aws

Partner Integration Guide

AWS Security Hub

AWS Security Hub: Partner Integration Guide

Table of Contents

Descripción general de la integración de terceros conAWS Security Hub

Esta guía está diseñada paraAWSPartner Network (APN) Socios que desean crear una integración conAWS Security Hub.

Como socio de APN, puede integrarse con Security Hub de una o varias de las siguientes formas.

- Enviar hallazgos a Security Hub
- Consumir los resultados de Security Hub
- Ambos envían hallazgos y consumen los resultados de Security Hub
- Utilizar Security Hub como centro de una oferta de proveedor de servicios de seguridad administrados (MSSP)
- Consulta conAWSclientes sobre cómo implementar y utilizar Security Hub

Esta guía de incorporación se centra principalmente en los socios que envían hallazgos a Security Hub.

Temas

Por qué integrarse conAWS Security Hub?

AWS Security Hubproporciona una vista integral de las alertas de seguridad de alta prioridad y del estado de seguridad en todas las cuentas de Security Hub. Security Hub permite a los socios como usted enviar los hallazgos de seguridad a Security Hub para proporcionar a sus clientes información sobre los hallazgos de seguridad que genera.

Una integración con Security Hub puede añadir valor de las siguientes formas.

- Satisface a los clientes que han solicitado una integración de Security Hub
- Proporciona a sus clientes una vista única de susAWShallazgos relacionados con la seguridad

- Permite a los nuevos clientes descubrir su solución cuando buscan socios que proporcionan hallazgos relacionados con tipos específicos de eventos de seguridad

Antes de crear una integración con Security Hub, examine los motivos de la integración. Es más probable que una integración tenga éxito si sus clientes desean una integración de Security Hub con su producto. Puede crear una integración únicamente por razones de marketing o para adquirir nuevos clientes. Sin embargo, si crea la integración sin ninguna información actual del cliente y no tiene en cuenta las necesidades de sus clientes, es posible que la integración no produzca los resultados esperados.

Preparación para enviar hallazgos aAWS Security Hub

Como socio de APN, no puede enviar información a Security Hub para sus clientes hasta que el equipo de Security Hub le permita como proveedor de búsqueda. Para habilitar como proveedor de hallazgos, debe completar los siguientes pasos de incorporación. Al hacerlo, se garantiza una experiencia positiva de Security Hub para usted y sus clientes.

A medida que completes los pasos de incorporación, asegúrate de seguir las pautas dethe section called “Sugerencias para crear y actualizar los hallazgos”,the section called “Directrices para el mapeo del ASFF”, ythe section called “Directrices para el uso del`BatchImportFindings`API”.

1. Asigne sus hallazgos de seguridad a laAWSFormato de hallazgo de seguridad (ASFF) de.
2. Cree su arquitectura de integración para llevar los hallazgos al punto final de Regional Security Hub correcto. Para ello, definirá si enviará los hallazgos de los suyosAWSCuenta o desde las cuentas de tu cliente.
3. Pide a tus clientes que suscriban el producto a su cuenta. Para ello, pueden utilizar la consola o la`EnableImportFindingsForProduct`Operación API. Consulte[Administración de integraciones de productos](#)en laAWS Security HubGuía del usuario de.

   También puedes suscribirte el producto para ellos. Para ello, utilice un rol entre cuentas para acceder a la`EnableImportFindingsForProduct`Operación API en nombre del cliente.

   En este paso se establecen las políticas de recursos necesarias para aceptar las conclusiones de ese producto para esa cuenta.

En las siguientes publicaciones de blog se analizan algunas de las integraciones de socios existentes con Security Hub.

- Anuncio de la integración de Cloud Custodian conAWS Security Hub
- UsarAWS Fargatey Prowler para enviar los resultados de la configuración de seguridad sobreAWSservicios a Security Hub
- Cómo importarAWS ConfigEvaluaciones de reglas como hallazgos en Security Hub

Preparación para recibir los hallazgos deAWS Security Hub

Para recibir las conclusiones deAWS Security Hub, utilice una de las siguientes opciones:

- Haga que sus clientes envíen automáticamente todos los hallazgos aCloudWatchEventos: . Un cliente puede crear específicosCloudWatchreglas de eventos para enviar hallazgos a destinos específicos, como un SIEM o un bucket de S3.
- Pida a sus clientes que seleccionen conclusiones o grupos de hallazgos específicos desde la consola de Security Hub y, a continuación, tomen medidas al respecto.

Por ejemplo, sus clientes pueden enviar conclusiones a un SIEM, un sistema de emisión de tickets, una plataforma de chat o un flujo de trabajo de corrección. Esto formaría parte de un flujo de trabajo de clasificación de alertas que un cliente realiza dentro de Security Hub.

Estas acciones se denominan acciones personalizadas. Cuando un usuario realiza una acción personalizada,CloudWatchse crea para esos hallazgos específicos. Como socio, puede aprovechar esta capacidad y crearCloudWatchreglas de eventos u objetivos para que un cliente las utilice como parte de una acción personalizada. Tenga en cuenta que esta capacidad no envía automáticamente todos los hallazgos de un tipo o clase en particular aCloudWatchEventos: . Esta función es para que un usuario tome medidas sobre hallazgos específicos.

En las siguientes publicaciones de blog se describen las soluciones que utilizan la integración con Security Hub yCloudWatchEventos para acciones personalizadas.

- Cómo integrarAWS Security HubAcciones personalizadas conPagerDuty
- Cómo habilitar acciones personalizadas enAWS Security Hub
- Cómo importarAWS ConfigEvaluaciones de reglas como hallazgos en Security Hub

Recursos para obtener información sobreAWS Security Hub

Los siguientes materiales pueden ayudarle a comprender mejor elAWS Security Hubsolución y cómoAWSlos clientes pueden utilizar el servicio.

- Introducción aAWS Security HubVídeo de
- Guía del usuario de Security Hub
- Referencia de API de Security Hub
- Seminario web de incorporación

También le recomendamos que habilite Security Hub en uno de susAWScuentas y obtenga experiencia práctica con el servicio.

Requisitos previos de socios

Antes de comenzar una integración conAWS Security Hub, debe cumplir con uno de los siguientes criterios:

- Eres unAWSSelecciona Socio de nivel o superior.
- Te has unido alAWSRuta del socio del ISV, y el producto que utiliza para la integración de Security Hub ha completado unAWSRevisión técnica fundacional (FTR). A continuación, se concede al producto un «Revisado porAWS«insignias.

También debe tener en vigor un acuerdo de confidencialidad mutua conAWS.

Casos de uso de integración y permisos requeridos

AWS Security HubpermiteAWSclientes para recibir los hallazgos de los socios de APN. Los productos del socio pueden ejecutarse dentro o fuera del clienteAWSaccount. La configuración de permisos de la cuenta del cliente difiere según el modelo que utiliza el producto asociado.

En Security Hub, el cliente siempre controla qué socios pueden enviar los resultados a la cuenta del cliente. Los clientes pueden revocar los permisos de un socio en cualquier momento.

Para permitir que un socio envíe resultados de seguridad a su cuenta, el cliente se suscribe primero al producto asociado en Security Hub. El paso de suscripción es necesario para todos los casos de uso que se describen a continuación. Para obtener más detalles sobre cómo los clientes administran las integraciones de productos, consulteAdministración de integraciones de productosen laAWS Security HubGuía del usuario de.

Después de que un cliente se suscriba a un producto asociado, Security Hub crea automáticamente una política de recursos administrados. La política concede al producto de un socio permiso para utilizar`BatchImportFindings`Operación de la API para enviar resultados a Security Hub de la cuenta del cliente.

Estos son los casos comunes de los productos de socios que se integran con Security Hub. La información incluye los permisos adicionales necesarios para cada caso de uso.

Socio alojado: resultados enviados desde la cuenta de socio

Este caso de uso cubre a los socios que alojan un producto por su cuentaAWSaccount. Para enviar resultados de seguridad deAWScliente, el socio llama al`BatchImportFindings`Operación de la API desde la cuenta de producto de un socio.

Para este caso de uso, la cuenta de cliente solo necesita los permisos que se establecen cuando el cliente se suscribe al producto asociado.

En la cuenta de socio, el principal de IAM que llama al`BatchImportFindings`La operación de la API debe tener una política de IAM que permita a la entidad llamar`BatchImportFindings`.

Permitir que un producto asociado envíe conclusiones al cliente en Security Hub es un proceso de dos pasos:

1. El cliente crea una suscripción a un producto asociado en Security Hub.

2. Security Hub genera la política de recursos administrados correcta con la confirmación del cliente.

Para enviar los resultados de seguridad relacionados con la cuenta del cliente, el producto de socio utiliza sus propias credenciales para llamar alBatchImportFindingsOperación de la API.

A continuación se muestra un ejemplo de una política de IAM que otorga al principal de la cuenta de socio los permisos necesarios de Security Hub.

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

Socio alojado: resultados enviados desde la cuenta de cliente

Este caso de uso cubre a los socios que alojan un producto por su cuentaAWScuenta, pero usa un rol multicuenta para acceder a la cuenta del cliente. Se llama aBatchImportFindingsOperación de la API desde la cuenta del cliente.

Para este caso de uso, para llamar alBatchImportFindingsOperación de API, la cuenta de socio asume un rol de IAM administrado por el cliente en la cuenta del cliente.

Esta llamada se realiza desde la cuenta del cliente. Por lo tanto, la política de recursos administrados debe permitir que el ARN del producto de la cuenta del producto asociado se utilice en la llamada. La política de recursos administrados de Security Hub concede permiso para la cuenta del producto de socio y el ARN del producto asociado. El ARN del producto es el identificador único del socio como proveedor. Dado que la llamada no procede de la cuenta del producto asociado, el cliente debe conceder permiso explícitamente para que el producto asociado envíe los resultados a Security Hub.

La práctica recomendada para los roles multicuenta entre cuentas de socio y cliente es utilizar un identificador externo que proporciona el socio. Este identificador externo forma parte de la definición

de la política multicuenta de la cuenta del cliente. El socio debe proporcionar el identificador cuando asume el rol. Un identificador externo proporciona una capa adicional de seguridad al concederAWSacceso a una cuenta de un socio. El identificador exclusivo garantiza que el socio utilice la cuenta de cliente correcta.

La habilitación de un producto de socio para enviar hallazgos al cliente en Security Hub con una función multicuenta se realiza en cuatro pasos:

1. El cliente, o socio que utiliza funciones multicuentas que trabajan en nombre del cliente, inicia la suscripción a un producto en Security Hub.
2. Security Hub genera la política de recursos administrados correcta con la confirmación del cliente.
3. El cliente configura el rol entre cuentas de forma manual o medianteAWS CloudFormation. Para obtener más información sobre roles entre cuentas, consulteProporcionar acceso aAWScuentas de propiedad de tercerosen laIAM User Guide.
4. El producto almacena de forma segura la función de cliente y el ID externo.

A continuación, el producto envía los resultados a Security Hub:

1. El producto llama alAWS Security Token Service(AWS STS) para asumir la función de cliente.
2. El producto llama al`BatchImportFindings`Operación de API en Security Hub con las credenciales temporales del rol asumido.

A continuación se muestra un ejemplo de política de IAM que concede los permisos de Security Hub necesarios a la función entre cuentas del socio.

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

La`Resource`de la política identifica la suscripción del producto específica. Esto garantiza que el socio solo pueda enviar los hallazgos del producto asociado al que está suscrito el cliente.

Alojado por el cliente: resultados enviados desde la cuenta de cliente

Este caso de uso cubre a los socios que tienen un producto que se implementa en elAWSaccount. La`BatchImportFindings`La API se llama desde la solución que se ejecuta en la cuenta del cliente.

En este caso de uso, se deben conceder permisos adicionales al producto asociado para llamar al`BatchImportFindings`API. La forma en que se concede este permiso difiere en función de la solución de socio y de cómo se configura en la cuenta del cliente.

Un ejemplo de este enfoque es un producto asociado que se ejecuta en una instancia EC2 de la cuenta del cliente. Esta instancia de EC2 debe tener un rol de instancia EC2 asociado que otorgue a esa instancia la capacidad de llamar al`BatchImportFindings`Operación de la API. Esto permite que la instancia de EC2 envíe los resultados de seguridad a la cuenta del cliente.

Este caso de uso equivale funcionalmente a un escenario en el que un cliente carga los hallazgos en su cuenta de un producto que posee.

El cliente permite que el producto asociado envíe los resultados de la cuenta del cliente al cliente en Security Hub:

1. El cliente implementa el producto de socio en suAWScuenta manualmente usandoAWS CloudFormation, u otra herramienta de implementación.
2. El cliente define la política de IAM necesaria para que el producto de socio utilice cuando envía conclusiones a Security Hub.
3. El cliente adjunta la política a los componentes necesarios del producto asociado, como una instancia EC2, un contenedor o una función Lambda.

Ahora, el producto puede enviar los resultados a Security Hub:

1. El producto asociado utiliza elAWSSDK oAWS CLIllamar a`BatchImportFindings`Operación de la API en Security Hub. Realiza la llamada desde el componente de la cuenta del cliente a la que se adjunta la póliza.

