AWS Security Hub

合作伙伴集成指南

亚马逊云科技

AWS Security Hub: 合作伙伴集成指南

Table of Contents

第三方集成概述 AWS Security Hub

本指南适用于 AWS 希望创建与 AWS Security Hub.

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

- 发送结果至 Security Hub
- 消费发现 Security Hub
- 两者都将结果发送到 Security Hub
- 使用 Security Hub 作为托管安全服务提供商(MSSP)提供的中心
- 咨询 AWS 客户如何部署和使用 Security Hub

本入职指南主要关注发送结果的合作伙伴 Security Hub.

主题

为何与 AWS Security Hub?

AWS Security Hub 提供全面的高优先级安全警报和安全状态视图 Security Hub 账户。 Security Hub 允许像您这样的合作伙伴将安全发现发送到 Security Hub 为您的客户提供您生成的安全发现的洞察力。

与 Security Hub 可以通过以下方式添加值。

- 满足您要求的 Security Hub 集成
- 为客户提供他们 AWS 与安全相关的结果
- 让新客户能够在提供与特定安全事件类型相关的调查结果的合作伙伴时发现您的解决方案

在您与 Security Hub，检查您的整合原因。如果您的客户希望 Security Hub 与您的产品集成。您可以根据营销原因或收购新客户构建集成。但是，如果您在没有任何当前客户意见的情况下建立集成，并且不考虑客户的需求，那么整合可能不会产生预期结果。

准备将结果发送至 AWS Security Hub

作为APN合作伙伴，您不能将信息发送到 Security Hub 为您的客户提供 Security Hub 团队将您作为寻找提供商。要启用为寻找提供商，您必须完成以下入职步骤。这样做确保积极的体验 Security Hub 对于您和您的客户。

1. 将您的安全结果映射到 AWS 安全查找格式(ASFF)。
2. 构建您的集成架构，将结果推向正确的区域 Security Hub 端点。为此，您定义您是否将发现自己的 AWS 客户账户内或客户账户内的。
3. 让您的客户将产品订购至客户。为此，他们可以使用控制台或 `EnableImportFindingsForProduct` API操作。参见 管理产品集成 在 AWS Security Hub 用户指南.

您也可以订阅这些产品。为此，您使用跨客户角色访问 `EnableImportFindingsForProduct` 代表客户的API操作。

此步骤确定接受该客户产品发现所需的资源政策。

以下博客帖子讨论了与安全枢纽的一些现有合作伙伴集成。

- 宣布云托管人与AWSSecurityHub集成
- 使用 AWS Fargate 和Prowler发送安全配置结果 AWS 服务 Security Hub
- 如何导入 AWS Config 规则评估的结果 Security Hub

准备接收发现 AWS Security Hub

接收发现 AWS Security Hub，使用以下选项之一:

- 让您的客户自动发送所有调查结果 CloudWatch Events. 客户可以创建特定 CloudWatch 将结果发送到特定目标（例如SIEM或S3桶）的事件规则。
- 让您的客户从内部选择具体的结果或团体 Security Hub 控制台，然后对他们采取行动。

例如，您的客户可以将结果发送到SIEM、票务系统、聊天平台或修复工作流程。这将是客户在 Security Hub.

这些称为自定义操作。当用户采取自定义操作时， CloudWatch 为这些具体结果创建事件。作为合作伙伴，您可以充分利用这种能力 CloudWatch 用作自定义操作一部分的客户的事件规则或目标。请注意，此功能不会自动发送特定类型或类别的所有发现 CloudWatch Events. 此功能供用户对特定发现采取措施。

以下博客帖子概述了使用与 Security Hub 和 CloudWatch Events 对于自定义操作。

- 如何整合 AWS Security Hub 带页面的自定义操作
- 如何启用自定义操作 AWS Security Hub
- 如何导入 AWS Config 规则评估的结果 Security Hub

学习资源 AWS Security Hub

以下材料可帮助您更好地了解 AWS Security Hub 解决方案 AWS 客户可以使用服务。

- 介绍 AWS Security Hub 视频
- 安全枢纽用户指南
- 安全集线器API参考
- 入职培训网络

我们还鼓励您启用 Security Hub 您的 AWS 客户并获得有关服务的一些实践经验。

合作伙伴前提

在您开始与 AWS Security Hub，您必须满足以下要求。

- 必须是良好站点的合作伙伴 选择 或更高级别 AWS 合作伙伴网络(APN)。
- 必须与 AWS.

集成使用情况和必要的权限

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内部或外部运行 AWS 账户。客户帐户中的权限配置根据合作伙伴产品使用的模型而不同。

在 Security Hub，客户始终控制哪些合作伙伴可以将结果发送到客户的账户。客户可以随时撤销合作伙伴的权限。

为使合作伙伴能够将安全结果发送到客户帐户，客户首先订阅了合作伙伴产品 Security Hub. 订阅步骤是以下所有使用情形的必要步骤。有关客户如何管理产品整合的详细信息，请参阅 管理产品集成 在 AWS Security Hub 用户指南.

客户订购合作伙伴产品后， Security Hub 自动创建管理资源策略。本政策授予合作伙伴产品的使用 `BatchImportFindings` 将结果发送到API操作 Security Hub 对于客户帐户。

以下是与 Security Hub. 信息包括每个使用情形所需的额外权限。

合作伙伴托管:从合作伙伴账户发出的结果

这种使用案例涵盖了自己主办产品的合作伙伴 AWS 账户。发送安全发现 AWS 客户，合作伙伴呼叫 `BatchImportFindings` 合作伙伴产品帐户的API操作。

对于此使用情形，客户帐户只需要在客户订购合作伙伴产品时建立的权限。

在合作伙伴账户中， IAM 致电 `BatchImportFindings` API操作必须具有 IAM 允许负责人致电的政策 `BatchImportFindings`.

启用合作伙伴产品将结果发送给客户 Security Hub 是一个两步流程:

1. 客户在 Security Hub.
2. Security Hub 通过客户确认生成正确的管理资源策略。

要发送与客户账户相关的安全发现，合作伙伴产品使用他们自己的凭证来调用 `BatchImportFindings` API 操作。

以下是 IAM 在合伙人账户中授予本金必要的政策 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:从客户账户发出的结果

这种使用案例涵盖了自己主办产品的合作伙伴 AWS 帐户，但使用跨客户角色访问客户帐户。他们称之为 `BatchImportFindings` 客户帐户的API操作。

对于此使用情形，请致电 `BatchImportFindings` API操作，合作伙伴帐户假设客户管理 IAM 客户账户中的角色。

本次通话是由客户的账户进行的。因此，管理资源策略必须允许产品ARN在呼叫中使用合作伙伴产品的帐户。TheThethe Security Hub 管理资源政策授予合作伙伴产品账户和合作伙伴产品ARN的权限。产品ARN是作为提供商的合作伙伴唯一标识符。由于该电话不来自合作伙伴产品账户，客户必须明确授予合作伙伴产品的许可，以将结果发送至 Security Hub.

合作伙伴和客户账户之间的跨客户角色的最佳实践是使用合作伙伴提供的外部标识符。此外部标识符是客户帐户中的跨客户策略定义的一部分。合作伙伴在承担角色时必须提供标识符。外部标识符在授予时提供额外的安全层 AWS 帐户访问合作伙伴。唯一标识符可确保合作伙伴使用正确的客户帐户。

启用合作伙伴产品将结果发送给客户 Security Hub 跨客户角色发生在四个步骤中:

1. 使用代表客户工作的跨客户角色的客户或合作伙伴， Security Hub.
2. Security Hub 通过客户确认生成正确的管理资源策略。
3. 客户可以手动或使用 AWS CloudFormation. 有关跨客户角色的信息，请参阅 提供第三方拥有的AWS账户访问 在 IAM 用户指南.
4. 产品安全存储客户角色和外部ID。

接下来，产品将结果发送到 Security Hub:

1. 产品致电 AWS Security Token Service （ AWS STS)以承担客户角色。
2. 产品致电 `BatchImportFindings` API操作 Security Hub 使用假定角色的临时凭据。

以下是 IAM 授予必要的政策 Security Hub 对合作伙伴的跨客户角色的权限。

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

TheThethe `Resource` 本政策的部分确定特定产品订阅。这确保合作伙伴只能发送客户订阅的合作伙伴产品的发现。

客户托管:从客户账户发出的结果

此使用案例涵盖在客户中部署产品的合作伙伴 AWS 账户。TheThethe `BatchImportFindings` API从客户帐户中运行的解决方案中调用。

对于此使用情形，合作伙伴产品必须获得其他权限，以致电 `BatchImportFindings` API。如何根据合作伙伴解决方案以及如何在客户帐户中配置此权限来授予此权限。

这种方法的示例是在客户帐户ec2实例上运行的合作伙伴产品。此EC2实例必须具有EC2实例角色，该角色将该实例附加到该实例中 `BatchImportFindings` API操作。这允许EC2实例向客户账户发送安全发现。

此使用情况与客户将结果加载到他们拥有的产品的情境相当。

客户使合作伙伴产品能够将客户账户的结果发送给客户 Security Hub:

1. 客户将合作伙伴产品部署到 AWS 帐户手动使用 AWS CloudFormation或其他部署工具。
2. 客户定义必要的 IAM 合作伙伴产品将发现发送至 Security Hub.
3. 客户将政策附加到合作伙伴产品的必要组成部分，例如EC2实例、容器或 Lambda 功能。

现在，产品可以将结果发送到 Security Hub:

1. 合作伙伴产品使用 AWS SDK或 AWS CLI 致电 `BatchImportFindings` API操作 Security Hub. 它将来自客户帐户中的组件的呼叫附加到策略中。
2. 在API调用期间，生成必要的临时凭据，以允许 `BatchImportFindings` 呼叫成功。

以下是 IAM 授予必要的政策 Security Hub 客户账户中合作伙伴产品的权限。

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

合作伙伴入职流程

作为合作伙伴，您可以在入职流程中完成几个高级别的步骤。您必须完成这些步骤，才能将安全发现发送到 AWS Security Hub.

