriptions.

确保您使用的客户账户和产品账户是实际注册账户。有些合作伙伴使用了产品 ARN 中的产品的账号，但尝试使用完全不同的账户来调用BatchImportFindings. 在其他情况下，它们创造了ProductSubscriptions对于其他客户账户，甚至是他们自己的产品账户。他们不是创造ProductSubscriptions对于他们试图将结果导入到的客户账户。

37.我在哪里发送问题、评论和错误？

<securityhub-partners@amazon.com>

38.我向哪个地区发送与全球相关的商品的调查结果AWS服务？ 例如，我可以在哪里发送与 IAM 相关的调查结果？

将调查结果发送到检测到调查结果的同一个区域。对于 IAM 之类的服务，您的解决方案可能会在多个区域中找到相同的 IAM 问题。在这种情况下，调查结果将发送到检测到问题的每个地区。

如果客户在三个区域运行 Security Hub，并且在所有三个区域中检测到同一个 IAM 问题，则将调查结果发送到所有三个区域。

问题解决后，将查找结果的更新发送到您发送原始调查结果的所有地区。

《合作伙伴集成指南》的文档历史记录

下表介绍了本指南的文档更新。

变更	说明	日期
更新了控制台徽标的要求	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版本的徽标才能显示在 Security Hub 控制台上。徽标必须为 SVG 格式。	2021 年 5 月 10 日
更新了新集成合作伙伴的先决条件	Security Hub 现在还允许已加入的合作伙伴AWSISV 合作伙伴路径，以及谁使用已完成的集成产品AWS基础技术审查（FTR）。以前，所有集成合作伙伴都必须是AWS选择级别合作伙伴。	2021 年 4 月 29 日
newFindingProviderFields ASFF 中的对象	更新了有关将调查结果映射到 ASFF 的信息。对于`Confidence`，`Criticality`，`RelatedFindings`，`Severity`，以及`Types`，合作伙伴将其值映射到中的字段`FindingProviderFields`。	2021 年 3 月 18 日
创建和更新调查结果的新原则	添加了一组用于在 Security Hub 中创建新发现和更新现有发现的新准则。	2020 年 12 月 4 日
该指南的初始版本	这个Partner 集成指南提供AWS合作伙伴提供有关如何	2020 年 6 月 23 日

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。