2. Durante la llamada a la API, se generan las credenciales temporales necesarias para permitir elBatchImportFindingsllama a tener éxito.

A continuación se muestra un ejemplo de una política de IAM que otorga los permisos de Security Hub necesarios al producto asociado de la cuenta de cliente.

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

Proceso de incorporación de socios

Como socio, puede esperar completar varios pasos de alto nivel como parte de su proceso de incorporación. Debe completar estos pasos antes de poder enviar los resultados de seguridad aAWS Security Hub.

1. Inicias un compromiso con el equipo de socios de APN o el equipo de Security Hub y expresas interés en convertirte en socio de Security Hub. Identifica las direcciones de correo electrónico que desea agregar a los canales de comunicación de Security Hub.
2. AWSle proporciona los materiales de incorporación de socios de Security Hub.
3. Te invitamos al canal de Slack, socio de Security Hub, donde puedes hacer preguntas relacionadas con tu integración.
4. Proporciona a los contactos de socios de APN un borrador del manifiesto de integración de productos para su revisión.

   El manifiesto de integración de productos contiene información que se utiliza para crear el producto asociado Amazon Resource Name (ARN) para la integración conAWS Security Hub.

   Proporciona al equipo de Security Hub información que aparece en la página del proveedor de socios de la consola de Security Hub. También se utiliza para proponer nuevos conocimientos administrados relacionados con la integración y agregarlos a la biblioteca de información de Security Hub.

   Esta versión inicial del manifiesto de integración de productos no tiene por qué tener los detalles completos. Sin embargo, debería contener al menos la información del caso de uso y del conjunto de datos.

   Para obtener información detallada acerca del manifiesto y la información necesaria, consulteManifiesto de integración de productos.
5. El equipo de Security Hub le proporciona un ARN de producto para su producto. El ARN se utiliza para enviar los hallazgos a Security Hub.
6. Cree su integración para enviar hallazgos o recibir hallazgos de Security Hub.

   Mapeo de los hallazgos al ASFF

   Para enviar los hallazgos a Security Hub, debe asignar los hallazgos a laAWSFormato de hallazgo de seguridad de (ASFF) de.

El ASFF proporciona una descripción coherente de los resultados que se pueden compartir entreAWSservicios de seguridad, socios y sistemas de seguridad para clientes. Esto reduce los esfuerzos de integración, fomenta un lenguaje común y proporciona un plan para los implementadores.

ASFF es el formato de protocolo de cable requerido que se debe utilizar para enviar los hallazgos aAWS Security Hub. Los hallazgos se representan como documentos JSON que se adhieren al esquema JSON ASFF y RFC-7493 El formato de mensaje I-JSON. Para obtener más información sobre el esquema ASFF, consulteAWSFormato de los hallazgos de seguridad de (ASFF)en laAWS Security HubGuía del usuario de.

Consulte the section called “Directrices para el mapeo del ASFF”.

Creación y prueba de la integración

Puede completar todas las pruebas de su integración mediante unAWScuenta de la suya. Al hacerlo, obtendrá una visibilidad completa de cómo aparecen los hallazgos en Security Hub. También le ayuda a comprender la experiencia del cliente con sus hallazgos de seguridad.

Usa el`BatchImportFindings`Operación de API para enviar hallazgos nuevos y actualizados a Security Hub.

A lo largo de la creación de una integración de Security Hub,AWSle anima a mantener informados a sus contactos de socios de APN sobre el progreso de su integración. También puede solicitar ayuda a los contactos de socios de APN para obtener ayuda con las preguntas de integración.

Consulte the section called “Directrices para el uso del`BatchImportFindings`API”.

7. Demuestra la integración al equipo de productos de Security Hub. Esta integración debe demostrarse utilizando una cuenta que posee el equipo de Security Hub.

   Si se sienten cómodos con la integración, el equipo de Security Hub da la aprobación para avanzar y incluirlo como proveedor.

8. Usted proporcionaAWScon un manifiesto final para revisión.
9. El equipo de Security Hub crea la integración de proveedores en la consola de Security Hub. A continuación, los clientes pueden descubrir y habilitar la integración.
10. (Opcional) Participa en esfuerzos de marketing adicionales para promover la integración de Security Hub. Consulte Go-to-marketActividades de.

Como mínimo, Security Hub recomienda proporcionar los siguientes activos.

- Vídeo de demostración (3 minutos como máximo) de la integración de trabajo. El vídeo se utiliza con fines de marketing y se publica en elAWS YouTubechannel.
- Diagrama de arquitectura de una diapositiva para agregar a la presentación de diapositivas de primera llamada de Security Hub.

Go-to-marketActividades de

Los socios también pueden participar en actividades de marketing opcionales para ayudar a explicar y promover susAWS Security HubIntegración de.

Si quieres crear tu propio contenido de marketing relacionado con Security Hub, antes de publicar el contenido, envía un borrador a tu administrador de socios de APN para que lo revise y apruebe. Esto garantiza que todos estén alineados con la mensajería.

AWSLos socios de la Red de socios (APN) pueden utilizar la Central de Marketing de Partner de APN y el programa de Fondos de Desarrollo de Mercado (MDF) para crear campañas y obtener apoyo financiero. Para obtener más información sobre estos programas, póngase en contacto con el gerente de socios.

Entrada en la página de socios de Security Hub

Una vez que se haya aprobado como socio de Security Hub, su solución se puede mostrar en elAWS Security Hubpágina de socios.

Para aparecer en esta página, proporcione los siguientes detalles a los contactos de socios de APN. Puede ser su gestor de desarrollo de socios (PDM), arquitecto de soluciones de socios (PSA) o un correo electrónico a`<securityhub-pms@amazon.com>`.

- Una breve descripción de su solución, su integración con Security Hub y el valor que la integración con Security Hub proporciona a los clientes. Esta descripción está limitada a 700 caracteres, incluidos los espacios.
- URL de una página que describe la solución. Este sitio debe ser específico de suAWSintegración y, más concretamente, la integración de Security Hub. Debe centrarse en la experiencia del cliente y en el valor que reciben los clientes cuando utilizan la integración.
- Una copia de alta resolución de su logotipo de 600 x 300 píxeles. Para obtener más información sobre los requisitos de este logotipo, consultethe section called “Logotipo para la página de socios”.

Notas de prensa

Como socio aprobado, puede publicar opcionalmente un comunicado de prensa en su sitio web y canales de relaciones públicas. El comunicado de prensa debe ser aprobado porAWS.

Antes de publicar el comunicado de prensa, debe enviarlo aAWSpara su revisión por parte del marketing de socios de APN, el liderazgo de Security Hub yAWSServicios de seguridad externos (ESS). El comunicado de prensa puede incluir una propuesta de presupuesto para el vicepresidente de ESS.

Para iniciar este proceso, trabaje con su PDM. Tenemos un acuerdo de nivel de servicio (SLA) de 10 días hábiles para revisar los comunicados de prensa.

AWSBlog de la red de socios (APN)

También podemos ayudarlo a publicar una entrada de blog que cree en el blog de APN. La entrada del blog debe centrarse en la historia de un cliente y un caso de uso. No se puede posicionar únicamente en torno a ser un socio de lanzamiento de integración.

Si está interesado, póngase en contacto con su PDM o PSA para iniciar el proceso. Los blogs de APN pueden tardar 8 semanas o más en aprobarse y publicarse finales.

Aspectos clave que debe saber sobre el blog de APN

Cuando cree una publicación de blog, tenga presentes los siguientes elementos.

¿Qué incluye una publicación de blog?

- Las publicaciones de los socios deben ser educativas y proporcionar una amplia experiencia sobre un tema relevante paraAWSclientes.
- La longitud ideal no es superior a 1.500 palabras. Los lectores valoran el contenido educativo profundo que les enseña lo que es posible enAWS.
- El contenido debe ser original del blog de APN. No vuelva a utilizar contenido de fuentes como publicaciones de blog o documentos técnicos existentes.

¿Cuáles son otros límites para publicar en el blog de APN?

- Solo los socios de nivel Advanced o Premier pueden publicar en el blog de APN. Existen excepciones para los socios Select que tienen una designación de programa de APN, como la prestación de servicios.
- Cada socio está limitado a tres puestos por año. Con decenas de miles de socios de APN,AWSdebe ser equitativa en su cobertura.

Cada publicación debe tener un patrocinador técnico que pueda validar la solución o el caso de uso.

¿Cuánto tiempo lleva editar una publicación de blog antes de que se publique?

Después de enviar el primer borrador completo de la publicación del blog, tarda de cuatro a seis semanas en editarse.

¿Por qué escribir para el blog de APN?

Una publicación de blog de APN puede proporcionar los siguientes beneficios.

- Credibilidad— Para los socios de APN, tener una historia publicada porAWSpuede influir en los clientes a nivel mundial.
- Visibility— El blog de APN es uno de los blogs más leídos enAWScon 1,79 millones de visitas de páginas en 2019, incluido el tráfico influido.
- Negocio— Las publicaciones de socios de APN tienen botones de conexión que pueden generar clientes potenciales a través del programa de participación del cliente (ACE) de APN.

¿Qué tipo de contenido es el que mejor se ajusta?

Los siguientes tipos de contenido son los más adecuados para una publicación de blog de APN.

- El contenido técnico es el tipo de historia más popular. Esto incluye focos de solución e información práctica. Más del 75% de los lectores analizan este contenido técnico.
- Los clientes valoran historias de 200 niveles o superiores que demuestran cómo funciona algo enAWSo cómo un socio de APN resolvió un problema empresarial para los clientes.
- Las publicaciones escritas por expertos técnicos o expertos en la materia tienen el mejor desempeño por mucho.

Hoja de marketing o hoja de marketing

Una hoja elegante es un documento de una página que describe el producto, su arquitectura de integración y los casos de uso conjuntos de clientes.

Si creas una hoja elegante para tu integración, envía una copia al equipo de Security Hub. Lo añadirán a la página de socios.

Libro blanco o libro electrónico

Si crea un documento técnico o un libro electrónico que describa su producto, su arquitectura de integración y casos de uso conjuntos de clientes, envíe una copia al equipo de Security Hub. Lo agregarán a la página de socios de Security Hub.

Seminario web de

Si realiza un seminario web sobre su integración, envíe una grabación del seminario web al equipo de Security Hub. El equipo se vinculará a él desde la página de socios.

El equipo también puede proporcionar un experto en temas de Security Hub para que participe en su seminario web.

Vídeo de demostración

Para fines de marketing, puede producir un vídeo de demostración de la integración de trabajo. Publica dicho vídeo en la cuenta de tu plataforma de vídeo y el equipo de Security Hub lo vinculará desde la página del socio.

Manifiesto de integración de productos

Cada socio deAWS Security Hub integración debe completar un manifiesto de integración de productos que proporcione los detalles necesarios para la integración propuesta.

El equipo de Security Hub utiliza esta información de varias maneras:

- Para crear el listado de tu sitio web
- Para crear la tarjeta de producto para la consola de Security Hub
- Para informar al equipo de producto de su caso de uso.

Para evaluar la calidad de la integración propuesta y la información proporcionada, el equipo de Security Hub utiliza elthe section called “Lista de comprobación de preparación del producto”. Esta lista de verificación determina si la integración está lista para lanzarse.

Toda la información técnica que proporcione también debe reflejarse en la documentación.

Puede descargar una versión en PDF del manifiesto de integración de productos en la sección Recursos de la página deAWS Security Hub socios. Tenga en cuenta que la página de socios no está disponible en las regiones China (Pekín) y China (Ningxia).

Contenido

  - Línea directa
  - Detección de latidos
- AWS Security Hubinformación de la consola
  - Información de la empresa
  - Información del producto

Caso de uso e información de marketing

Los siguientes casos de uso pueden ayudarle a configurarAWS Security Hub para diferentes propósitos.

Caso práctico para encontrar proveedores y consumidores

Necesario para los proveedores de software independientes (ISV).

Para describir su caso práctico en torno a su integración conAWS Security Hub, responda a las siguientes preguntas. Si no tiene previsto enviar ni recibir los hallazgos, anótelo en esta sección y, a continuación, complete la siguiente.

La siguiente información debe estar reflejada en su documentación.

- ¿Enviará los hallazgos, los recibirá o ambos?
- Si tiene previsto enviar hallazgos, ¿qué tipos de hallazgos enviará? ¿Enviará todos los hallazgos o un subconjunto específico de hallazgos?
- Si planea recibir los hallazgos, ¿qué hará con esos hallazgos? ¿Qué tipos de hallazgos recibirá? Por ejemplo, ¿recibirá todos los hallazgos, los hallazgos de un tipo determinado o solo los hallazgos específicos que seleccione un cliente?
- ¿Tiene previsto actualizar los hallazgos? Si es así, ¿qué campos actualizará? Security Hub recomienda actualizar los hallazgos en lugar de crear siempre otros nuevos. La actualización de los hallazgos existentes ayuda a reducir el ruido de búsqueda para los clientes.

  Para actualizar una búsqueda, envía una búsqueda con un identificador de búsqueda que se asigna a una búsqueda que ya ha enviado.