1. 您与APN合作伙伴团队或 Security Hub 并且表达了成为 Security Hub. 您确定要添加到 Security Hub 沟通渠道。
2. AWS 为您提供 Security Hub 合作伙伴入职培训材料。
3. 您受邀参加 Security Hub 合作伙伴SLACK渠道，您可以在其中询问与您的集成相关的问题。
4. 您为APN合作伙伴联系人提供一份草案产品整合清单，供审核。

   产品集成清单包含用于创建合作伙伴产品亚马逊资源名称(ARN)的信息，用于与 AWS Security Hub.

   它提供 Security Hub 在合作伙伴提供商页面上显示的信息的团队 Security Hub 控制台。它还用于提出与整合相关的新管理见解，以添加到 Security Hub Insight库。

   产品整合清单的初始版本不必具有完整详情。但应至少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 产品整合清单 (p. 12).
5. TheThethe Security Hub 团队为您提供产品ARN。您使用ARN将结果发送到 Security Hub.
6. 您建立集成，将结果发送至或接收发现 Security Hub.

   将结果映射到ASFF

   将结果发送至 Security Hub，您必须将调查结果映射到 AWS 安全查找格式(ASFF)。

   ASFF提供一致的研究结果描述 AWS 安全服务、合作伙伴和客户安全系统。这可以减少整合工作、鼓励常用语言，并为实施者提供蓝图。

   ASFF是用于将结果发送至 AWS Security Hub. 结果表示为JSON文档，其符合ASFFJSON架构和RFC-7493I-JSON消息格式。有关ASFF架构的详细信息，请参阅 AWS安全查找格式(ASFF) 在 AWS Security Hub 用户指南.

   请参阅the section called “ASFF映射指南” (p. 26)。

   建立和测试整合

   您可以使用 AWS 您拥有的帐户。这样您就可以全面了解如何在 Security Hub. 它还帮助您了解客户对您的安全发现的体验。

   您使用 `BatchImportFindings` API操作将新的和更新的结果发送到 Security Hub.

   整个 Security Hub 集成， AWS 鼓励您让您的APN合作伙伴联系人了解您的整合进度。您还可以询问APN合作伙伴联系人，以获得整合问题的帮助。

   请参阅the section called “使用 `BatchImportFindings` API” (p. 31)。
7. 您展示了与 Security Hub 产品团队。此集成必须使用客户的账户 Security Hub 团队拥有。

   如果他们对整合感到舒适， Security Hub 团队提供批准，向前移动以将您列为提供商。
8. 您提供 AWS 使用最终清单进行审核。
9. TheThethe Security Hub 团队在 Security Hub 控制台。然后，客户可以发现并启用集成。
10. （可选）您参与其他营销活动，促进您的 Security Hub 集成。请参阅上市活动 (p. 9)。

    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）。视频用于营销目的，并发布到 AWS Youtube频道。

- 添加到 Security Hub 第一次呼叫幻灯片甲板。

上市活动

合作伙伴还可以参与可选的营销活动，以帮助解释和推广 AWS Security Hub 集成。

如果您想创建您自己的营销内容，请创建与 Security Hub在发布内容之前，请发送草稿至您的APN合作伙伴经理进行审核和批准。这可确保每个人都能在消息传递上保持一致。

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。

在 Security Hub Partners页面

在您被批准为 Security Hub 合作伙伴，您的解决方案可以显示在 AWSSecurityHubPartners页面.

要在此页面上列出，请向您的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发展经理(PDM)、合作伙伴解决方案架构师(PSA)或发送电子邮件至 <SecurityHub-PMS@Amazon.com>.

- 简要描述您的解决方案，其与 Security Hub以及与 Security Hub 向客户提供。此描述限于700个字符，包括空格。
- 描述解决方案的页面的URL。本网站应具体说明 AWS 集成和更具体的 Security Hub 集成。它应重点关注客户在使用整合时获得的体验和价值。
- 标识为600x300像素的高分辨率拷贝。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" (p. 14).

新闻稿

作为经批准的合作伙伴，您可以选择在您的网站和公共关系渠道发布新闻稿。新闻稿必须经过批准 AWS.

在您发布新闻稿之前，您必须提交给 AWS 由APN合作伙伴营销部门审核， Security Hub 领导者，以及 AWS 外部安全服务(ESS)。新闻稿可以包括ESS副总裁提议的报价。

要启动此过程，请与PDM合作。我们拥有10个工作日的服务级别协议(SLA)来审查新闻稿。

AWS 合作伙伴网络(APN)博客

我们还可以帮助您发布作者向APN博客的博客录入。博客录入必须关注客户故事和使用案例。它不能仅仅围绕成为集成发布合作伙伴。

如果您感兴趣，请联系您的PDM或PSA开始流程。APN博客可能需要8周或更长时间进行最终批准和发布。

关于APN博客的关键事项

创建博客帖子时，请记住以下项目。

博客帖子怎么样？

合作伙伴帖子应该是教育，并且提供有关主题的深厚专业知识 AWS 客户。

理想长度不超过1,500字。读者值得深入的教育内容，教导他们可以做些什么 AWS.

内容应为APN博客的原始内容。不要使用现有博客帖子或白皮书等来源的重新用途内容。

在APN博客上发布的其他限制是什么？

只有高级或顶级级别合作伙伴才能发布到APN博客。对于具有APN计划名称的选定合作伙伴，例如服务交付。

每个合作伙伴每年仅限三个帖子。成千上万个APN合作伙伴， AWS 在其覆盖范围内必须保持平衡。

每张帖子都必须有一位技术赞助商，他们可以验证解决方案或使用案例。

在发布博客之前，编辑博客的时间是多久？

在您提交博客帖子的第一个全长草稿后，需要四到六周的时间来编辑。

为什么要写入APN博客？

APN博客帖子可提供以下优势。

- 可信度 – 对于APN合作伙伴，有一个由 AWS 可以影响全球客户。
- 可见性 – APN博客是AWS的最新博客之一，2019年的页面视图为179万页，包括影响流量。
- 业务 – APN合作伙伴帖子有可通过APN客户互动(ACE)计划生成潜在客户的连接按钮。

哪种类型的内容最适合您？

以下内容类型最适合于APN博客帖子。

- 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如何信息。超过75%的读者看到这个技术内容。
- 客户价值200级或以上的故事，展示了如何工作 AWS 或者APN合作伙伴如何解决客户的业务问题。
- 由技术专家或主题专家撰写的帖子在远期实施。

光滑片材或营销表

光滑片是一个单页文档，概述了您的产品、集成架构以及联合客户使用情形。

如果您为整合创建了一个光滑的表格，请发送一份副本到 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

如果您创建了一个白皮书或电子书，概述了您的产品、集成架构和联合客户使用情形，请发送一份副本到 Security Hub 团队。他们将把它添加到 Security Hub 合作伙伴页面。

网络研

如果您进行了关于整合的网络研讨会，请发送网络研讨会记录到 Security Hub 团队。团队将从合作伙伴页面链接。

团队还可以提供 Security Hub 主题专家参与您的网络研讨会。

演示视频

出于营销目的，您可以生成工作集成演示视频。在视频平台帐户上发布此视频，以及 Security Hub 团队将从合作伙伴页面链接。

产品整合清单

每 AWS Security Hub 集成合作伙伴必须完成产品整合清单，提供拟定集成的必要详情。

TheThethe Security Hub 团队通过以下几种方式使用这些信息:

- 创建您的网站列表
- 创建产品卡 Security Hub 控制台
- 通知您使用案例的产品团队。

评估拟定集成的质量以及提供的信息， Security Hub 团队使用 the section called “产品准备检查清单” (p. 31). 此检查清单确定您的集成是否已准备就绪。

您提供的所有技术信息都必须反映在您的文件中。

您可以从 资源 部分 AWS Security Hub 合作伙 第页。

内容：

使用案例和营销信息

以下用例可帮助您配置 AWS Security Hub 出于不同目的。

寻找提供商和消费者使用案例

独立软件供应商(ISV)要求。

描述您的使用情形， AWS Security Hub，回答以下问题。如果您不计划发送或接收结果，请在本节中注明，然后完成下一部分。

以下信息必须反映在您的文件中。

- 您是否会发现结果、接收结果或两者？
- 如果您计划发送结果，您将发送哪些类型的结果？ 您是否会发送所有发现或发现的具体子集？
- 如果您计划接收调查结果，您将如何处理这些结果？ 您将收到哪些类型的结果？ 例如，您是否会收到所有调查结果、某种类型的发现，或者只有客户选择的具体结果？
- 您是否计划更新结果？ 如果是，您将更新哪些字段？ Security Hub 建议您更新结果，而不是始终创建新的结果。更新现有发现有助于减少客户发现噪音。

  要更新查找，您会发送一个查找ID，找到已经发送到发现的查找ID。

要获得有关使用案例和数据集的早期反馈，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。

为您的工作提供两个客户使用情形 Security Hub. 这些可以是私人用例。TheThethe Security Hub 团队不会在任何地方广告他们。他们应该描述以下任一项或两项。

- 如何帮助客户引导 Security Hub? 例如，您是否帮助客户使用专业服务、特殊模块或 AWS CloudFormation 模板？
- 您如何帮助客户实现和扩展 Security Hub? 例如，您是否提供了响应或补救模板、建立的自定义集成或用于设置执行仪表板的商业智能工具？

数据集

如果您将结果发送到 Security Hub.