Para recibir comentarios anticipados sobre su caso de uso y sus conjuntos de datos, póngase en contacto con el equipo de APN Partner o Security Hub.

Caso de uso de Consulting Partner (CP)

Obligatorio si es socio consultor de Security Hub.

Proporcione dos casos de uso de clientes para su trabajo con Security Hub. Estos pueden ser casos de uso privado. El equipo de Security Hub no los anuncia en ningún lado. Deben describir una de las siguientes acciones o ambas.

- ¿Cómo ayuda a los clientes a poner en marcha Security Hub? Por ejemplo, ¿ha ayudado a los clientes a utilizar servicios profesionales, un módulo de Terraform o unaAWS CloudFormation plantilla?
- ¿Cómo ayuda a los clientes a poner en funcionamiento y ampliar Security Hub? Por ejemplo, ¿ha proporcionado plantillas de respuesta o corrección, ha creado integraciones personalizadas o ha utilizado herramientas de inteligencia empresarial para configurar un panel ejecutivo?

Conjuntos de datos

Obligatorio si envía los resultados a Security Hub.

Para los hallazgos que enviará a Security Hub, proporcione la siguiente información.

- Los hallazgos en su formato nativo, como JSON o XML
- Un ejemplo de cómo convertirá los resultados alAWS Security Finding Format (ASFF)

Informe al equipo de Security Hub si necesita alguna actualización del ASFF para respaldar su integración.

Arquitectura

Obligatorio si envía o recibe los resultados de Security Hub.

Describa cómo se integrará con Security Hub. Esta información también debe estar reflejada en su documentación.

Debe proporcionar diagramas de arquitectura. A la hora de preparar los diagramas de arquitectura, tenga en cuenta lo siguiente:

- ¿QuéAWS servicios, agentes del sistema operativo, etc. utilizará?

- Si va a enviar los hallazgos a Security Hub, ¿los enviará desde laAWS cuenta del cliente o desde su propiaAWS cuenta?
- Si va a recibir hallazgos, ¿cómo utilizará la integración de CloudWatch eventos?
- ¿Cómo va a convertir los hallazgos en ASFF?
- ¿Cómo agrupará los hallazgos, realizará un seguimiento del estado de búsqueda y evitará limitar los límites?

Configuración

Obligatorio si envía o recibe los resultados de Security Hub.

Describa cómo un cliente configurará su integración con Security Hub.

Como mínimo, debe utilizarAWS CloudFormation plantillas o una infraestructura similar, como plantillas de código. Algunos socios han proporcionado una interfaz de usuario para permitir la integración con un solo clic.

La configuración no debería tardar más de 15 minutos. La documentación del producto también debe proporcionar una guía de configuración para la integración.

Promedio de hallazgos por día por cliente

Obligatorio si envía los resultados a Security Hub.

¿Cuántas actualizaciones de búsqueda al mes (promedio y máximo) espera enviar a Security Hub a toda su base de clientes? Se aceptan estimaciones de órdenes de magnitud.

Latency (Latencia)

Obligatorio si envía los resultados a Security Hub.

¿Con qué rapidez tardará procesar por lotes y enviar los resultados a Security Hub? En otras palabras, ¿cuál es la latencia desde que se crea el hallazgo en el producto hasta que se envía a Security Hub?

Esta información debe reflejarse en la documentación del producto para la integración. Es una pregunta habitual de los clientes.

Descripción de la empresa y del producto

Necesario para todas las integraciones con Security Hub.

Describa brevemente su empresa y su producto, con un énfasis específico en la naturaleza de su integración con Security Hub. La utilizamos en nuestra página de socios de Security Hub.

Si va a integrar varios productos con Security Hub, puede proporcionar una descripción independiente para cada producto, pero los combinaremos en una sola entrada en la página de socios.

Cada descripción no puede tener más de 700 caracteres con espacios.

Activos del sitio web de

Necesario para todas las integraciones con Security Hub.

Como mínimo, debe proporcionar una URL para usarla como hipervínculo Más información en la página de socios de Security Hub. Debe ser una página de inicio de marketing que describa la integración entre el producto y Security Hub.

Si integra varios productos con Security Hub, puede tener una sola página de destino para ellos. Security Hub recomienda que esta página de destino incluya un enlace a las instrucciones de configuración.

También puede proporcionar enlaces a otros recursos, como blogs, seminarios web, vídeos de demostración o documentos técnicos. Security Hub también enlazará a ellos desde la página de sus socios.

Logotipo para la página de socios

Necesario para todas las integraciones de Security Hub.

Proporcione la URL de un logotipo para que aparezca en la página de socios de Security Hub. El logotipo debe cumplir los siguientes criterios:

- Tamaño: 600 x 300 píxeles
- Recorte: ajustado y sin relleno
- Fondo: transparente

- Formato: PNG

Logotipos para la consola Security Hub

Necesario para todas las integraciones.

Proporcione las URL de los logotipos del modo claro y del modo oscuro para que se muestren en la consola de Security Hub.

Los logotipos deben cumplir los siguientes criterios:

- Formato: SVG
- Tamaño: 175 x 40 píxeles. Si es más grande, la imagen debe utilizar esa proporción.
- Recorte: ajustado sin relleno
- Fondo: transparente

Para obtener instrucciones detalladas sobre el logotipo pequeño, consultethe section called "Directrices para el logotipo de la consola".

Búsqueda de tipos

Obligatorio si envía los resultados a Security Hub.

Proporcione una tabla que documente los tipos de búsqueda con formato ASFF que utiliza y cómo se alinean con los tipos de búsqueda nativos. Para obtener más información sobre cómo buscar tipos en ASFF, consulte la taxonomía de tipos de ASFF en la Guía delAWS Security Hub usuario.

Es recomendable que también incluya esta información en la documentación del producto.

Línea directa

Necesario para todas las integraciones con Security Hub.

Proporcione una dirección de correo electrónico y un número de teléfono o número de localizador para un punto de contacto técnico. Security Hub se comunicará con este contacto en relación con cualquier problema técnico, por ejemplo, cuando una integración deje de funcionar.

También proporcione un punto de contacto las 24 horas del día, los 7 días de la semana para problemas técnicos de alta gravedad.

Detección de latidos

Se recomienda si envía los resultados a Security Hub.

¿Puede enviar a Security Hub un «latido» cada cinco minutos que indique que su integración con Security Hub funciona?

Si puede, hágalo utilizando el tipo de búsquedaHeartbeat.

AWS Security Hubinformación de la consola

Proporcione alAWS Security Hub equipo un texto JSON que contenga la información. Security Hub utiliza esta información para crear el ARN del producto, mostrar la lista de proveedores en la consola e incluir la información gestionada propuesta en la biblioteca de información de Security Hub.

Información de la empresa

La información de la empresa proporciona información sobre su empresa. A continuación se muestra un ejemplo:

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

La información de la empresa contiene los siguientes campos:

Campo	Obligatorio	Descripción
id	Sí	El identificador único de la empresa. El identific ador de la empresa debe ser único en todas las empresas. Es probable que sea igual o similar aname. Tipo: String Longitud mínima: 5 caracteres

Campo	Obligatorio	Descripción
		Longitud máxima: 24 caracteres Caracteres permitidos: letras minúsculas, números y guiones Debe comenzar con una letra minúscula. Debe terminar con una letra minúscula o un número.
`name`	Sí	El nombre de la empresa del proveedor que se mostrará en la consola de Security Hub. Tipo: String Longitud máxima: 16 caracteres
`description`	Sí	La descripción de la empresa del proveedor que se mostrará en la consola de Security Hub. Tipo: String Longitud máxima: 200 caracteres

Información del producto

En esta sección, se proporciona información acerca de su producto. A continuación se muestra un ejemplo:

```
{
    "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"
}
```

La información del producto contiene los siguientes campos.

Campo	Obligatorio	Descripción
`IntegrationType`	Sí	Indica si el producto envía los hallazgos a Security Hub, si los recibe de Security Hub o si ambos envían y reciben los hallazgos. Si es un socio de Tipo: Matriz de cadena Valores válidos: `SEND_FINDINGS_TO_SECURITY_HUB` | `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	Sí	El identificador único del producto. Deben ser únicos dentro de una empresa. No tienen por qué ser únicos en todas las empresas. Es probable que sea igual o similar a `name`. Tipo: String Longitud mínima: 5 caracteres Longitud máxima: 24 caracteres Caracteres permitidos: letras minúsculas, números y guiones Debe comenzar con una letra minúscula. Debe terminar con una letra minúscula o un número.
`regionsNotSupported`	Sí	¿Cuáles de las siguientesAWS regiones no son compatibles? En otras palabras, ¿en qué regiones Security Hub no debería mostrarle

Campo	Obligatorio	Descripción
		como opción en la página de socios de la consola de Security Hub? Tipo: String Proporcione únicamente el código de región. Por ejemplo, `us-west-1` . Para ver una lista de las regiones, consulte los puntos de enlace regionales en la Referencia general de AWS. Los códigos de región para elAWS GovCloud (US) son`us-gov-west-1` (paraAWS GovCloud (US-Oeste)) y`us-gov-east-1` (paraAWS GovCloud (US-Este)). Los códigos de región para las regiones de China son`cn-north-1` (para China (Beijing)) y`cn-northwest-1` (para China (Ningxia)).

Campo	Obligatorio	Descripción
`commercialAccountNumber`	Sí	El número deAWS cuenta principal del producto para lasAWS regiones. Si envía los hallazgos a Security Hub, la cuenta que proporcione se basará en el lugar desde el que envíe los hallazgos. • Desde tuAWS cuenta. En este caso, proporcione el número de cuenta que utiliza para enviar las conclusiones. • Desde laAWS cuenta del cliente. En este caso, Security Hub recomienda que proporcione el número de cuenta principal que utiliza para probar la integración. Lo ideal es que utilices la misma cuenta para todos tus productos en todas las regiones. Si esto no es posible, póngase en contacto con el equipo de Security Hub. Si solo recibe información de Security Hub, este número de cuenta no es obligatorio. Tipo: String

Campo	Obligatorio	Descripción
`govcloudAccountNumber`	No	El número deAWS cuenta principal del producto paraAWS GovCloud (US) Regions (si el producto está disponible enAWS GovCloud (US)). Si envía los hallazgos a Security Hub, la cuenta que proporcione se basará en el lugar desde el que envíe los hallazgos. • Desde tuAWS cuenta. En este caso, proporcione el número de cuenta que utiliza para enviar las conclusiones. • Desde laAWS cuenta del cliente. En este caso, Security Hub recomienda que proporcione el número de cuenta principal que utiliza para probar la integración. Lo ideal es que utilices la misma cuenta para todos tus productos en todasAWS GovCloud (US) las regiones. Si esto no es posible, póngase en contacto con el equipo de Security Hub. Si solo recibe información de Security Hub, este número de cuenta no es obligatorio. Tipo: String

Campo	Obligatorio	Descripción
`chinaAccountNumber`	No	El número deAWS cuenta principal del producto para las regiones de China (si el producto está disponible en las regiones de China). Si envía los hallazgos a Security Hub, la cuenta que proporcione se basará en el lugar desde el que envíe los hallazgos. • Desde tuAWS cuenta. En este caso, proporcione el número de cuenta que utiliza para enviar las conclusiones. • Desde laAWS cuenta del cliente. En este caso, Security Hub recomienda que proporcione el número de cuenta principal que utiliza para probar la integración del producto. Lo ideal es que utilices la misma cuenta para todos tus productos en todas las regiones de China. Si esto no es posible, póngase en contacto con el equipo de Security Hub. Si solo recibe información de Security Hub, puede tratarse de cualquier cuenta que posea en una región de China. Tipo: String
`name`	Sí	El nombre del producto del proveedor que se mostrará en la consola de Security Hub. Tipo: String Longitud máxima: 24 caracteres

Campo	Obligatorio	Descripción
`description`	Sí	La descripción del producto del proveedor que se mostrará en la consola de Security Hub. Tipo: String Longitud máxima: 200 caracteres
`importType`	Sí	El tipo de política de recursos del socio. Durante el proceso de incorporación de socios de`NEITHER` • Con`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, solo puede enviar los hallazgos a Security Hub desde la cuenta que figura en el ARN del producto. • Con`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, solo puedes enviar los resultados de la cuenta de cliente a la que te suscribiste. Tipo: String Valores válidos: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` |`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` | `NEITHER`

Campo	Obligatorio	Descripción
`category`	Sí	Las categorías que definen tu producto. Sus selecciones se muestran en la consola de Security Hub. Elige hasta tres categorías. No se permiten selecciones personalizadas. Si cree que falta su categoría, póngase en contacto con el equipo de Security Hub. Tipo: matriz Categorías disponibles: • `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 Managemen t` • `Configuration and Patch Management` • `Configuration Management Database (CMDB)` • `Consulting Partner` • `Container Security` • `Cyber Range` • `Data Access Management` • `Data Classification`

Campo	Obligatorio	Descripción
		• 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) • Human Resources Information System • Interactive Application Security Testing (IAST) • Instant Messaging • IoT Security • IT Security Training • IT Ticketing and Incident Management

Campo	Obligatorio	Descripción
		• `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`	No	La URL delAWS Marketplace destino del producto. La URL se muestra en la consola de Security Hub. Tipo: String Debe ser unaAWS Marketplace URL. Si no tiene unAWS Marketplace anuncio, deje este campo en blanco.

Campo	Obligatorio	Descripción
`configurationUrl`	Sí	La URL de la documentación del producto acerca de la integración con Security Hub. Este contenido se aloja en su sitio web o en una página web que usted administre, como una GitHub página. Tipo: String La documentación debe incluir la información. • Instrucciones de configuración • Enlaces aAWS CloudFormation plantillas (si es necesario) • Información sobre su caso de uso de la integración • Latency (Latencia) • Mapeo de ASFF • Tipos de hallazgos • Arquitectura

Directrices y listas de comprobación

A medida que preparas los materiales necesarios para tuAWS Security Hubintegración, utilice estas directrices.

La lista de comprobación de preparación se utiliza para realizar una revisión final de la integración antes de que Security Hub la ponga a disposición de los clientes de Security Hub.

Temas

Directrices para que el logotipo se muestre en elAWS Security Hubconsola

Para que el logotipo se muestre en elAWS Security HubConsole, siga estas directrices.

Modos claro y oscuro

Debe proporcionar un modo claro y una versión en modo oscuro del logotipo.

Formato

Formato de archivo SVG

Background color (Color de fondo)

Transparent

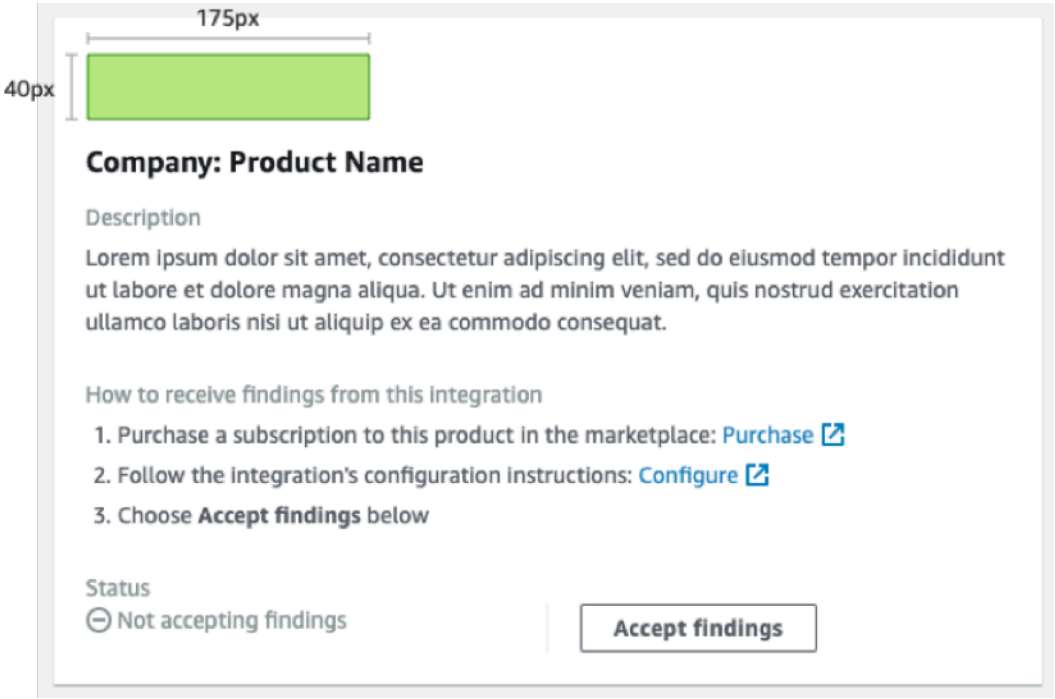
Size

La relación ideal es de 175 px de ancho por 40 px de alto.

La altura mínima es de 40 px.

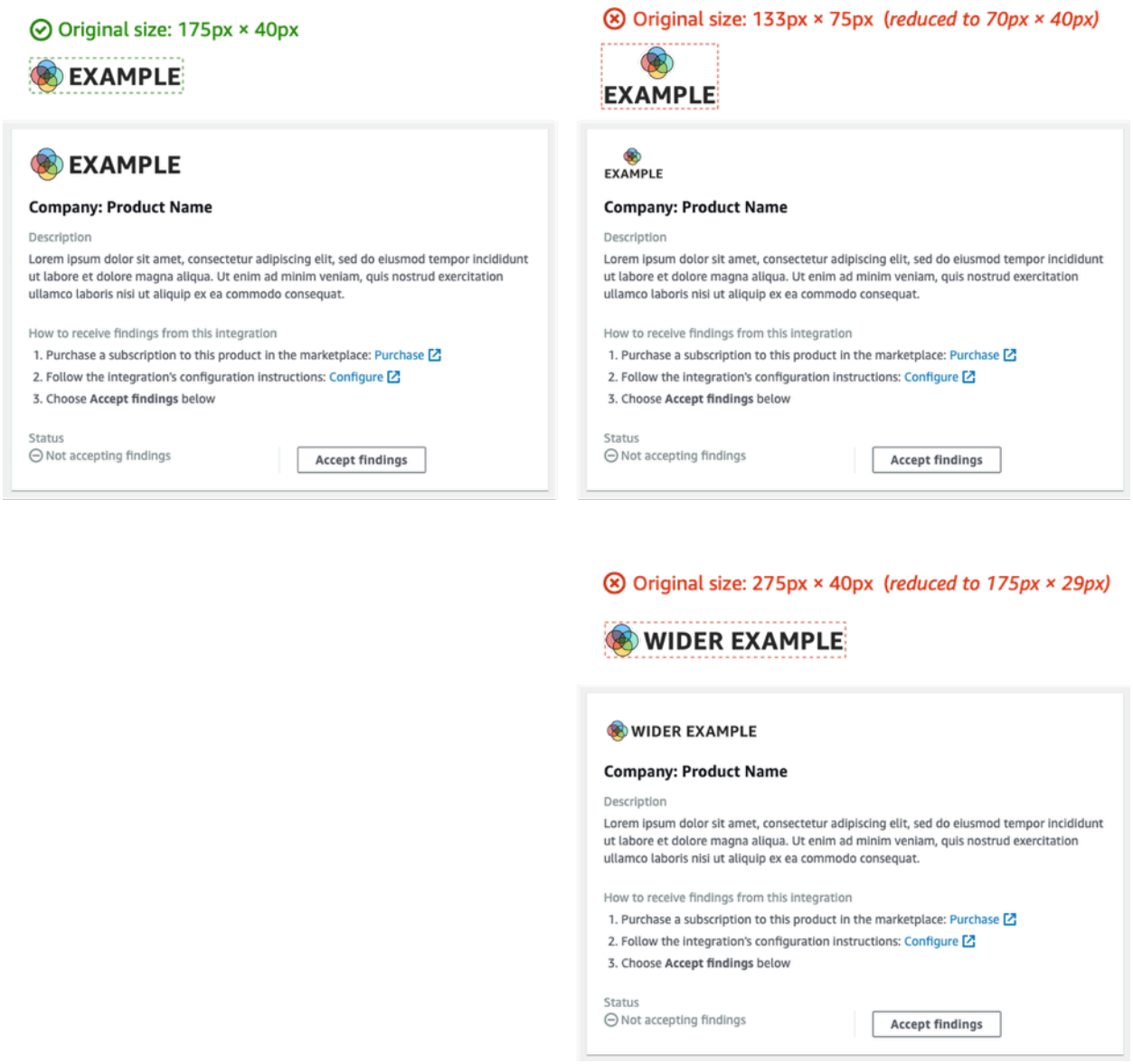
Los logotipos rectangulares funcionan mejor.

La imagen siguiente muestra cómo se muestra un logotipo ideal en la consola de Security Hub.



Si tu logotipo no coincide con estas dimensiones, Security Hub reduce el tamaño a una altura máxima de 40 px y un ancho máximo de 175 px. Esto afecta a cómo se muestra el logotipo en la consola de Security Hub.

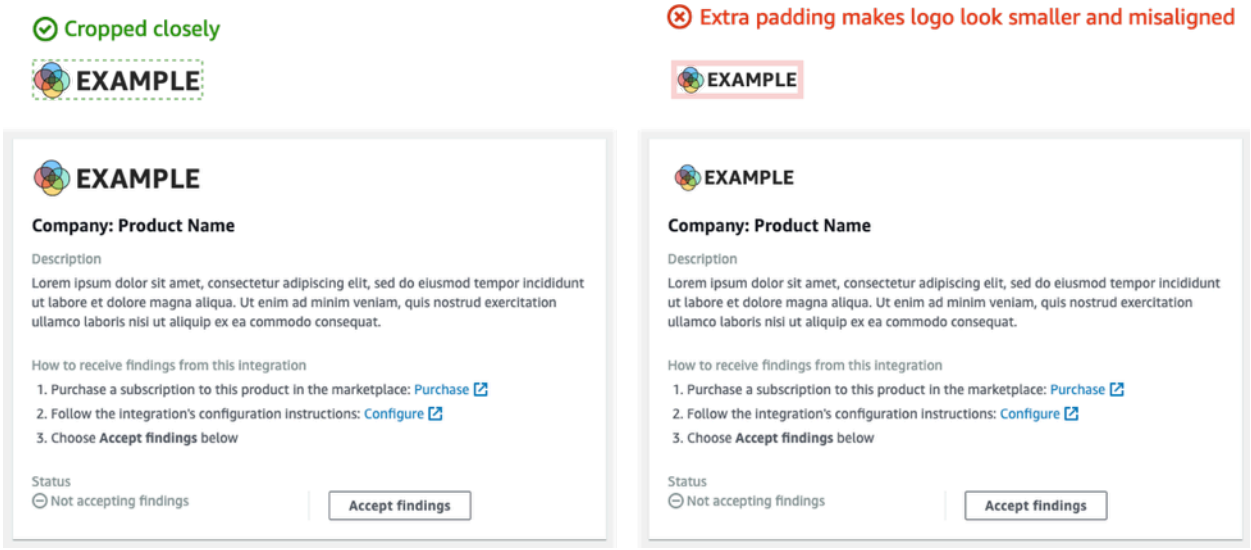
La siguiente imagen compara la visualización de un logotipo que utiliza el tamaño ideal con los logotipos que eran más anchos o más altos.



Recorte

Recorta la imagen del logotipo lo más cerca posible. No proporcione acolchado adicional.

La siguiente imagen muestra la diferencia entre un logotipo recortado de cerca y un logotipo con relleno adicional.



Sugerencias para crear y actualizar los hallazgos

A medida que planifique cómo creará y actualizará los hallazgos enAWS Security Hub, tenga en cuenta los siguientes principios.

Haga que los hallazgos sean específicos para que los clientes puedan tomar medidas en relación con ellos fácilmente.

Los clientes desean automatizar las acciones de respuesta y corrección y correlacionar los hallazgos con otros hallazgos. Para respaldar esto, los hallazgos deben tener las características siguientes:

- Por lo general, deben tratar un recurso único o principal.
- Deberían tener un único tipo de hallazgo.
- Deberían ocuparse de un único evento de seguridad.

Cuando una búsqueda contiene datos para varios eventos de seguridad, resulta más difícil para los clientes tomar medidas al respecto.

Asigne todos los campos de búsqueda a laAWSFormato de hallazgo de seguridad (ASFF) de. Permita que los clientes confíen en Security Hub como fuente de verdad.

Los clientes esperan que todos los campos que se encuentren en el formato de búsqueda nativo también estén representados en el ASFF de Security Hub.

Los clientes desean que todos los datos estén presentes en la versión de Security Hub del hallazgo. La falta de datos hace que pierdan la confianza en Security Hub como fuente central de información de seguridad.

Minimizar la redundancia en los hallazgos. No abrumes a los clientes con la búsqueda de volúmenes.

Security Hub no es una herramienta general de administración de registros. Debe enviar conclusiones a Security Hub que sean altamente procesables y que los clientes puedan responder directamente, corregir o correlacionar con otros hallazgos.

Cuando haya un cambio menor en la búsqueda, actualice la búsqueda en lugar de crear una nueva búsqueda.

Cuando se produzca un cambio importante en el hallazgo, como la puntuación de gravedad o el identificador de recursos, cree un nuevo hallazgo.

Por ejemplo, crear resultados para análisis de puertos individuales en tiempo real no es muy útil. Dado que el escaneo de puertos puede realizarse de forma continua, produciría un gran volumen de hallazgos. Es mucho más convincente y preciso simplemente actualizar el último tiempo de escaneo y contar con un único hallazgo para un escaneo de puertos en un puerto MongoDB desde un nodo TOR.

Permita a los clientes personalizar sus hallazgos para que sean más significativos.

Los clientes desean poder ajustar ciertos campos de búsqueda para que sean más relevantes para su entorno o requisitos.

Por ejemplo, los clientes desean poder agregar notas, etiquetas y ajustar las puntuaciones de gravedad en función del tipo de cuenta o del tipo de recurso al que está asociado la búsqueda.