对于您将发送至 Security Hub，提供以下信息。

- 以本机格式发现，例如JSON或XML
- 如何将结果转换为AWS安全发现格式(ASFF)的示例

让 Security Hub 团队知道您是否需要对ASFF进行任何更新来支持您的集成。

架构

如果您发现发现或接收发现 Security Hub.

描述您将如何与 Security Hub. 这些信息也必须反映在您的文件中。

您必须提供架构图。准备架构图时，请考虑以下内容:

- 什么 AWS 服务、操作系统代理，以及您将使用哪些内容？
- 如果您将发现 Security Hub，您会发出客户发现的结果 AWS 客户或自己的 AWS 账户？
- 如果您将收到结果，您将如何使用 CloudWatch Events 集成？
- 您将如何将结果转化为ASFF？
- 您将如何批次发现、跟踪发现状态并避免限制限制？

: Configuration

如果您发现发现或接收发现 Security Hub.

描述客户将如何配置您与SecurityHub的集成。

您必须至少使用 AWS CloudFormation 模板或类似基础架构，例如代码模板。有些合作伙伴提供了支持一键式集成的用户界面。

配置不应超过15分钟。您的产品文件还必须为您的整合提供配置指南。

每位客户每天的平均结果

如果您将结果发送到 Security Hub.

您预计将发送至每月（平均和最大值）的每月查找更新数量 Security Hub 您的客户群？ 数量级估计值可接受。

Latency

如果您将结果发送到 Security Hub.

您将如何快速批处理并将结果发送至 Security Hub? 换句话说，在产品中创建发现时的延迟是多少？ Security Hub?

这些信息必须反映在您的整合产品文件中。这是客户的常见问题。

公司和产品描述

所有与 Security Hub.

简要描述您的公司和产品，特别重点介绍 Security Hub 集成。我们在我们的 Security Hub 合作伙伴页面。

如果您正在整合多个产品， Security Hub，您可以为每个产品提供单独的描述，但我们将把它们融入合作伙伴页面的单个条目。

每个描述的空格不能超过700个字符。

合作伙伴网站资产

所有与 Security Hub.

您至少必须提供一个URL用于 了解更多 超链接 Security Hub 合作伙伴页面。它应该是一个营销登陆页面，描述您的产品与 Security Hub.

如果您将多个产品与 Security Hub，您可以为他们提供单个登录页面。 Security Hub 建议此登录页面包含配置说明的链接。

您还可以提供其他资源链接，例如博客、网络研讨会、演示视频或白皮书。 Security Hub 也将链接到他们的合作伙伴页面。

“合作伙伴徽标”页面

所有需要 Security Hub 集成。

提供一个URL以显示在 Security Hub 合作伙伴页面。徽标必须符合以下标准:

- 大小:600x300像素
- 裁剪:无衬垫
- 背景:透明
- 格式 PNG

标识 Security Hub 控制台

所有集成都需要。

提供一个URL以显示在 Security Hub 控制台。徽标必须符合以下标准:

- 尺寸:175x40像素
- 裁剪:紧密无衬垫
- 背景:透明
- 格式 PNG

有关小徽标的详细指南，请参阅 the section called “控制台徽标指南” (p. 23).

查找类型

如果您将结果发送到 Security Hub.

提供一个表格，用于记录您使用的ASFF格式化查找类型以及它们如何与您的本地查找类型对齐。有关ASFF中查找类型的详细信息，请参阅 ASFF类型分类 在 AWS Security Hub 用户指南.

我们建议您在产品文件中添加此信息。

热线

所有与 Security Hub.

为联系人的技术点提供电子邮件地址和电话号码或寻呼机号码。 Security Hub 就任何技术问题与此联系人进行沟通，例如集成不再工作。

还提供全天候的高严重性技术问题联系人。

心跳寻找

如果您将结果发送到 Security Hub.

您能否发送 Security Hub 每五分钟发现“心跳”结果，表明您与 Security Hub 是否功能？

如果可以，请使用查找类型 `Heartbeat`.

AWS Security Hub 控制台信息

将JSON文本提供给 AWS Security Hub 包含以下信息的团队。 Security Hub 使用此信息创建您的产品 ARN，在控制台中显示提供商列表，并在 Security Hub Insight库。

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	Description
`id`	是	公司的唯一标识符。公司标识符在公司间必须是唯一的。 这可能与或类似于 `name`. Type ：字符串 最小长度:5个字符 最大长度:24个字符 允许的字符: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束。
`name`	是	要在 Security Hub 控制台。 Type ：字符串 最大长度:16个字符
`description`	是	供应商公司的描述显示在 Security Hub 控制台。 Type ：字符串 最大长度:200个字符

产品信息

本节提供有关您产品的信息。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	Description
`IntegrationType`	是	指明您的产品是否将发现发送到 Security Hub，接收来自 Security Hub，或者发送和接收发现。

字段	必填	Description
		如果您是咨询合作伙伴，请将此字段留空。 Type 字符串阵列 有效值：{、} `SEND_FINDINGS_TO_SECURITY_HUB` || `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	是	产品的唯一标识符。在公司内，这些必须是唯一的。他们不需要在公司内独树一帜。这可能与 `name`. Type ：字符串 最小长度:5个字符 最大长度:24个字符 允许的字符: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束。
`regionsNotSupported`	是	以下哪项 AWS 您不支持哪些地区？ 换言之，在哪些地区 Security Hub 不会在我们的合作伙伴页面中显示您的选项 Security Hub 控制台？ Type ：字符串 仅提供地区代码。例如：`us-west-1`。 如需区域列表，请参阅 区域端点 在 AWS General Reference. 区域代码 AWS GovCloud (US) 是 `us-gov-west-1` （对于 AWS GovCloud (US-West))和 `us-gov-east-1` （对于 AWS GovCloud（美国东部））。 地区代码 中国区域 是 `cn-north-1` （对于 中国（北京））)和 `cn-northwest-1` （对于 中国 (宁夏)）。

字段	必填	Description
`commercialAccountNumber`	是	主要 AWS 产品账号 AWS 地区。 如果您将结果发送至 Security Hub，您提供的帐户基于您发出的发现的位置。 • 从您的 AWS 账户。在这种情况下，提供您用于提交发现的账号。 • 从客户的 AWS 账户。在这种情况下， Security Hub 建议您提供用于测试集成的主要帐号。 理想情况下，您将在所有地区使用相同的产品帐户。如果不可能，请联系 Security Hub 团队。 如果您只接收来自 Security Hub，此帐号不是必填项。 Type ：字符串
`govcloudAccountNumber`	否	主要 AWS 产品账号 AWS GovCloud (US) 地区（如果您的产品可用 AWS GovCloud (US)）。 如果您将结果发送至 Security Hub，您提供的帐户基于您发出的发现的位置。 • 从您的 AWS 账户。在这种情况下，提供您用于提交发现的账号。 • 从客户的 AWS 账户。在这种情况下， Security Hub 建议您提供用于测试集成的主要帐号。 理想情况下，您可以在所有产品中使用同一个客户 AWS GovCloud (US) 地区。如果不可能，请联系 Security Hub 团队。 如果您只接收来自 Security Hub，此帐号不是必填项。 Type ：字符串

字段	必填	Description
`chinaAccountNumber`	否	主要 AWS 中国地区产品账号（如果您的产品在中国地区）。 如果您将结果发送至 Security Hub，您提供的帐户基于您发出的发现的位置。 • 从您的 AWS 账户。在这种情况下，提供您用于提交发现的账号。 • 从客户的 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帐号。 理想情况下，您可以在所有中国区域使用相同的产品帐户。如果不可能，请联系 Security Hub 团队。 如果您只接收来自 Security Hub，这可以是您在中国地区拥有的任何账户。 Type ：字符串
`name`	是	要在 Security Hub 控制台。 Type ：字符串 最大长度:24个字符
`description`	是	提供商产品的描述显示在 Security Hub 控制台。 Type ：字符串 最大长度:200个字符

`importType`	是	合作伙伴的资源策略类型。
		
		在合作伙伴入职流程中，您可以指定以下资源策略之一，或者您可以指定 `NEITHER`.
		