Directrices para mapear los hallazgos en elAWSFormato de los hallazgos de seguridad de (ASFF)

Utilice las siguientes directrices para asignar sus hallazgos al ASFF. Para obtener descripciones detalladas de cada campo y objeto ASFF, consulteAWSFormato de los hallazgos de seguridad de (ASFF)en laAWS Security HubGuía del usuario de.

Información identificativa

`SchemaVersion` es siempre `2018-10-08`.

`ProductArn`es el ARN queAWS Security Hubte asigna.

`Id`es el valor que Security Hub utiliza para indexar los hallazgos. El identificador de hallazgo debe ser único para garantizar que no se sobrescriban otros hallazgos. Para actualizar una búsqueda, vuelva a enviar la búsqueda con el mismo identificador.

`GeneratorId`puede ser lo mismo que`Id`o puede hacer referencia a una unidad lógica discreta, como AmazonGuardDutyID de detector,AWS ConfigID de grabadora o ID de IAM Access Analyzer.

Title y Description

`Title`debe contener información sobre el recurso afectado.`Title`está limitado a 256 caracteres, incluidos los espacios.

Añada información más detallada a`Description`.`Description`está limitado a 1024 caracteres, incluidos los espacios. Puede considerar agregar truncamiento a las descripciones. A continuación se muestra un ejemplo:

```
"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.",
```

Tipos de búsqueda

Proporciona la información del tipo de búsqueda en`FindingProviderFields.Types`.

`Types`debe coincidir con elTipos de taxonomía para el ASFF.

Si es necesario, puede especificar un clasificador personalizado (el tercer espacio de nombres).

Marcas temporales

El formato ASFF incluye algunas marcas de hora diferentes.

`CreatedAt` y `UpdatedAt`

Debes enviar`CreatedAt`y`UpdatedAt`cada vez que llamas`BatchImportFindings`para cada hallazgo.

Los valores deben coincidir con el formato ISO8601 de Python 3.8.

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

`FirstObservedAt` y `LastObservedAt`

`FirstObservedAt`y`LastObservedAt`debe coincidir cuando el sistema haya observado el hallazgo. Si no registra esta información, no necesita enviar estas marcas de hora.

Los valores coinciden con el formato ISO8601 de Python 3.8.

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

Severity

Proporciona información de gravedad en el`FindingProviderFields.Severity`objeto, que contiene los siguientes campos.

`Original`

El valor de gravedad de su sistema.`Original`puede ser cualquier cadena, para acomodar el sistema que utiliza.

`Label`

Indicador de Security Hub necesario de la gravedad de la búsqueda. Los valores permitidos son los siguientes.

- `INFORMATIONAL`— No se ha encontrado ningún problema.
- `LOW`— La cuestión no requiere acción por sí sola.
- `MEDIUM`— La cuestión debe abordarse pero no urgentemente.
- `HIGH`— La cuestión debe abordarse con carácter prioritario.
- `CRITICAL`— La cuestión debe solucionarse inmediatamente para evitar más daños.

Los hallazgos que cumplen los requisitos deben tener siempre`Label`establecer como`INFORMATIONAL`. Ejemplos de`INFORMATIONAL`las conclusiones son conclusiones de los controles de seguridad aprobados yAWS Firewall Managerhallazgos que se solucionan.

Los clientes suelen ordenar los hallazgos por su gravedad para ofrecer a sus equipos de operaciones de seguridad una lista de tareas pendientes. Sea conservador al establecer la gravedad del hallazgo en`HIGH`o`CRITICAL`.

La documentación de integración debe incluir los fundamentos de la asignación.

Remediation

`Remediation`tiene dos elementos. Estos elementos se combinan en la consola de Security Hub.

`Remediation.Recommendation.Text`aparece en el directorio`Corrección`sección de los detalles de la búsqueda. Está hipervinculado al valor de`Remediation.Recommendation.Url`.

Actualmente, solo los resultados de los estándares de Security Hub, IAM Access Analyzer y Firewall Manager muestran hipervínculos a la documentación sobre cómo corregir la búsqueda.

SourceUrl

Utilizar solo`SourceUrl`si puedes proporcionar una URL enlazada profunda a tu consola para ese hallazgo específico. De lo contrario, omítalo de la asignación.

Security Hub no admite hipervínculos de este campo, pero se expone en la consola de Security Hub.

Malware, Network, Process, ThreatIntelIndicators

Cuando proceda, utilice`Malware`,`Network`,`Process`, o bien`ThreatIntelIndicators`. Cada uno de estos objetos se expone en la consola de Security Hub. Utilice estos objetos en el contexto de la búsqueda que está enviando.

Por ejemplo, si detecta malware que realiza una conexión saliente a un nodo de comando y control conocido, proporcione los detalles de la instancia EC2 en`Resource.Details.AwsEc2Instance`. Proporcionar la información pertinente`Malware`,`Network`, y`ThreatIntelIndicator`objetos de esa instancia EC2.

Malware

`Malware`es una lista que acepta hasta cinco matrices de información de malware. Haga que las entradas de malware sean relevantes para el recurso y la búsqueda.

Cada entrada tiene los siguientes campos.

`Name`

El nombre del malware. El valor es una cadena de hasta 64 caracteres.

`Name`debe proceder de una información sobre amenazas o de una fuente investigadora comprobada.

`Path`

La ruta al malware. El valor es una cadena de hasta 512 caracteres.`Path`debe ser una ruta de archivo del sistema Linux o Windows, excepto en los siguientes casos.

- Si escanea objetos en un bucket de S3 o en un recurso compartido de EFS con las reglas de YARA,`Path`es la ruta de objeto S3:// o HTTPS.
- Si escaneas archivos en un repositorio de Git, entonces`Path`es la URL de Git o la ruta de clon.

`State`

El estado del malware. Los valores permitidos son`OBSERVED`| `REMOVAL_FAILED`|`REMOVED`.

En el título y la descripción de búsqueda, asegúrese de proporcionar contexto para lo que ocurrió con el malware.

Por ejemplo, si`Malware.State`es`REMOVED`, el título y la descripción de la búsqueda deben reflejar que el producto ha eliminado el malware que se encuentra en la ruta.

Si`Malware.State`es`OBSERVED`, el título y la descripción de la búsqueda deben reflejar que el producto ha encontrado este malware ubicado en la ruta.

`Type`

Indica el tipo de malware. Los valores permitidos son`ADWARE`|`BLENDED_THREAT`|`BOTNET_AGENT`|`COIN_MINER`|`EXPLOIT_KIT`|`KEYLOGGER`|`MACRO`|`POTEN`

Si necesitas un valor adicional para`Type`, póngase en contacto con el equipo de Security Hub.

Network

`Network`es un solo objeto. No se pueden añadir varios detalles relacionados con la red. Cuando realice una asignación de los campos, utilice las siguientes directrices.

Información de destino y origen

El destino y el origen son fáciles de asignar registros de flujo TCP o VPC o registros WAF. Son más difíciles de usar cuando se describe la información de la red para un hallazgo sobre un ataque.

Normalmente, la fuente es de donde se originó el ataque, pero podría tener otras fuentes como se enumeran a continuación. Debe explicar el origen en la documentación y describirlo también en el título y la descripción de búsqueda.

- Para un ataque DDoS en una instancia EC2, el origen es el atacante, aunque un ataque DDoS real puede utilizar millones de hosts. El destino es la dirección IPv4 pública de la instancia EC2.`Direction`está IN.
- En el caso de malware que se observa comunicándose desde una instancia EC2 a un nodo de comando y control conocido, el origen es la dirección IPV4 de la instancia EC2. El destino es el nodo de comando y control.`Direction`es`OUT`. También proporcionaría`MalwareyThreatIntelIndicators`.

`Protocol`

`Protocol`siempre se asigna a un nombre registrado de la Autoridad de Números Asignados de Internet (IANA), a menos que pueda proporcionar un protocolo específico. Debe usarlo siempre y proporcionar la información del puerto.

`Protocol`es independiente de la información de origen y destino. Solo proporciónalo cuando tenga sentido hacerlo.

`Direction`

`Direction`siempre es relativo a laAWSLímites de red.

- `IN`significa que está entrandoAWS(VPC, servicio).
- `OUT`significa que está saliendo delAWSLímites de red.

Process

`Process`es un solo objeto. No se pueden añadir varios detalles relacionados con el proceso. Cuando realice una asignación de los campos, utilice las siguientes directrices.

`Name`

`Name`debe coincidir con el nombre del ejecutable. Acepta como máximo 64 caracteres.

`Path`

`Path`es la ruta del sistema de archivos al ejecutable del proceso. Acepta hasta 512 caracteres.

`Pid`, **`ParentPid`**

`Pid`y`ParentPid`debe coincidir con el identificador de proceso de Linux (PID) o el ID de evento de Windows. Para diferenciar, utilice Imágenes de máquina de Amazon (AMI) de EC2 para proporcionar la información. Los clientes pueden diferenciar entre Windows y Linux.

Marcas de tiempo (**`LaunchedAt`**y**`TerminatedAt`**)

Si no puede recuperar esta información de forma fiable y no es exacta en milisegundos, no la proporcione.

Si un cliente confía en las marcas de hora para la investigación forense, entonces no tener marca de hora es mejor que tener una marca de hora incorrecta.

ThreatIntelIndicators

`ThreatIntelIndicators`acepta una matriz de hasta cinco objetos de información de amenazas.

Para cada entrada,`Type`se encuentra en el contexto de la amenaza específica. Los valores permitidos son`DOMAIN|EMAIL_ADDRESS|HASH_MD5|HASH_SHA1|HASH_SHA256|HASH_SHA512|IPV4_ADDRESS|IPV6_`

A continuación, mostramos algunos ejemplos de cómo asignar indicadores de información de amenazas:

- Has encontrado un proceso que sabes que está asociado con Cobalt Strike. Lo aprendiste deFireEyedel blog de.

  Establezca `Type` en `PROCESS`. Crea también un`Process`objeto para el proceso.
- El filtro de correo ha encontrado a alguien que envía un paquete hash conocido desde un dominio malicioso conocido.

  Crear dos`ThreatIntelIndicator`objetos. Un objeto es para el`DOMAIN`. El otro es para el`HASH_SHA1`.
- Has encontrado malware con una regla de Yara (Loki, Fenrir, Awss3VirusScan,BinaryAlert).

  Crear dos`ThreatIntelIndicator`objetos. Uno es para el malware. El otro es para el`HASH_SHA1`.

Resources

Para`Resources`, utilice los tipos de recursos proporcionados y los campos de detalle siempre que sea posible. Security Hub añade constantemente nuevos recursos al ASFF. Para recibir un registro mensual de los cambios en el ASFF, póngase en contacto con`<securityhub-partners@amazon.com>`.

Si no puede colocar la información en los campos de detalles de un tipo de recurso modelado, asigne los detalles restantes a`Details.Other`.

Para un recurso que no está modelado en ASFF, defina`Type`a`Other`. Para obtener información detallada, utilice`Details.Other`.

También puede utilizar la`Other`tipo de recurso para organizaciones no gubernamentales,AWShallazgos.

ProductFields

Utilizar solo`ProductFields`si no puede utilizar otro campo seleccionado para`Resource`so un objeto descriptivo como`ThreatIntelIndicators`,`Network`, o bien`Malware`.

Si lo utilizas`ProductFields`, debe proporcionar una justificación estricta para esta decisión.

Conformidad

Utilizar solo`Compliance`si sus conclusiones están relacionadas con el cumplimiento.

Security Hub utiliza`Compliance`para las conclusiones que genera sobre la base de los controles.

Firewall Manager utiliza`Compliance`por sus conclusiones porque están relacionadas con el cumplimiento.

Campos restringidos

Estos campos están destinados a que los clientes realicen un seguimiento de su investigación de un hallazgo.

No asigne estos campos u objetos.

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

Para estos campos, asigne los campos que se encuentran en el`FindingProviderFields`objeto. No asigne a los campos de nivel superior.

- `Confidence`— Incluya solo un puntaje de confianza (0-99) si su servicio tiene una funcionalidad similar o si respalda al 100% su hallazgo.
- `Criticality`— El puntaje de criticidad (0-99) pretende expresar la importancia del recurso asociado al hallazgo.
- `RelatedFindings`: proporcione resultados relacionados únicamente si puede realizar un seguimiento de los hallazgos relacionados con el mismo recurso o tipo de búsqueda. Para identificar un hallazgo relacionado, debe hacer referencia al identificador de búsqueda de un hallazgo que ya se encuentra en Security Hub.

Directrices para el uso del**`BatchImportFindings`**API

Cuando se utiliza el`BatchImportFindings`Operación de API para enviar hallazgos aAWS Security Hub, utilice las siguientes directrices.

- Debes llamar`BatchImportFindings`utilizando la cuenta asociada a los hallazgos. El identificador de la cuenta asociada es el valor del`AwsAccountId`atributo para la búsqueda.
- Envía el lote más grande que puedas. Security Hub acepta hasta 100 hallazgos por lote, hasta 240 KB por búsqueda y hasta 6 MB por lote.
- El límite de velocidad del acelerador es de 10 TPS por cuenta y región, con una ráfaga de 30 TPS.
- Debe implementar un mecanismo para conservar el estado de los hallazgos si existen problemas de limitación o de red. También necesita el estado de búsqueda para poder enviar actualizaciones de búsqueda a medida que una búsqueda entra y sale de conformidad.
- Para obtener información acerca de las longitudes máximas de cadenas y otras limitaciones, consulteAWSFormato de los hallazgos de seguridad de (ASFF)en laAWS Security HubGuía del usuario de.