		• 带有 `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`，您只能从产品ARN中列出的账户发送发现。
		• 带有 `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`，您只能从订阅的客户账户发送结果。
		
		Type ：字符串
		
		有效值:
		`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
		||
		`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`
		||
		
		`NEITHER`

字段	必填	Description
`category`	是	定义产品的类别。您的选择显示在 Security Hub 控制台。 最多选择三个类别。 不允许自定义选择。如果您认为类别缺失，请联系 Security Hub 团队。 Type 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` • `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)`

字段	必填	Description
		• 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 • 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	产品的URL AWS Marketplace 目的地。URL显示在 Security Hub 控制台。 Type ：字符串 必须是 AWS Marketplace URL。 如果您没有 AWS Marketplace 列表，将此字段留空。

字段	必填	Description
`configurationUrl`	是	与您的产品文档相关的URL Security Hub. 此内容在您的网站上或您管理的网页上托管，例如Github页面。 Type ：字符串 您的文件应包含以下信息。 • 配置说明 • 链接至 AWS CloudFormation 模板（如有必要） • 关于整合使用情况的信息 • Latency • ASFF映射 • 包括的结果类型 • 架构

指南和检查表

为您准备所需材料时 AWS Security Hub 集成，使用这些指南。

准备检查清单用于对整合进行最终审核 Security Hub 使其可以 Security Hub 客户。

主题

徽标上显示的标识指南 AWS Security Hub 控制台

要显示在 AWS Security Hub 控制台，遵循这些指南。

格式

PNG文件格式

Background color

透明背景是优选的。

如果背景不透明，请使用纯白色背景。

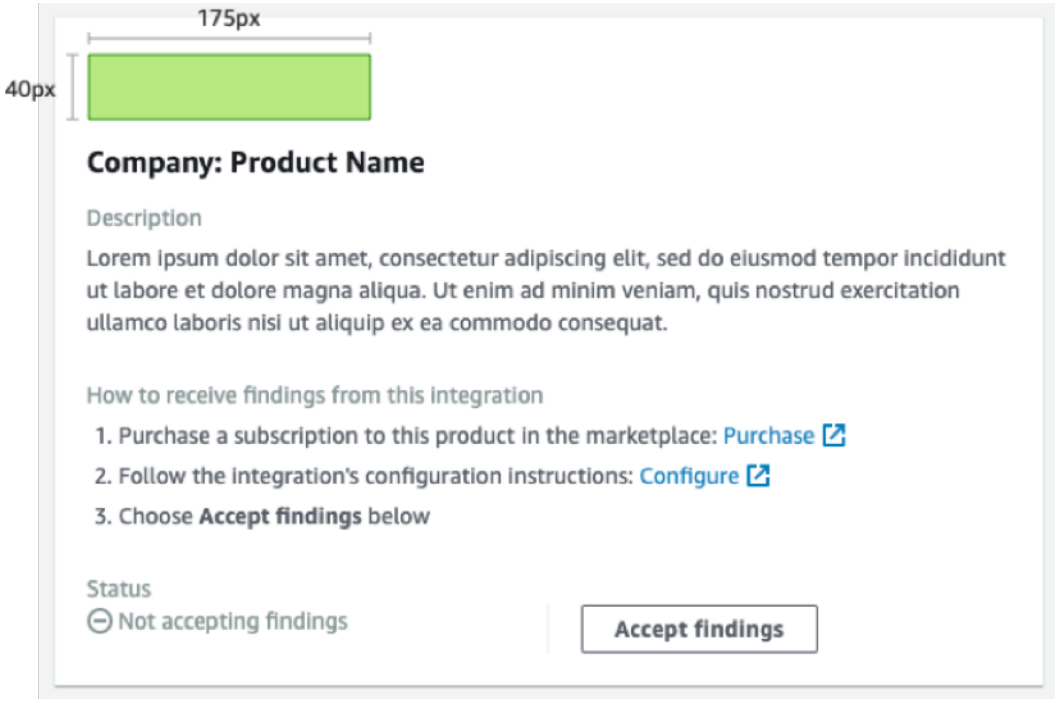
Size

理想尺寸为175px宽x40px高。

最小高度为40px。

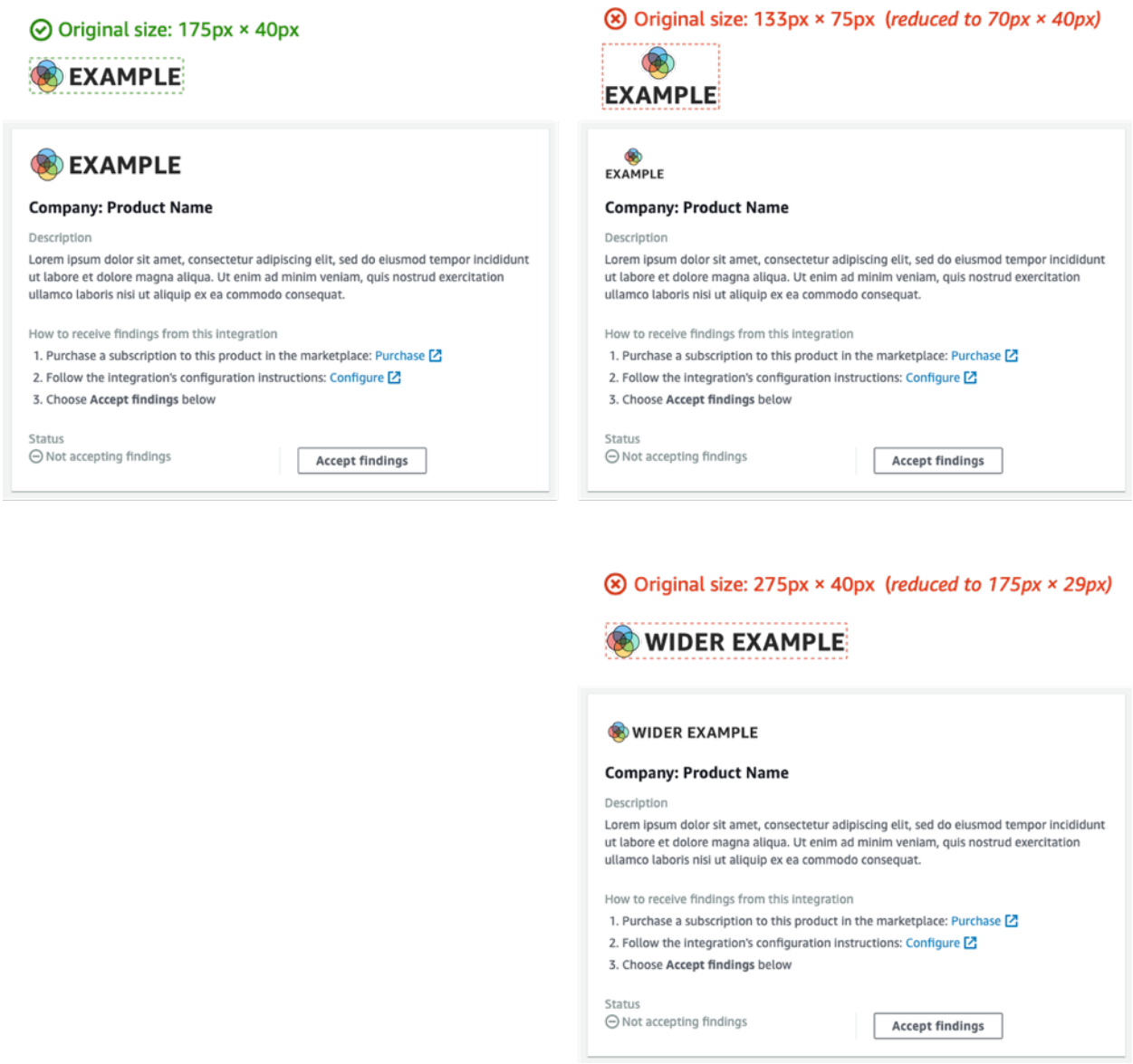
矩形徽标最佳工作。

下图显示了如何在 Security Hub 控制台。



如果您的徽标与这些尺寸不匹配，安全枢纽将大小降低到40px的最大高度，最大宽度为175px。这会影响徽标在 Security Hub 控制台。

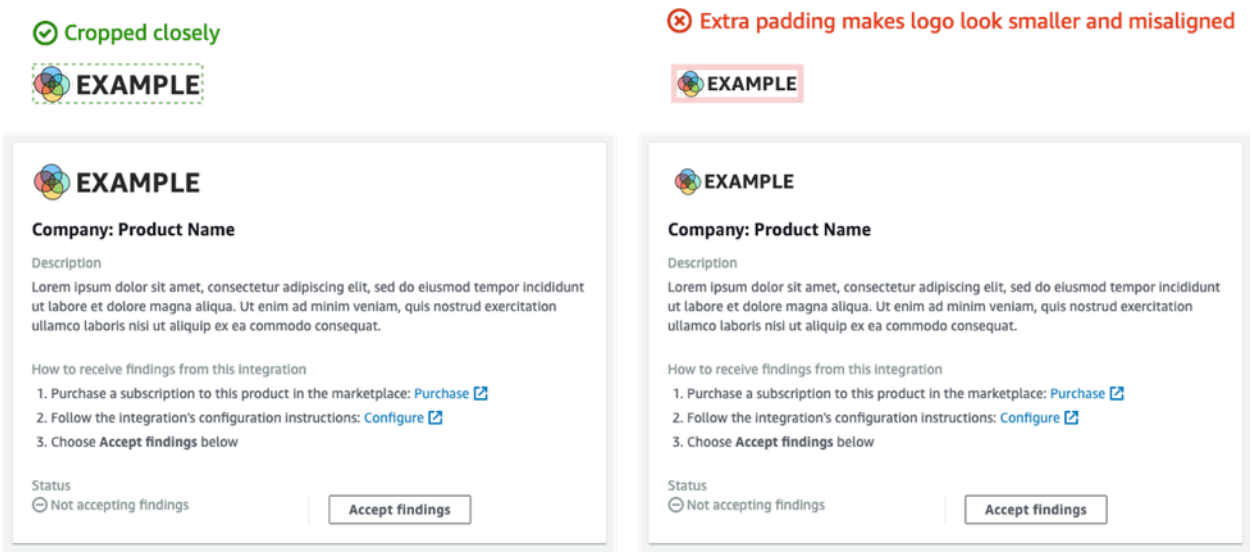
以下图像比较了徽标的显示屏，该徽标的理想尺寸是更宽或更高。



裁剪

尽可能缩短徽标图像。不要提供额外的衬垫。

以下图片显示了一个标识与附加衬垫的徽标之间的差异。



将结果映射到AWS安全发现格式(ASFF)的指南

使用以下指南将您的结果映射到ASFF。有关每个ASFF字段和对象的详细描述，请参阅 AWS安全查找格式(ASFF) 在 AWS Security Hub 用户指南.

识别信息

`SchemaVersion` 始终为 `2018-10-08`。

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

`Id` 是价值 Security Hub 用于索引结果。查找标识符必须唯一，以确保其他结果不会被覆盖。要更新查找，请使用相同标识符重新提交查找。

`GeneratorId` 可以与 `Id` 或者可以参考离散逻辑单元，例如 Amazon GuardDuty 检测器ID， AWS Config 记录器ID，或 IAM 访问分析仪ID。

Title $and Description

`Title` 应包含有关受影响资源的一些信息。`Title` 不超过256个字符，包括空格。

添加更多详细信息至 `Description`。 `Description` 限制为1024个字符，包括空格。您可以考虑将截断添加到描述。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

`Types` 应匹配 ASFF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格式包括一些不同的时间戳。

`CreatedAt` 和 `UpdatedAt`

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

值必须与Python3.8的ISO8601格式匹配。

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

`FirstObservedAt` 和 `LastObservedAt`

`FirstObservedAt` 和 `LastObservedAt` 在系统观察到发现时必须匹配。如果您未记录此信息，则无需提交这些时间戳。

值与Python3.8的ISO8601格式匹配。

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

Severity

对于新发现，您可以在 `Severity` 对象。

`Original`

系统的严重性值。`Original` 可以是任何字符串，以适应您使用的系统。

`Label`

所需的 Security Hub 发现严重性的指示符。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，以防止进一步伤害。

您可以设置 `Label` 只有当您创建新的发现。对于现有的调查结果，只有客户可以更改 `Label`.

合规的结果应始终具有 `Label` 设置为 `INFORMATIONAL`。示例 `INFORMATIONAL` 结果是通过的安全检查结果 AWS Firewall Manager 已补救的结果。

客户通常按照其严重程度排序结果，向其安全运营团队提供待办事项列表。将查找严重性设置为 `HIGH` 或 `CRITICAL`.

您的整合文件必须包含您的映射理由。

Remediation

`Remediation` 有两个元素。这些元素与 Security Hub 控制台。

`Remediation.Recommendation.Text` 显示在 补救 查找详细信息的部分。它与 `Remediation.Recommendation.Url`.

目前只有来自 Security Hub 标准， IAM 访问分析仪，和 Firewall Manager 显示有关如何修复发现的文档的超链接。

SourceUrl

仅使用 `SourceUrl` 如果您可以为该特定查找提供控制台的深度链接URL。否则，将其从映射中忽略。

Security Hub 不支持此字段中的超链接，但是 Security Hub 控制台。

Malware, Network, Process, ThreatIntelIndicators

如适用，请使用 `Malware`， `Network`， `Process`，或 `ThreatIntelIndicators`。这些对象中的每个对象都在 Security Hub 控制台。在发现发现的情况下使用这些对象。

例如，如果检测到对已知命令和控制节点进行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` 该EC2实例的对象。

Malware

`Malware` 是接受最多五个恶意软件信息的列表。使其与资源和发现相关的恶意软件条目。

每个条目都有以下字段。

`Name`

恶意软件的名称。该值最多为64个字符。

`Name` 应来自审查的威胁情报或研究人员。

`Path`

恶意软件的路径。该值最多为512个字符。`Path` 应为Linux或Windows系统文件路径，但以下情况除外。

- 如果您在S3桶中扫描对象或EFS分享的YARA规则，那么 `Path` S3://或HTTPS对象路径。
- 如果您扫描了GIT存储库中的文件，那么 `Path` 是GITURL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，确保您提供恶意软件发生的情况。

例如，如果 `Malware.State` 是 `REMOVED`，然后，查找标题和描述应反映您的产品已删除位于Path上的恶意软件。

IFIFIF `Malware.State` 是 `OBSERVED`，然后，查找标题和描述应反映出您的产品在路径上遇到此恶意软件。

`Type`

表示恶意软件的类型。允许的值为 `ADWARE` || `BLENDED_THREAT` || `BOTNET_AGENT` || `COIN_MINER` || `EXPLOIT_KIT` || `KEYLOGGER` || `MACRO` || `POTENTIALLY_UNWANTED` || `SPYWARE` || `RANSOMWARE` || `REMOTE_ACCESS` || `ROOTKIT` || `TROJAN` || `VIRUS` || `WORM`.

如果您需要其他值 `Type`，联系 Security Hub 团队。

Network

`Network` 是单个对象。您无法添加多个网络相关的详细信息。在映射字段时，请使用以下指南。

目的地和源信息

目标和源易于地图TCP或VPC流量日志或WAF日志。当您描述关于攻击的网络信息时，它们更难使用。

通常，源是发起的攻击，但可能有以下列出的其他来源。您应该解释文件中的来源，并在查找标题和描述中描述。

- 对于EC2实例上的DDos攻击，源是攻击者，但真正的DDos攻击可能使用数百万主机。目标是ec2实例的公共Ipv4地址。`Direction` 位于。
- 对于观察到ec2实例与已知命令和控制节点通信的恶意软件，源是ec2实例的Ipv4地址。目标是命令和控制节点。`Direction` 是 `OUT`。您还将提供 `Malware` 和 `ThreatIntelIndicators`.

`Protocol`

`Protocol` 除非您可以提供特定协议，否则始终映射到已分配的编号权限(IANA)注册名称。您应始终使用此信息并提供端口信息。

`Protocol` 独立于源信息和目标信息。只有在有意义的情况下才能提供。

`Direction`

`Direction` 始终相对于 AWS 网络边界。

- `IN` 意味着 AWS （VPC、服务）。
- `OUT` 意味着 AWS 网络边界。

Process

`Process` 是单个对象。您无法添加多个与流程相关的详细信息。在映射字段时，请使用以下指南。

`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` 是流程可执行文件的文件系统路径。最多可接受512个字符。

`Pid`, **`ParentPid`**

`Pid` 和 `ParentPid` 应与Linux过程标识符(PID)或Windows事件ID匹配。要区分，请使用EC2Amazon机器图像(AMI)提供信息。客户可能会在Windows和Linux之间区分。

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

如果您无法可靠地检索这些信息，并且这些信息不准确，请勿提供。

如果客户依赖于取证调查的时间戳，则没有时间戳优于错误时间戳。

ThreatIntelIndicators

`ThreatIntelIndicators` 接受多达5个威胁智能对象的阵列。

对于每个条目， `Type` 在特定威胁的情况下。允许的值为 `DOMAIN` || `EMAIL_ADDRESS` || `HASH_MD5` || `HASH_SHA1` || `HASH_SHA256` || `HASH_SHA512` || `IPV4_ADDRESS` || `IPV6_ADDRESS` || `MUTEX` || `PROCESS` || `URL`.

以下是如何映射威胁情报指标的一些示例:

- 您找到了一个您知道与CobaltStrike相关的流程。您从FireEye博客中学到了这一点。

  设置 `Type` 至 `PROCESS`。同时创建 `Process` 进程对象。
- 您的邮件筛选器发现某人从已知的恶意域发送了一个知名的哈希包。

创建两个 `ThreatIntelIndicator` 对象。一个对象是 `DOMAIN`。另一个是 `HASH_SHA1`.

- 您发现了YARA规则的恶意软件（Loki、Fenrir、Awss3VirusScan、BinaryAlert）。

  创建两个 `ThreatIntelIndicator` 对象。一个用于恶意软件。另一个是 `HASH_SHA1`.

Resources

对于 `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。要收到ASFF更改的每月日志，请联系 `<SecurityHub-Partners@Amazon.com>`.

如果您不能适合建模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`.

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

您还可以使用 `Other` 非-资源类型AWS 结果。

ProductFields

仅使用 `ProductFields` 如果您不能使用其他策划字段 `Resources` 或描述性对象，例如 `ThreatIntelIndicators`， `Network`，或 `Malware`.

如果您使用 `ProductFields`，您必须为此决策提供严格的理由。

合规性

仅使用 `Compliance` 如果您的研究结果与合规性相关。

Security Hub 使用 `Compliance` 根据控制措施生成的结果。

Firewall Manager 使用 `Compliance` 因为它们与合规相关。

受限字段

这些字段旨在让客户跟踪其调查结果。

不要映射到这些字段或对象。

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

如果您要映射到以下字段，您只能在创建新的查找结果时填写这些字段 Security Hub. 您不能使用 `BatchImportFindings` 要更改现有查找中这些字段和对象的值。

- `Confidence` – 如果您的服务具有类似功能，或者您的发现100%，则只包括信心评分(0-99)。

  Security Hub 不会在 Security Hub 控制台。信心分数只存储在发现中。
- `Criticality` – 关键性评分(0-99)旨在表达与发现相关的资源的重要性。

  Security Hub 不会揭示 Security Hub 控制台。关键性分数只存储在发现中。
- `RelatedFindings` – 只有当您能够跟踪与相同资源或发现类型相关的结果时，才能提供相关的结果。要识别相关的发现，您必须参考已经中的查找标识符 Security Hub.