Lista de comprobación de preparación del producto

LaAWS Security Huby los equipos de socios de APN utilizan esta lista de comprobación para validar que la integración está lista para iniciarse.

Asignación de ASFF

Estas preguntas están relacionadas con la asignación de su hallazgo a laAWSFormato de hallazgo de seguridad (ASFF) de.

¿Todos los datos de búsqueda del socio están mapeados en ASFF?

Mapee todos sus hallazgos al ASFF de alguna manera.

Utilizar campos curados, tales como tipos de recursos modelados,`Network`,`Malware`, o bien`ThreatIntelIndicators`.

Asigne cualquier otra cosa en`Resource.Details.Other`o`ProductFields`según proceda.

¿Utiliza el socio?**`Resource.Details`**campos, tales como**`AwsEc2instance`**,**`AwsS3Bucket`**, y**`Container`**? ¿Utiliza el socio?**`Resource.Details.Other`**para definir detalles de recursos que no están modelados en el ASFF?

Siempre que sea posible, utilice los campos proporcionados para recursos seleccionados como instancias EC2, buckets de S3 y grupos de seguridad en sus hallazgos.

Asignar otra información relacionada con los recursos a`Resource.Details.Other`solo cuando no hay una coincidencia directa.

¿El socio asigna valores a**`UserDefinedFields`**?

No utilice `UserDefinedFields`.

Considere la posibilidad de utilizar otro campo seleccionado, como`Resource.Details.Other`o`ProductFields`.

¿Mapea la información del socio en**`ProductFields`**que podrían mapearse en otros campos del ASFF?

Utilizar solo`ProductFields`para información específica del producto, como información de control de versiones, resultados de gravedad específicos del producto u otra información que no se puede asignar a un campo seleccionado o`Resources.Details.Other`.

¿Importa el socio sus propias marcas de hora para**`FirstObservedAt`**?

La`FirstObservedAt`timestamp tiene por objeto registrar la hora en que se observó un hallazgo en el producto. Asigne este campo si es posible.

¿Proporciona el socio valores únicos generados para cada identificador de búsqueda, excepto los resultados que desea actualizar?

Todas las conclusiones de Security Hub se indexan en el identificador de búsqueda (`Id`atributo). Este valor debe ser siempre único para garantizar que los resultados no se actualicen accidentalmente.

También debe mantener el estado del identificador de búsqueda con el fin de actualizar los hallazgos.

¿Proporciona el socio un valor que asigna los hallazgos a un ID de generador?

`GeneratorID`no debe tener el mismo valor que el ID de búsqueda.

`GeneratorID`debería poder vincular lógicamente los hallazgos por lo que los generó.

Puede ser un subcomponente dentro de un producto (Producto A - Vulnerabilidad frente al producto A - EDR) o algo similar.

¿Utiliza el socio los espacios de nombres de tipos de búsqueda requeridos de forma que sea relevante para su producto? ¿Utiliza el socio las categorías o clasificadores de tipos de búsqueda recomendados en sus tipos de búsqueda?

La taxonomía del tipo de hallazgo debe corresponder estrechamente a los hallazgos que genera el producto.

Espacios de nombres de primer nivel descritos en elAWSEl formato de búsqueda de seguridad es obligatorio.

Puede utilizar valores personalizados para los espacios de nombres de segundo y tercer nivel (categorías o clasificadores).

¿El socio captura la información del flujo de red en el**`Network`**campos, si tienen datos de red?

Si su producto se capturaNetFlowinformación, asignarlo a la`Network`.

¿El socio captura la información del proceso (PID) en el**`Process`**campos, si tienen datos de proceso?

Si el producto captura información del proceso, asígnala a la`Process`.

¿El socio capta información de malware en el**`Malware`**campos, si tienen datos de malware?

Si el producto captura información de malware, asígnala a la`Malware`.

¿El socio captura información de inteligencia de amenazas en el**`ThreatIntelIndicators`**campos, si tienen datos de inteligencia de amenazas?

Si el producto captura información de inteligencia de amenazas, asígnala a la`ThreatIntelIndicators`.

¿Proporciona el socio una calificación de confianza para los hallazgos? Si lo hacen, ¿se proporciona una justificación?

Siempre que utilice este campo, proporcione una justificación en su documentación y manifiesto.

¿Utiliza el socio un ID canónico o ARN para el ID de recurso de la búsqueda?

Al identificarAWSrecursos, la práctica recomendada es utilizar el ARN. Si no hay un ARN disponible, utilice el ID de recurso canónico.

Configuración y función de la integración

Estas preguntas están relacionadas con la configuración yday-to-dayfunción de la integración.

¿Proporciona el socio uninfrastructure-as-code(iAC) para implementar la integración con Security Hub, como Terraform,AWS CloudFormation, o bienAWS Cloud Development Kit (AWS CDK)?

Para integraciones que enviarán resultados de la cuenta del cliente o utilizaránCloudWatchEventos para consumir hallazgos, se requiere algún tipo de plantilla iAC.

AWS CloudFormationes preferible, peroAWS CDKo Terraform también puede utilizarse.

¿El producto asociado tiene una configuración con un solo clic en su consola para integrarlo con Security Hub?

Algunos productos asociados utilizan un conmutador o un mecanismo similar en su producto para activar la integración. Esto puede implicar el aprovisionamiento automático de recursos y permisos. Si envías resultados desde una cuenta de producto, la configuración con un solo clic es el método preferido.

¿El socio solo envía resultados de valor?

Por lo general, solo debe enviar resultados que tengan valor de seguridad a los clientes de Security Hub.

Security Hub no es una herramienta general de administración de registros. No debe enviar todos los registros posibles a Security Hub.

¿Proporcionó el socio una estimación de cuántos hallazgos enviará por día por cliente y con qué frecuencia (media y ráfaga)?

Se utilizan números de hallazgos únicos para calcular la carga en Security Hub. Un hallazgo único se define como un hallazgo con un mapeo ASFF diferente de otro hallazgo.

Por ejemplo, si un hallazgo solo se ha rellenado`ThreatIntelIndicators`y otro poblado solamente`Resources.Details.AWSEc2Instance`, son dos hallazgos únicos.

¿Tiene el socio una forma elegante de manejar los errores 4xx y 5xx de modo que no se limiten y que todos los hallazgos se puedan enviar más adelante?

Actualmente hay una tasa de ráfaga de 30 a 50 TPS en el`BatchImportFindings`Operación de API. Si se devuelven errores 4xx o 5xx, debe conservar el estado de esos hallazgos fallidos para poder volver a intentarlos en su totalidad más adelante. Puedes hacerlo a través de una cola de letras muertas u otraAWSservicios de mensajería como Amazon SNS o Amazon SQS.

¿Mantiene el socio el estado de sus hallazgos para que sepa archivar los hallazgos que ya no están presentes?

Si planea actualizar los hallazgos sobrescribiendo el ID de búsqueda original, debe contar con un mecanismo para conservar el estado de forma que se actualice la información correcta para la búsqueda correcta.

Si proporciona hallazgos, no utilice el`BatchUpdateFindings`operación para actualizar los hallazgos. Esta operación solo debe ser utilizada por los clientes. Solo utilizas`BatchUpdateFindings`cuando investiga y tome medidas en relación con los hallazgos.

¿El socio gestiona los reintentos de una manera que no compromete los resultados exitosos enviados anteriormente?

Debe disponer de un mecanismo para conservar los ID de búsqueda originales en caso de errores para no duplicar ni sobrescribir las conclusiones correctas por error.

¿Actualiza el socio los hallazgos llamando al**`BatchImportFindings`**operación con el ID de búsqueda de los hallazgos existentes?

Para actualizar una búsqueda, debe sobrescribir la búsqueda existente enviando el mismo ID de búsqueda.

La`BatchUpdateFindings`la operación solo debe ser utilizada por los clientes.

¿Actualiza el socio los hallazgos mediante el**`BatchUpdateFindings`**API?

Si toma medidas sobre los hallazgos, puede utilizar el`BatchUpdateFindings`para actualizar campos específicos.

¿Proporciona el socio información sobre la cantidad de latencia entre el momento en que se crea un hallazgo y el momento en que se envía desde su producto a Security Hub?

Debe minimizar la latencia para garantizar que los clientes vean los hallazgos lo antes posible en Security Hub.

Esta información se requiere en el manifiesto.

Si la arquitectura del socio va a enviar los hallazgos a Security Hub desde una cuenta de cliente, ¿lo han demostrado correctamente? Si la arquitectura del socio va a enviar los hallazgos a Security Hub desde su propia cuenta, ¿lo han demostrado satisfactoriamente?

Durante las pruebas, los hallazgos deben enviarse correctamente desde una cuenta de su propiedad distinta de la cuenta proporcionada para el ARN del producto.

El envío de un hallazgo desde la cuenta del propietario del ARN del producto puede eludir ciertas excepciones de error de las operaciones de la API.

¿El socio proporciona un hallazgo de latidos a Security Hub?

Para demostrar que la integración funciona correctamente, debe enviar una búsqueda de latidos. El hallazgo de latidos se envía cada cinco minutos y utiliza el tipo de hallazgo`Heartbeat`.

Esto es importante si envías los resultados de una cuenta de producto.

¿Se integró el socio con la cuenta del equipo de productos de Security Hub durante las pruebas?

Durante la validación de preproducción, debe enviar ejemplos de búsqueda al equipo de productos de Security HubAWSaccount. Estos ejemplos demuestran que los hallazgos se envían y asignan correctamente.

Documentación

Estas preguntas están relacionadas con la documentación de la integración que proporciona.

¿El socio aloja su documentación en un sitio web dedicado?

La documentación debe alojarse en su sitio web como página web estática, wiki, Leer los documentos u otro formato dedicado.

Documentación de alojamiento enGitHubno satisface el requisito del sitio web dedicado.

¿La documentación del socio proporciona instrucciones sobre cómo configurar la integración de Security Hub?

Puede configurar la integración mediante una plantilla iAC o una integración de «un clic» basada en consola.

¿La documentación del socio proporciona una descripción de su caso de uso?

El caso de uso que proporciona en el manifiesto también debe describirse en la documentación.

¿La documentación del socio proporciona una justificación para los hallazgos que envían?

Debe proporcionar la justificación de los tipos de hallazgos que envía.

Por ejemplo, el producto podría producir hallazgos de vulnerabilidades, malware y antivirus, pero solo envía descubrimientos de vulnerabilidades y malware a Security Hub. En ese caso, debe proporcionar una justificación de por qué no envía hallazgos de antivirus.

¿Proporciona la documentación del socio una justificación de cómo el socio asigna sus conclusiones al ASFF?

Debe proporcionar la justificación de la asignación de los hallazgos nativos de un producto a ASFF. Los clientes desean saber dónde buscar información específica del producto.

¿La documentación del socio proporciona orientación sobre cómo actualiza el socio los hallazgos, si actualizan los hallazgos?

Proporcione a los clientes información sobre cómo mantiene el estado, garantiza la idempotencia y sobrescriba los hallazgos conup-to-dateinformación de.

¿Describe la documentación del socio cómo encontrar latencia?

Minimiza la latencia para garantizar que los clientes vean los hallazgos lo antes posible en Security Hub.

Esta información se requiere en el manifiesto.

¿Describe la documentación del socio cómo se asigna su puntuación de gravedad a la puntuación de gravedad del ASFF?

Proporcionar información sobre cómo mapear`Severity.Original`a`Severity.Label`.

Por ejemplo, si el valor de gravedad es una calificación por letra (A, B, C), debe proporcionar información sobre cómo asignar la calificación de la letra a la etiqueta de gravedad.

¿La documentación del socio proporciona una justificación para las calificaciones de confianza?

Si proporciona puntuaciones de confianza, estas puntuaciones deben clasificarse.

Si utiliza puntuaciones de confianza o asignaciones rellenadas estáticamente derivadas de la inteligencia artificial o el aprendizaje automático, debe proporcionar contexto adicional.

¿Anota la documentación del socio qué regiones admite y qué no admite el socio?

Nota Regiones compatibles o no para que los clientes sepan en qué regiones no intentan integrarse.

Información de tarjeta del producto

Estas preguntas están relacionadas con la tarjeta del producto que se muestra en elIntegracionesde la consola de Security Hub.

¿Es el proporcionadoAWSID de cuenta válido y contiene 12 dígitos?

Los identificadores de cuenta tienen 12 dígitos de longitud. Si un ID de cuenta contiene menos de 12 dígitos, el ARN del producto no será válido.

¿La descripción del producto contiene 200 caracteres o menos?

La descripción del producto proporcionada en el JSON dentro del manifiesto no debe tener más de 200 caracteres, incluidos los espacios.

¿El enlace de configuración lleva a documentación para la integración?

El enlace de configuración debe llevar a la documentación en línea. No debe conducir a su sitio web principal ni a páginas de marketing.