使用 BatchImportFindings API

使用 BatchImportFindings 将结果发送到API操作 AWS Security Hub，使用以下指南。

- 发送您可以使用的最大批次。 Security Hub 最多可接受100个结果或240KB每批，以先到者为准。
- 油门速率限制为10TPS，连拍30TPS。
- 如果存在限制或网络问题，您必须实施一个机制来保留结果状态。您还需要查找状态，以便您可以将发现更新提交到合规中的调查结果中。
- 有关字符串最大长度和其他限制的信息，请参阅 AWS安全查找格式(ASFF) 在 AWS Security Hub 用户指南.

产品准备检查清单

TheThethe AWS Security Hub APN合作伙伴团队使用此检查清单验证整合是否已准备就绪。

ASFF映射

这些问题与AWS安全发现格式(ASFF)的映射有关。

所有合作伙伴的查找数据都映射到ASFF吗？

以某种方式将所有调查结果地图。

使用建模资源类型等策划字段， Network， Malware，或 ThreatIntelIndicators.

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

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** 要定义未在ASFF中建模的资源详情？

在可能的情况下，在您的调查结果中使用EC2实例、S3桶和安全组等规划资源的提供字段。

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。

合作伙伴地图值是否为 **UserDefinedFields**?

请勿使用 UserDefinedFields。

考虑使用另一个策划字段，例如 Resource.Details.Other 或 ProductFields.

合作伙伴地图信息是否为 **ProductFields** 可以映射到其他ASFF字段？

仅使用 ProductFields 对于特定于产品的信息，例如版本控制信息、产品特定的严重性结果或无法映射到策划字段或 Resources.Details.Other.

合作伙伴是否导入自己的时间戳 **FirstObservedAt**?

TheThethe FirstObservedAt 时间戳用于记录在产品中观察到发现的时间。如果可能，映射此字段。

合作伙伴是否提供针对每个查找标识符生成的唯一值，但他们希望更新的结果除外？

所有调查结果 Security Hub 在查找标识符上编制索引（ Id 属性）。该值必须始终是唯一的，以确保结果不会意外更新。

您还应该维护查找标识符状态以更新结果。

合作伙伴是否提供将结果映射到发生器ID的值？

GeneratorID 不应与查找ID的值相同。

`GeneratorID` 应能够根据生成的结果来实现逻辑链接结果。

这可以是产品（产品A-漏洞与产品A-EDR）或类似物品的子组件。

合作伙伴是否使用与其产品相关的所需查找类型名称Pacpaces？ 合作伙伴是否使用建议的查找类型类别或分类器来查找其类型？

发现类型分类应密切地映射产品生成的结果。

AWS安全发现格式中概述的一级命名空间是必需的。

您可以使用二级和三级命名空间（类别或分类器）的自定义值。

合作伙伴是否采集网络流信息 **`Network`** 字段，如果他们有网络数据？

如果您的产品捕获Netflow信息，请将其映射到 `Network` 字段。

合作伙伴捕获流程(PID)信息是否在 **`Process`** 字段，如果他们有流程数据？

如果产品捕获流程信息，请将其映射到 `Process` 字段。

合作伙伴是否在 **`Malware`** 字段，如果他们有恶意软件数据？

如果您的产品捕获恶意软件信息，请将其映射到 `Malware` 字段。

合作伙伴是否会在 **`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。

合作伙伴是否为发现提供了信心评级？ 如果他们做的话，是否提供了理由？

在您使用该字段时，请在您的文件和清单中提供理由。

合作伙伴是否在发现中使用资源ID的典型ID或ARN？

识别 AWS 资源，最好的做法是使用ARN。如果ARN不可用，请使用典型资源ID。

集成设置和功能

这些问题与整合的设置和日常功能有关。

合作伙伴是否提供基础架构为代码(IAC)模板来部署与 Security Hub，例如Terraform， AWS CloudFormation，或 AWS 云开发工具包 (AWS CDK)?

对于将从客户账户或使用中发出的结果 CloudWatch Events 要消耗结果，需要一些IAC模板形式。

AWS CloudFormation 优先，但是 AWS CDK 也可以使用Terraform。

合作伙伴产品是否在其控制台上安装一键式设置，以便与 Security Hub?

某些合作伙伴产品使用产品中的切换或类似机制来激活集成。这可能会自动配置资源和权限。如果您从产品帐户发出结果，一键式设置是首选方法。

合作伙伴是否仅发送价值发现？

您通常只发送具有安全值的结果 Security Hub 客户。

Security Hub 不是一般日志管理工具。您不应将每个可能的日志发送到 Security Hub.

合作伙伴是否提供了每个客户每天发送的发现的估计结果，以及频率（平均和突发）？

用于计算负载的唯一结果数量 Security Hub. 独特的发现定义为从另一个发现中具有不同ASFF映射的发现。

例如，如果只填充一个查找 `ThreatIntelndicators` 另一个已填充 `Resources.Details.AWSEc2Instance`，这些是两个独特的发现。

合作伙伴是否拥有处理4XX和5XX错误的优雅方式，这样他们不会受到限制，而且可以稍后发出所有调查结果？

目前有30个–50TPS突发速率 `BatchImportFindings` API操作。如果返回了4xx或5xx错误，您必须保留这些失败的结果的状态，以便您可以在Totality后重试。您可以通过一个死字母队列或其他 AWS 消息传递服务，如 Amazon SNS 或 Amazon SQS.

合作伙伴是否维持发现状态，以便他们知道存档结果不再存在？

如果您计划通过覆盖原始发现ID来更新结果，则必须有一个保留状态的机制，以便更新正确的信息。

如果您提供发现，请勿使用 `BatchUpdateFindings` 操作以更新结果。此操作只能由客户使用。您仅使用 `BatchUpdateFindings` 当您调查并对结果采取行动时。

合作伙伴的处理是否以之前发送成功发现的方式重试？

您应该有一种机制来保留错误情况下的原始查找ID，以便在错误中不复制或覆盖成功的结果。

合作伙伴是否通过致电 **`BatchImportFindings`** 使用现有结果的查找ID的操作？

要更新查找，您必须通过提交相同的查找ID来覆盖现有查找。

TheThethe `BatchUpdateFindings` 操作只能由客户使用。

合作伙伴是否使用 **`BatchUpdateFindings`** API？

如果您对结果采取行动，您可以使用 `BatchUpdateFindings` 操作以更新特定字段。

合作伙伴是否提供有关创建发现的时间范围以及从产品发送到 Security Hub?

您应尽量减少延迟，以确保客户尽快查看结果 Security Hub.

清单中需要此信息。

如果合作伙伴的架构是从客户账户发送结果到安全枢纽，他们是否已成功展示这一点？ 如果合作伙伴的体系结构是将结果发送到 Security Hub 在他们自己的账户中，他们是否已成功展示这一点？

在测试期间，必须从您拥有的账户中成功发送结果，该帐户与产品ARN提供的帐户不同。

从产品ARN业主帐户发送查找可以绕过API操作的某些错误例外。

合作伙伴是否会发现 Security Hub?

要显示您的集成正常工作，您应发送心跳结果。心跳发现每5分钟发送一次，并使用查找类型 `Heartbeat`.

如果您从产品账户发出结果，这很重要。

合作伙伴是否与 Security Hub 测试期间的产品团队帐户？

在生产前验证期间，您应将发现示例发送到 Security Hub 产品团队 AWS 账户。这些示例显示发现结果已正确发送和映射。

文档：

这些问题与您提供的整合文件相关。

合作伙伴是否在专用网站上主持文档？

文档应作为静态网页、Wiki、阅读文件或其他专用格式托管在您的网站上。

Github上的托管文件不符合专用网站要求。

合作伙伴文件是否提供了如何设置 Security Hub 集成？

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。

合作伙伴文件是否提供其使用案例的描述？

您在清单中提供的使用情况也应在文件中描述

合作伙伴文件是否为发现发现提供理由？

您应该提供发出的结果类型的理由。

例如，您的产品可能会产生漏洞、恶意软件和防病毒的结果，但您只会将漏洞和恶意软件发现发送到 Security Hub. 在这种情况下，您必须提供您不发送防病毒发现的理由。

合作伙伴文件是否提供了合作伙伴如何将结果映射到ASFF的理由？

您应该提供产品本地发现对ASFF的映射理由。客户想知道哪里寻找特定产品信息。

合作伙伴文件是否提供了如何更新结果的合作伙伴更新结果的指导？

向客户提供如何保留状态的信息、确保能效以及使用最新信息覆盖发现的信息。

合作伙伴文件是否描述了发现延迟？

最大限度地减少延迟，以确保客户尽快查看结果 Security Hub.

清单中需要此信息。

合作伙伴文件是否描述了其严重性评分如何映射到ASFF严重性评分？

提供有关您如何地图的信息 `Severity.Original` 至 `Severity.Label`.

例如，如果您的严重性值为字母级别(A,B,C)，您应该提供如何将字母级别映射至严重性标签的信息。

合作伙伴文件是否提供了信心评级的理由？

如果您提供信心评分，这些分数应排列。

如果您使用来自人工智能或机器学习的静态填充的信心评分或映射，则应提供其他背景。

合作伙伴文件是否记录合作伙伴所做的哪些地区并且不支持？

注意不支持或不支持的地区，以便客户知道哪些地区不会尝试集成。

产品卡信息

这些问题与显示在 集成 第页，共页 Security Hub 控制台。

提供的 AWS 帐户ID有效，包含12位数字？

账户标识符长12位。如果帐户ID包含少于12位数，则产品ARN将无效。

产品描述是否包含200个或更少字符？

清单中的JSON中提供的产品描述不应超过200个字符，包括空格。

配置链接是否导致集成的文档？

配置链接应导致您的在线文档。它不应导致您的主网站或营销页面。

购买链接（如果提供）导致 AWS Marketplace 产品列表？

如果您提供购买链接，则必须为 AWS Marketplace 条目。 Security Hub 不接受未由 AWS.

产品类别是否正确描述产品？

在清单中，您可以提供最多三个产品类别。这些应与JSON匹配，不能为自定义。您不能提供三个以上的产品类别。

公司和产品名称是否有效且正确？

公司名称必须为16个或更少个字符。

产品名称必须为24个或更少字符。

产品卡JSON中的产品名称必须与清单中的名称匹配。

营销信息

这些问题与整合的营销相关。

是指 Security Hub 在700个字符内的合作伙伴页面，包括空格？

TheThethe Security Hub 合作伙伴页面最多可接受700个字符，包括空格。

团队将编辑更长的描述。

是 Security Hub 合作伙伴页面徽标不超过600x300px？

在PNG或JPG中提供公司徽标的公开访问URL，不超过600x300像素。

在 Security Hub 合作伙伴页面向合作伙伴的专用网页提供了关于整合的专用网页？

TheThethe 了解更多 链接不应导致合作伙伴的主网站或文件信息。

该链接应始终向专用网页上提供有关整合的营销信息。

合作伙伴是否为如何使用其集成提供演示或教学视频？

演示或集成巡视视频是可选的，但建议使用。

是 AWS 合作伙伴网络博客发布在合作伙伴及其合作伙伴发展经理或合作伙伴发展代表中？

AWS 合作伙伴网络博客帖子应提前与合作伙伴发展经理或合作伙伴发展代表协调。

它们与您自己创建的任何博客帖子分开。

允许4人–6周交货期。在使用私人产品ARN完成测试后，应开始此工作。

是否已发布合作伙伴指导的新闻稿？

您可以与您的合作伙伴发展经理或合作伙伴发展代表合作，获得外部安全服务副总裁的报价。您可以在新闻稿中使用此报价。

是否发布了合作伙伴主导的博客帖子？

您可以创建自己的博客帖子，以展示 AWS 合作伙伴网络博客。

是否发布了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整合。

如果您需要 Security Hub 在使用私人产品ARN完成测试后，与产品团队合作。

合作伙伴是否请求社交媒体支持 AWS?

发布后，您可以使用 AWS 安全营销领导者使用 AWS 官方社交媒体渠道，分享有关您在线研讨会的详细信息。

AWS Security Hub 合作伙伴常见

以下是有关设置和维护与 AWS Security Hub.

1. 有哪些好处 Security Hub 集成？
   - 客户满意度 – 与 Security Hub 是因为您有客户要求。

     Security Hub 是 AWS 客户。它被设计为第一站 AWS 安全和合规专业人员每天都会了解他们的安全和合规状态。

     倾听您的客户。他们会告诉您他们是否希望在安全中心看到您的调查结果。
   - 发现机会 – 我们推广合作伙伴， Security Hub 控制台，包括链接到 AWS Marketplace 列表。这是客户探索新安全产品的绝佳方式。
   - 营销机会 – 具有批准的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，并展示他们的整合 AWS 客户。
2. 那里有哪些类型的合作伙伴？
   - 发现结果的合作伙伴 Security Hub
   - 接收发现的合作伙伴 Security Hub
   - 发送和接收结果的合作伙伴
   - 帮助客户设置、定制和使用的咨询合作伙伴 Security Hub 在他们的环境中
3. 合作伙伴如何与 Security Hub 在高层工作？

   您从客户账户或自己的客户处收集结果 AWS 将结果的格式转化为 AWS 安全查找格式(ASFF)。然后将这些结果推向适当的 Security Hub 区域端点。

   您也可以使用 CloudWatch Events 接收发现 Security Hub.
4. 完成与 Security Hub?
   a. 提交您的合作伙伴清单信息。
   b. 接收产品ARNS以与 Security Hub，如果您将发现SecurityHub。
   c. 将您的结果映射到ASFF。
   d. 定义您的体系结构，以便将结果发送到和接收发现 Security Hub.
   e. 为客户创建部署框架。例如， AWS CloudFormation 脚本可以满足此目的。
   f. 记录您的设置并为客户提供配置说明。
   g. 定义客户可与您的产品配合使用的任何自定义洞察（相关性规则）。
   h. 展示您与 Security Hub 团队。
   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、光滑片材）。
5. 提交合作伙伴清单的流程是什么？ 和 AWS 将结果发送至 Security Hub?

   将清单信息提交至 Security Hub 团队，使用 `<SecurityHub-Partners@Amazon.com>`.

   您已在七个日历日内发放产品ARNS。
6. 我应该发送什么类型的发现 Security Hub?

   Security Hub 定价部分基于所摄入的结果数量。因此，您应避免发送不为客户提供价值的发现。

   例如，一些漏洞风险管理供应商只会将发现的结果发送到可能的10分的“常见漏洞评分系统(CVSS)”分数中。

7. 我将结果发送到 Security Hub?

   以下是主要方法:

   - 您发出自己指定的调查结果 AWS 帐户使用 `BatchImportFindings` 操作。
   - 您使用 `BatchImportFindings` 操作。您可以使用假设角色的方法，但这些方法不是必要的。

8. 如何收集我的调查结果，并将其推向 Security Hub 区域终点？

   合作伙伴使用了不同的方法，因为它非常依赖于解决方案的架构。

   例如，一些合作伙伴构建了一个可以部署为 AWS CloudFormation 脚本。该脚本从客户环境中收集合作伙伴的结果，将其转化为ASFF，并将其发送到 Security Hub 区域端点。

   其他合作伙伴构建一个完整向导，让客户可以单击体验，将结果推送到 Security Hub.

9. 我如何知道何时开始发现结果 Security Hub?

   Security Hub 支持部分批次授权 `BatchImportFindings` API操作，以便您将所有发现发送到 Security Hub 对于所有客户。

   如果您的某些客户尚未订阅 Security Hub， Security Hub 没有取得这些结果。它只会进行批次中的授权发现。

10. 我需要完成哪些步骤，以将结果发送给客户 Security Hub 实例？

    a. 确保正确 IAM 政策已落实。

    b. 为帐户启用产品订阅（资源策略）。使用 `EnableImportFindingsForProduct` API操作或 集成 第页。客户可以这样做，或者您可以使用跨客户角色代表客户行事。

    c. 确保 `ProductArn` 发现是您产品的公共ARN。

    d. 确保 `AwsAccountId` “查找”是客户帐户ID。

    e. 确保您的发现没有根据AWS安全发现格式(ASFF)的任何形成的数据。例如，填充必填字段，并且没有无效值。

    f. 将结果分批发送至正确的区域端点。

11. 什么 IAM 我必须准备好发出发现的权限？

    IAM 必须为 IAM 呼叫的用户或角色 `BatchImportFindings` 或其他API调用。

    最简单的测试是从管理账户中执行此操作。您可以将这些 `action: 'securityhub:BatchImportFindings'` 和 `resource: <productArn and/or productSubscriptionArn>`.

    同一帐户中的资源可以配置 IAM 不需要资源策略的策略。

    排除 IAM 来电者的政策问题 `BatchImportFindings`，设置 IAM 来电者政策如下:

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

    确保检查是否存在 `Deny` 来电者的政策。在您处理此事之后，您可以将策略限制在以下内容中:

```
{
    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？

要从特定合作伙伴产品接收发现，客户（或代表客户工作的跨客户角色的合作伙伴）必须建立产品订阅。要从控制台中执行此操作，它们使用 集成 第页。要从API中执行此操作，它们使用 `EnableImportFindingsForProduct` API操作。

产品订阅创建一份资源政策，授权客户接收或发送合作伙伴的结果。有关详细信息，请参阅 使用案例和权限 (p. 4)。

Security Hub 合作伙伴有以下类型的资源政策:

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

在合作伙伴入职流程中，您可以申请一种或两种类型的政策。

带有 `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`，您只能将结果发送到 Security Hub 您产品的ARN中列出的账户。

带有 `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`，您只能从订阅的客户账户发送结果。

13.假设客户创建了一个主账户，并添加了一些会员帐户。客户是否需要将每个会员帐户订阅给我？ 或者客户是否只订阅主账户，然后我可以将结果与所有会员帐户中的资源发送到一起？

此问题询问是否根据主账户注册为所有会员帐户创建权限。

客户必须为每个账户订购产品订阅。他们可以通过API以编程方式进行此操作。

14.我的产品ARN是什么？

您的产品ARN是您的唯一标识符 Security Hub 为您生成并用于提交结果。您收到的产品为您与 Security Hub. 正确的产品ARN必须是您发送至 Security Hub. 没有产品ARN的结果已丢弃。产品ARN使用以下格式:

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

以下是 示例。

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

对于每个地区的产品ARN， Security Hub 已部署。账户ID、公司和产品名称由您的合作伙伴清单提交项决定。除地区代码外，您不会更改与您的产品ARN相关的任何信息。地区代码必须与您提交发现的地区匹配。

常见错误是更改帐户ID以匹配您当前正在使用的帐户。帐户ID不会更改。您提交“主页”帐户ID作为清单提交的一部分。此帐户ID被锁定到您的产品ARN中。

当 WhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhenWhen Security Hub 在新区域启动，它自动使用标准区域代码生成这些区域的产品ARNS。

每个帐户还会自动配置私人产品ARN。在您收到官方公共产品ARN之前，您可以使用此ARN测试您自己的发展账户中的导入结果。

15.应使用哪种格式将结果发送至 Security Hub?

结果必须在AWS安全发现格式(ASFF)中提供。有关详细信息，请参阅 AWS安全查找格式(ASFF) 在 AWS Security Hub 用户指南.

预期您的本土发现中的所有信息都在ASFF中完全反映。自定义字段，如 `ProductFields` 和 `Resource.Details.Other` 允许您映射不适合在预定义字段中的数据。

16.使用正确的区域端点是什么？

您必须将结果发送到 Security Hub 与客户帐户相关的区域端点。

17.在哪里可以找到区域端点列表？

查看 Security Hub 端点列表.

18.我能提交跨区域结果吗？

Security Hub 尚未支持跨区提交本土研究结果 AWS 服务，例如 Amazon GuardDuty， Amazon Macie，和 Amazon Inspector. 如果客户允许， Security Hub 不妨碍您从不同地区提交调查结果。

在这种情况下，您可以从任何地方调用区域端点，ASFF的资源信息不必与端点的区域匹配。但是，`ProductArn` 必须与端点的区域匹配。

19.发送批次的规则和准则是什么？

您可以在单次呼叫中批次最多100个结果或240KB `BatchImportFindings`。在最高限度的情况下，排队和批次尽可能多的发现。

您可以从不同账户中批处理一组结果。但是，如果批次中的任何帐户未订阅 Security Hub，整个批次失败。这是 API 网关 基线授权模式。

20.我能否将更新发送至我创建的结果？

是的，如果您提交了与同一产品ARN和相同查找ID相同的查找，它将覆盖该发现的先前数据。请注意，所有数据都被覆盖，所以您应该提交完整的查找。

对于新发现和查找更新，客户会计量并计费出来。

21.我能否将更新发送给其他人创建的结果？

是，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、SIEMS、票务系统以及安全编排、自动化和响应(SOAR)平台使用。

22.如何发现结果？

Security Hub 在最后一次更新日期后90天内出现结果。在此之后，已将已老化的结果从 Security Hub Elasticsearch 群集。

如果您更新了具有相同查找ID的查找，并且已经关闭，则创建新的查找 Security Hub.

客户可以使用 CloudWatch Events 将结果从 Security Hub. 这样做可以让所有调查结果发送至客户选择的目标。

一般而言， Security Hub 建议您每90天创建新发现，并且不会永久更新结果。

23.什么样的节拍 Security Hub 落实到位？

Security Hub 节目 `GetFindings` API呼叫，因为访问结果的建议方法正在使用 CloudWatch Events.

Security Hub 不会对内部服务、合作伙伴或客户的任何其他限制实施以下行为: API 网关 和 Lambda 调用。

24.发现的结果的及时性或延迟SLA或期望 Security Hub 来源服务？

目标是尽可能实时实施初步发现和结果更新。您应将结果发送至 Security Hub 创建后5分钟内。

25.如何接收发现 Security Hub?

要接收结果，请使用以下方法之一。

- 所有发现都将自动发送至 CloudWatch Events. 客户可以创建特定 CloudWatch Events 将结果发送到特定目标（例如SIEM或S3桶）的规则。此功能替换了传统 `GetFindings` API操作。
- 使用 CloudWatch Events 对于自定义操作。 Security Hub 允许客户从控制台中选择具体的发现结果或结果组，并对他们采取行动。例如，他们可以将结果发送到SIEM、票务系统、聊天平台或补救工作流程。这将是客户在 Security Hub. 这些称为自定义操作。

  当用户选择自定义操作时， CloudWatch 为这些具体结果创建事件。您可以充分利用这种能力并建立起来 CloudWatch Events 用作自定义操作一部分的客户的规则和目标。请注意，此功能不用于自动发送特定类型或类别的所有发现 CloudWatch Events. 用户可以对特定发现采取措施。

  您可以使用自定义操作API操作，例如 `CreateActionTarget`，为您的产品自动创建可用操作（例如，使用 AWS CloudFormation 模板）。您还将使用 CloudWatch Events 规则API操作创建相应的 CloudWatch Events 与自定义操作相关联的规则。使用 AWS CloudFormation 模板，您也可以创建 CloudWatch Events 自动从 Security Hub 所有结果或具有特定特征的所有结果。

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

您必须展示 Security Hub 作为服务交付给客户的一部分。

您应该拥有解释您使用 Security Hub.

如果MSSP是寻找提供商，他们必须证明发现结果发生在 Security Hub.

如果MSSP仅接收来自 Security Hub，他们必须至少拥有 AWS CloudFormation 模板设置 CloudWatch Events 规则。

27.非MSSPAPN咨询合作伙伴成为 Security Hub 合作伙伴？

如果您是APN咨询合作伙伴，您可以成为 Security Hub 合作伙伴。您应该提交两个有关如何帮助特定客户进行以下操作的私人案例研究。

- 设置 Security Hub 带有 IAM 客户需求的权限。
- 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 使用控制台中合作伙伴页面上的配置说明。
- 帮助客户进行定制产品集成。
- 构建与客户需求和数据集相关的自定义洞察。
- 构建自定义操作。
- 构建补救手册。
- 构建与 Security Hub 合规标准。必须通过 Security Hub 团队。

案例研究不需要公开共享。

28.我如何部署与 Security Hub 我的客户？

集成架构 Security Hub 合作伙伴产品与合作伙伴的合作伙伴的解决方案的运营方式有所不同。您应确保集成的安装流程不超过15分钟。

如果您正在将集成软件部署到客户的 AWS 环境，您应该利用 AWS CloudFormation 用于简化集成的模板。有些合作伙伴创建了一个单击的集成，强烈鼓励他们。

29.我的文件要求是什么？

您必须提供文件的链接，说明您的产品与 Security Hub，包括您的使用 AWS CloudFormation 模板。

该文件还应包含有关您使用ASFF的信息。具体来说，这应该列出您用于不同结果的ASFF查找类型。如果您有任何默认洞察定义，我们建议您在此处添加这些定义。

考虑包括其他潜在信息:

- 与 Security Hub
- 发现的结果平均数

- 您的集成架构
- 您所做的地区并不支持
- 创建结果时的延迟以及发送至安全中心的时间
- 您是否更新了结果

30.什么是自定义洞察？

我们鼓励您为您的发现定义自定义见解。洞察是轻质的相关性规则，帮助客户优先考虑最需要关注和行动的结果和资源。

Security Hub 拥有 `CreateInsight` API操作。您可以在客户帐户内创建自定义洞察，作为 AWS CloudFormation 模板。这些见解显示在客户控制台上。

31.我能提交仪表板窗口小部件吗？

目前不可以。您只能创建管理的洞察。

32.您的定价模式是什么？

查看 Security Hub 定价信息.

33.如何将调查结果提交给 Security Hub 演示账户是我整合的最终批准流程的一部分？

将结果发送到 Security Hub 演示账户使用您提供的产品ARN，使用 `us-west-2` 作为区域。研究结果应该包括 `AwsAccountId` ASFF字段。要获取演示账号，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。此数据用于公共演示。当您向我们发送这些数据时，您授权我们在演示中使用。

34.什么是错误或成功消息 **`BatchImportFindings`** 提供？

Security Hub 提供授权的响应和响应 `BatchImportFindings`。更多的成功、故障和错误消息正在发展。

35.来源服务负责的处理错误是什么？

源服务负责处理所有错误。他们必须处理错误消息、重试、限制和报警。他们还必须处理通过 Security Hub 反馈机制。

36.常见问题的解决方法有哪些？

一个 `AuthorizerConfigurationException` 由一种畸形造成 `AwsAccountId` 或 `ProductArn`.

故障排除时，请注意以下事项:

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

  账户ID不会更改为 Security Hub 在产品ARNS中提供给您的团队。

`AccessDeniedException` 当发现发送到错误账户或账户不具有 `ProductSubscription`。错误消息将包含一个资源类型 `product` 或 `product-subscription`。此错误仅在跨帐户呼叫期间发生。如果您致电 `BatchImportFindings` 使用您自己的账户，在 `AwsAccountId` 和 `ProductArn`，操作使用 IAM 与政策有关 `ProductSubscriptions`.

确保您使用的客户账户和产品帐户是实际注册账户。某些合作伙伴已使用产品ARN的产品账号，但尝试使用完全不同的帐户来呼叫 `BatchImportFindings`。在其他情况下，他们创建了 `ProductSubscriptions` 对于其他客户账户，甚至是他们自己的产品帐户。他们没有创造 `ProductSubscriptions` 对于他们尝试将结果导入到的客户帐户。

37.我在哪里发送问题、评论和漏洞？

<SecurityHub-Partners@Amazon.com>

38.我将发现发现给与全球相关的项目 AWS 服务？ 例如，我在哪里发送 IAM 相关结果？

将结果发送到检测到发现的同一区域。服务，例如 IAM，您的解决方案可能会发现 IAM 多个区域的问题。在这种情况下，发现发现发生在检测到问题的每个区域。

如果客户运行 Security Hub 在三个地区和相同的 IAM 在所有三个地区检测到问题，然后将发现发送到所有三个地区。

解决问题时，将更新发送到发送原始发现所在地区的所有地区。

文档历史合作伙伴集成指南

下表描述了本指南的文件更新。

update-history-change	update-history-description	update-history-date
本指南初始版本 (p. 43)	这个 合作伙伴集成指南 提供 AWS 合作伙伴与如何建立与 AWS Security Hub.	June 23, 2020

如果我们为英文版本指南提供翻译，那么如果存在任何冲突，将以英文版本指南为准。在提供翻译时使用机器翻译。