¿El enlace de compra (si se proporciona) conduce alAWS Marketplacelistado para el producto?

Si proporcionas un enlace de compra, debe ser para unAWS Marketplaceentrada. Security Hub no acepta enlaces de compra que no estén alojados enAWS.

¿Las categorías de productos describen correctamente el producto?

En el manifiesto, puedes proporcionar hasta tres categorías de productos. Estos deben coincidir con el JSON y no pueden ser personalizados. No puedes proporcionar más de tres categorías de productos.

¿Son válidos y correctos los nombres de la empresa y los productos?

El nombre de la empresa debe tener 16 caracteres o menos.

El nombre del producto debe tener 24 caracteres o menos.

El nombre del producto de la tarjeta de producto JSON debe coincidir con el nombre del manifiesto.

Información de marketing

Estas preguntas están relacionadas con el marketing para la integración.

¿La descripción del producto de la página de socios de Security Hub tiene 700 caracteres, incluidos los espacios?

La página de socios de Security Hub solo acepta hasta 700 caracteres, incluidos los espacios.

El equipo modificará descripciones más largas.

¿El logotipo de la página de socios de Security Hub no supera los 600 x 300 px?

Proporcione una URL de acceso público con un logotipo de la empresa en PNG o JPG que no supere los 600 x 300 píxeles.

¿El hipervínculo Más información de la página de socios de Security Hub conduce a la página web dedicada del socio sobre la integración?

LaMás informaciónenlace no debe conducir al sitio web principal del socio ni a la información de documentación.

Este enlace debe ir siempre a una página web dedicada con información de marketing sobre la integración.

¿Proporciona el socio una demostración o un vídeo instructivo sobre cómo utilizar su integración?

Un vídeo tutorial de demostración o integración es opcional, pero recomendable.

Es unAWS¿Publicación de blog de Partner Network que se publica con el socio y su gerente de desarrollo de socios o representante de desarrollo de socios?

AWSLas publicaciones de blog de Partner Network deben coordinarse con anticipación con el gerente de desarrollo de socios o el representante de desarrollo de socios.

Estos son separados de cualquier publicación de blog que crees tú mismo.

Permita un plazo de entrega de 4 a 6 semanas. Este esfuerzo debe iniciarse una vez finalizada la prueba con el ARN del producto privado.

¿Se está publicando un comunicado de prensa dirigido por socios?

Puede trabajar con su gerente de desarrollo de socios o con el representante de desarrollo de socios para obtener una cotización del vicepresidente de servicios de seguridad externa. Puede utilizar esta cita en su comunicado de prensa.

¿Se está publicando una publicación de blog dirigida por socios?

Puedes crear tus propias publicaciones de blog para mostrar la integración fuera delAWSBlog de Partner Network.

¿Se está publicando un seminario web dirigido por socios?

Puede crear sus propios seminarios web para mostrar la integración.

Si necesita ayuda del equipo de Security Hub, colabore con el equipo de productos después de completar las pruebas con el ARN del producto privado.

¿El socio solicitó apoyo en las redes sociales aAWS?

Después de su lanzamiento, puede trabajar con elAWSPropuesta de uso del marketing de seguridadAWScanales oficiales de redes sociales para compartir detalles sobre tus seminarios web.

AWS Security HubPreguntas frecuentes sobre socios

A continuación se presentan preguntas comunes sobre cómo configurar y mantener una integración conAWS Security Hub.

1. ¿Cuáles son los beneficios de la integración de Security Hub?
   - satisfacción de los clientes— La razón principal para integrarse con Security Hub es porque tiene solicitudes de los clientes para hacerlo.

     Security Hub es el centro de seguridad y cumplimiento deAWSclientes. Está diseñado como la primera parada dondeAWSlos profesionales de seguridad y cumplimiento acuden cada día a entender su estado de seguridad y cumplimiento.

     Escucha a tus clientes. Le informarán si quieren ver sus hallazgos en Security Hub.
   - Oportunidades de— Promocionamos socios con integraciones certificadas dentro de la consola de Security Hub, incluidos enlaces a suAWS Marketplacelistados. Es una excelente manera para que los clientes descubran nuevos productos de seguridad.
   - Oportunidades comerciales— Los proveedores con integraciones aprobadas pueden participar en seminarios web, emitir comunicados de prensa, crear hojas sencillas y demostrar sus integraciones enAWSclientes.
2. ¿Qué tipos de socios existen?
   - Socios que envían los resultados a Security Hub
   - Socio que recibe los resultados de Security Hub
   - Socios que envían y reciben hallazgos
   - Socios consultores que ayudan a los clientes a configurar, personalizar y utilizar Security Hub en su entorno
3. ¿Cómo funciona la integración de socios con Security Hub a un alto nivel?

   Reúne los resultados de una cuenta de cliente o de la suya propiaAWScontabilizar y transformar el formato de los hallazgos en elAWSFormato de hallazgo de seguridad (ASFF) de. A continuación, puede enviar estos hallazgos al extremo regional de Security Hub apropiado.

   También puede utilizarCloudWatchEventos para recibir los resultados de Security Hub.
4. ¿Cuáles son los pasos básicos para completar una integración con Security Hub?

   a. Envíe la información del manifiesto de su socio.

b. Reciba ARN de productos para utilizarlos con Security Hub, si va a enviar los hallazgos a Security Hub.

c. Mapee sus hallazgos a ASFF. Consulte the section called “Directrices para el mapeo del ASFF”.

d. Defina la arquitectura para enviar hallazgos y recibir hallazgos de Security Hub. Siga los principios descritos enthe section called “Sugerencias para crear y actualizar los hallazgos”.

e. Cree un marco de implementación para los clientes. Por ejemplo,AWS CloudFormationlas secuencias de comandos pueden cumplir este propósito.

f. Documente su configuración y proporcione instrucciones de configuración para los clientes.

g. Defina cualquier información personalizada (reglas de correlación) que los clientes puedan utilizar con su producto.

h. Demuestre su integración al equipo de Security Hub.

i. Envíe información de marketing para su aprobación (idioma del sitio web, comunicado de prensa, diapositiva de arquitectura, vídeo, hoja lisa).

5. ¿Cuál es el proceso para presentar el manifiesto de socio? Y paraAWSservicios para enviar los hallazgos a Security Hub?

   Para enviar la información del manifiesto al equipo de Security Hub, utilice`<securityhub-partners@amazon.com>`.

   Se te emiten los ARN del producto en un plazo de siete días naturales.

6. ¿Qué tipos de hallazgos debo enviar a Security Hub?

   Los precios de Security Hub se basan en parte en el número de hallazgos ingeridos. Debido a esto, debe abstenerse de enviar hallazgos que no aporten valor a los clientes.

   Por ejemplo, algunos proveedores de administración de vulnerabilidades solo envían resultados con una puntuación del Sistema Común de Calificación de Vulnerabilidades (CVSS) de 3 o más de 10 posibles.

7. ¿Cuáles son los diferentes enfoques para enviar hallazgos a Security Hub?

   Estos son los principales enfoques:

   - Envía los hallazgos de su propia designaciónAWSCuenta utilizando elBatchImportFindings.
   - Envía los hallazgos desde la cuenta de cliente mediante laBatchImportFindings. Podrías usar enfoques de asume-role, pero estos enfoques no son necesarios.

Para obtener directrices generales sobre el uso`BatchImportFindings`, consulte[the section called “Directrices para el uso del`BatchImportFindings`API”](#).

8. ¿Cómo recopilo mis hallazgos y los empujo a un punto de enlace regional de Security Hub?

   Los socios han utilizado diferentes enfoques para ello, ya que depende en gran medida de la arquitectura de su solución.

   Por ejemplo, algunos socios crean una aplicación Python que se puede implementar comoAWS CloudFormationscript. El script recopila los hallazgos del socio del entorno del cliente, los transforma en ASFF y los envía al extremo regional de Security Hub.

   Otros socios crean un asistente completo que ofrece al cliente una experiencia de un solo clic para enviar los hallazgos a Security Hub.

9. ¿Cómo sé cuándo comenzar a enviar los hallazgos a Security Hub?

   Security Hub admite la autorización parcial de lotes para el`BatchImportFindings`Operación de API, para que puedas enviar todos tus hallazgos a Security Hub para todos tus clientes.

   Si algunos de sus clientes aún no se han suscrito a Security Hub, Security Hub no ingiere esos hallazgos. Solo ingiere los hallazgos autorizados que se encuentran en el lote.

10. ¿Qué pasos debo completar para enviar hallazgos a la instancia de Security Hub de un cliente?

    a. Asegúrese de que existan las políticas de IAM correctas.
    b. Habilitar una suscripción de productos (políticas de recursos) para las cuentas. Utilice el`EnableImportFindingsForProduct`Operación de la API deIntegraciones(Se ha creado el certificado). El cliente puede hacerlo o puede utilizar funciones multicuenta para actuar en nombre del cliente.
    c. Asegúrese de que`ProductArn`del hallazgo es el ARN público de tu producto.
    d. Asegúrese de que`AwsAccountId`del hallazgo es el ID de cuenta del cliente.
    e. Asegúrese de que sus hallazgos no tengan datos mal formados según elAWSFormato de hallazgo de seguridad (ASFF) de. Por ejemplo, los campos obligatorios se rellenan y no hay valores no válidos.
    f. Envíe los resultados por lotes al extremo regional correcto.

11. ¿Qué permisos de IAM deben estar vigentes para enviar los hallazgos?

    Las políticas de IAM deben configurarse para el usuario o rol de IAM que llama`BatchImportFindings`u otras llamadas a API.

La prueba más sencilla es hacerlo desde una cuenta de administrador. Puedes restringirlas `aaction: ‘securityhub:BatchImportFindings’yresource: <productArn and/or productSubscriptionArn>`.

Los recursos de la misma cuenta se pueden configurar con políticas de IAM sin necesidad de políticas de recursos.

Para descartar problemas de política de IAM de la persona que llamaBatchImportFindings, establezca la política de IAM para la persona que llama de la siguiente manera:

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

Asegúrate de comprobar que no hayDenypolíticas para el intermediario. Después de que funcione con eso, puede restringir la política a lo siguiente:

```
{
    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¿Qué es una suscripción de producto?

Para recibir los resultados de un producto de socio específico, el cliente (o el socio con funciones multicuenta que trabajan en nombre del cliente) debe establecer una suscripción de producto. Para hacerlo desde la consola de, utilizanIntegraciones(Se ha creado el certificado). Para hacerlo desde la API, utilizan elEnableImportFindingsForProductOperación de la API.

La suscripción del producto crea una política de recursos que autoriza que el cliente reciba o envíe las conclusiones del socio. Para obtener más información, consulte Casos de uso y permisos.

Security Hub tiene los siguientes tipos de políticas de recursos para socios:

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

Durante el proceso de incorporación de socios, puede solicitar uno o ambos tipos de políticas.

con`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, solo puedes enviar los hallazgos a Security Hub desde la cuenta que aparece en el ARN del producto.

con`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, solo puedes enviar los hallazgos desde la cuenta de cliente que te suscribiste.

13. Supongamos que un cliente ha creado una cuenta de administrador y ha añadido algunas cuentas de miembro. ¿El cliente tiene que suscribirme cada cuenta de miembro? ¿O el cliente solo se suscribe desde la cuenta de administrador y luego puedo enviar los resultados de los recursos de todas las cuentas de miembro?

    Esta pregunta pregunta si los permisos se crean para todas las cuentas de miembro según el registro de la cuenta de administrador.

    El cliente debe establecer una suscripción de producto para cada cuenta. Pueden hacerlo mediante programación a través de la API.

14. ¿Qué es el ARN de mi producto?

    El ARN de su producto es el identificador único que Security Hub genera para usted y que utiliza para enviar los hallazgos. Recibe un ARN de producto por cada producto que integra con Security Hub. El ARN del producto correcto debe formar parte de cada hallazgo que envíe a Security Hub. Se eliminan los hallazgos sin el ARN del producto. El ARN del producto utiliza el siguiente formato:

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

    A continuación se muestra un ejemplo:

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

    Se le proporciona un ARN de producto para cada región en la que se implementa Security Hub. El ID de cuenta, la empresa y los nombres de productos vienen dictados por los envíos de manifiestos de socios. Nunca cambias ninguna información asociada al ARN de tu producto,

excepto el código de región. El código de región debe coincidir con la región para la que envía los resultados.

Un error común es cambiar el ID de cuenta para que coincida con la cuenta desde la que trabajas actualmente. El ID de cuenta no cambia. Envía un ID de cuenta «principal» como parte del envío del manifiesto. Este ID de cuenta está bloqueado en el ARN del producto.

Cuando Security Hub se lanza en nuevas regiones, utiliza automáticamente los códigos de región estándar para generar los ARN de los productos para esas regiones.

Cada cuenta también se aprovisiona automáticamente con un ARN de producto privado. Puede utilizar este ARN para probar los hallazgos de importación dentro de su propia cuenta de desarrollo antes de recibir el ARN oficial del producto público.

15 ¿Qué formato se debe utilizar para enviar los hallazgos a Security Hub?

Los resultados deben proporcionarse en elAWSFormato de hallazgo de seguridad (ASFF) de. Para obtener más información, consulte .AWSFormato de los hallazgos de seguridad de (ASFF)en laAWS Security HubGuía del usuario de.

La expectativa es que toda la información de sus hallazgos nativos se refleje plenamente en el ASFF. Campos personalizados tales como`ProductFields`y`Resource.Details.Other`permite asignar datos que no encajan perfectamente en los campos predefinidos.

16 ¿Cuál es el endpoint regional correcto que se debe utilizar?

Debe enviar los resultados al endpoint regional de Security Hub asociado a la cuenta de cliente.

17 ¿Dónde puedo encontrar la lista de puntos finales regionales?

ConsulteLista de puntos finales de Security Hub.

18 ¿Puedo presentar los hallazgos entre regiones?

Security Hub aún no admite el envío de hallazgos entre regiones para el nativoAWSservicios, como AmazonGuardDuty, Amazon Macie y Amazon Inspector. Si su cliente lo permite, Security Hub no le impide enviar hallazgos de distintas regiones.

En este sentido, puede llamar a un extremo regional desde cualquier lugar y la información de recursos del ASFF no tiene que coincidir con la región del endpoint. Sin embargo,`ProductArn`debe coincidir con la región del endpoint.

19 ¿Cuáles son las reglas y directrices para enviar lotes de hallazgos?

Puede agrupar hasta 100 hallazgos o 240 KB en una sola llamada de`BatchImportFindings`. Poner en cola y agrupar tantos hallazgos como sea posible hasta este límite.

Puede agrupar un conjunto de hallazgos de cuentas diferentes. Sin embargo, si alguna de las cuentas del lote no está suscrita a Security Hub, se produce un error en todo el lote. Se trata de una limitación del modelo de autorización de línea base de API Gateway.

Consulte the section called “Directrices para el uso del`BatchImportFindings`API”.

20 ¿Puedo enviar actualizaciones de los hallazgos que he creado?

Sí, si envía una búsqueda con el mismo ARN del producto y el mismo ID de búsqueda, sobrescribe los datos anteriores de esa búsqueda. Tenga en cuenta que todos los datos se sobrescriben, por lo que debe enviar un hallazgo completo.

Los clientes reciben mediciones y facturas por nuevos hallazgos y actualizaciones de búsqueda.

21 ¿Puedo enviar actualizaciones de los hallazgos creados por otra persona?

Sí, si el cliente le concede acceso a la`BatchUpdateFindings`Operación de API, puedes actualizar ciertos campos mediante esa operación. Esta operación está diseñada para ser utilizada por clientes, SIEM, sistemas de emisión de tickets y plataformas de orquestación, automatización y respuesta de seguridad (SOAR).

22 ¿Cómo han envejecido los hallazgos?

Security Hub caduca los hallazgos 90 días después de la última actualización. Transcurrido este tiempo, los hallazgos caducados se purgan del Security HubOpenSearchclúster.

Si actualiza un hallazgo con el mismo ID de búsqueda y se ha caducado, se crea una nueva búsqueda en Security Hub.

Los clientes pueden utilizarCloudWatchEventos para sacar los hallazgos de Security Hub. Al hacerlo, todos los hallazgos se envían a los objetivos elegidos por el cliente.

En general, Security Hub recomienda crear nuevos hallazgos cada 90 días y no actualizar los hallazgos para siempre.

23 ¿Qué aceleradores pone en marcha Security Hub?

aceleradores de Security Hub`GetFindings`Llamadas a la API, ya que el enfoque recomendado para acceder a los hallazgos está utilizandoCloudWatchEventos: .

Security Hub no implementa ningún otro tipo de limitación en los servicios internos, socios o clientes más allá de la aplicada por las invocaciones de API Gateway y Lambda.

24 ¿Cuáles son los SLA de puntualidad o latencia o las expectativas para los hallazgos que se envían a Security Hub desde los servicios de origen?

El objetivo es ser lo más casi real posible para los hallazgos iniciales y las actualizaciones de los hallazgos. Debe enviar los hallazgos a Security Hub dentro de los cinco minutos posteriores a su creación.

25 ¿Cómo puedo recibir los resultados de Security Hub?

Para recibir los resultados, utilice alguno de los métodos siguientes.

- Todos los resultados se envían automáticamente aCloudWatchEventos: . Un cliente puede crear específicosCloudWatchReglas de eventos para enviar hallazgos a objetivos específicos, como un SIEM o un bucket de S3. Esta capacidad sustituyó al legado`GetFindings`Operación de la API.
- UsarCloudWatchEventos para acciones personalizadas. Security Hub permite a los clientes seleccionar resultados específicos o grupos de hallazgos desde la consola y tomar medidas al respecto. Por ejemplo, pueden enviar resultados a un SIEM, un sistema de emisión de tickets, una plataforma de chat o un flujo de trabajo de corrección. Esto formaría parte de un flujo de trabajo de clasificación de alertas que un cliente realiza dentro de Security Hub. Estas acciones se denominan acciones personalizadas.

  Cuando un usuario selecciona una acción personalizada, unCloudWatchse crea para esos hallazgos específicos. Podrías aprovechar esta capacidad y desarrollarCloudWatchReglas y objetivos de eventos para que un cliente las utilice como parte de una acción personalizada. Tenga en cuenta que esta capacidad no se utiliza para enviar automáticamente todos los resultados de un tipo o clase en particular aCloudWatchEventos: . Corresponde a un usuario tomar medidas sobre hallazgos específicos.

  Puede utilizar las operaciones de la API de acción personalizada, como`CreateActionTarget`, para crear automáticamente acciones disponibles para el producto (por ejemplo, utilizarAWS CloudFormationplantillas). También usaríasCloudWatchOperaciones de API de reglas de eventos para crear las correspondientesCloudWatchReglas de eventos asociadas a la acción personalizada. Uso deAWS CloudFormationplantillas, también puedes crearCloudWatchReglas de eventos para ingerir automáticamente de Security Hub todos los hallazgos o todos los hallazgos con ciertas características.

26 ¿Cuáles son los requisitos para que un proveedor de servicios de seguridad administrados (MSSP) se convierta en socio de Security Hub?

Debe demostrar cómo se utiliza Security Hub como parte de la prestación de servicios a los clientes.

Debe tener documentación de usuario que explique su uso de Security Hub.

Si el MSSP es un proveedor de búsquedas, debe demostrar el envío de hallazgos a Security Hub.

Si el MSSP solo recibe hallazgos de Security Hub, debe tener como mínimo unAWS CloudFormationplantilla para configurarCloudWatchReglas de eventos.

27 ¿Cuáles son los requisitos para que un socio consultor de APN que no sea MSSP se convierta en socio de Security Hub?

Si es socio consultor de APN, puede convertirse en socio de Security Hub. Debe presentar dos casos prácticos privados sobre cómo ayudó a un cliente específico a hacer lo siguiente.

- Configure Security Hub con los permisos de IAM que necesita el cliente.
- Ayuda a conectar soluciones de proveedor de software independiente (ISV) ya integradas a Security Hub mediante las instrucciones de configuración de la página de socios de la consola.
- Ayude a los clientes con integraciones de productos personalizadas.
- Cree información personalizada relevante para las necesidades de los clientes y los conjuntos de datos.
- Cree acciones personalizadas.
- Cree libros de jugadas de remediación.
- Compilación de inicios rápidos que se ajusten a los estándares de cumplimiento de Security Hub. El equipo de Security Hub debe validarlos.

Los estudios de casos no necesitan compartirse públicamente.

28 ¿Cuáles son los requisitos en torno a cómo implemento mi integración con Security Hub con mis clientes?

Las arquitecturas de integración entre Security Hub y los productos de socios varían de un socio a otro en términos de cómo se opera la solución de ese socio. Debe asegurarse de que el proceso de configuración de la integración no tarda más de 15 minutos.

Si está implementando software de integración en el clienteAWSentorno, debe aprovecharAWS CloudFormationplantillas para simplificar la integración. Algunos socios han creado una integración con un solo clic, lo que se recomienda encarecidamente.

29 ¿Cuáles son los requisitos de documentación?

Debe proporcionar un enlace a la documentación que describa el proceso de integración y configuración entre su producto y Security Hub, incluido el uso deAWS CloudFormationplantillas de.

Dicha documentación también debe incluir información sobre el uso del ASFF. Específicamente, debe enumerar los tipos de búsqueda de ASFF que está utilizando para sus diferentes hallazgos. Si tiene alguna definición de insight predeterminada, le recomendamos que también las incluya aquí.

Considere incluir otra información potencial:

- Su caso de uso para la integración con Security Hub
- Volumen medio de los resultados enviados
- Su arquitectura de integración
- Las regiones que usted admite y no admite
- Latencia entre cuándo se crean los hallazgos y cuándo se envían a Security Hub
- Si actualiza los hallazgos

30 ¿Qué son los insights personalizados?

Le animamos a definir información personalizada para sus hallazgos. Los insights son reglas de correlación ligeras que ayudan a un cliente a priorizar qué resultados y recursos requieren más atención y acción.

Security Hub tiene`CreateInsight`Operación de la API. Puede crear información personalizada dentro de una cuenta de cliente como parte de suAWS CloudFormationplantilla de. Estos conocimientos aparecen en la consola del cliente.

31 ¿Puedo enviar widgets de panel?

Actualmente no. Solo puede crear conocimientos administrados.

32 ¿Cuál es su modelo de precios?

ConsulteInformación sobre precios de Security Hub.

33. ¿Cómo envío los resultados a la cuenta demo de Security Hub como parte del proceso de aprobación final de mi integración?

    Envíe los resultados a la cuenta de demostración de Security Hub utilizando el ARN del producto proporcionado, medianteus-west-2como región. Los resultados deben incluir el número de cuenta demo en elAwsAccountIdcampo del ASFF. Para obtener el número de cuenta demo, póngase en contacto con el equipo de Security Hub.

    No nos envíe datos confidenciales ni información de identificación personal. Estos datos se utilizan para demostraciones públicas. Cuando nos envía estos datos, nos autoriza a utilizarlos en demostraciones.

34. Qué mensajes de error o de éxito**BatchImportFindings**proporcionar?

    Security Hub proporciona una respuesta para la autorización y una respuesta paraBatchImportFindings. Se están desarrollando mensajes de éxito, fallos y errores más nítidos.

35. ¿De qué gestión de errores es responsable el servicio de origen?

    Los servicios de origen son responsables de todo el tratamiento de errores. Deben gestionar mensajes de error, reintentos, limitación y alarmantes. También deben gestionar los comentarios o los mensajes de error enviados a través del mecanismo de comentarios de Security Hub.

36. ¿Cuáles son algunas soluciones a problemas comunes?

    UnAuthorizerConfigurationExceptiones causada por un mal formadoAwsAccountIdoProductArn.

    Al solucionar problemas, tenga en cuenta lo siguiente:

    - AwsAccountIddebe tener 12 dígitos exactamente.
    - ProductArndebe tener el siguiente formato: arn:aws:securityhub:*<us-west-2 or us-east-1>*:*<accountId>*:producto/*<company-id>*/*<product-id>*

      El ID de cuenta no cambia del que el equipo de Security Hub incluyó en los ARN del producto que le proporcionó.

    AccessDeniedExceptionse produce cuando se envía un hallazgo hacia o desde la cuenta incorrecta, o cuando la cuenta no tiene unProductSubscription. El mensaje de error contendrá un ARN con un tipo de recurso deproductoproduct-subscription. Este error solo se produce durante las llamadas entre cuentas. Si llamasBatchImportFindingscon tu propia

cuenta para la misma cuenta en`AwsAccountId`y`ProductArn`, la operación utiliza políticas de IAM y no tiene nada que ver con`ProductSubscriptions`.

Asegúrese de que la cuenta de cliente y la cuenta de producto que utiliza sean las cuentas registradas reales. Algunos socios han utilizado un número de cuenta para el producto del ARN del producto, pero intentan utilizar una cuenta completamente diferente para llamar`BatchImportFindings`. En otros casos, crearon`ProductSubscriptions`para otras cuentas de clientes o incluso para su propia cuenta de producto. No crearon`ProductSubscriptions`para la cuenta de cliente a la que intentaron importar hallazgos.

37. ¿Dónde envío preguntas, comentarios y errores?

    `<securityhub-partners@amazon.com>`

38. ¿A qué región envío los resultados de los artículos relacionados con el global?AWSservicios? Por ejemplo, ¿a dónde envío los hallazgos relacionados con IAM?

    Envíe los resultados a la misma región en la que se detectó el hallazgo. Para un servicio como IAM, es probable que su solución encuentre el mismo problema de IAM en varias regiones. En este caso, el hallazgo se envía a todas las regiones en las que se detectó el problema.

    Si el cliente ejecuta Security Hub en tres regiones y se detecta el mismo problema de IAM en las tres regiones, envíe la búsqueda a las tres regiones.

    Cuando se resuelva un problema, envíe la actualización de la búsqueda a todas las regiones a las que envió la búsqueda original.

Historial de documentos de la Guía de integración de

En la siguiente tabla se describen las actualizaciones de la documentación de esta guía.

Cambio	Descripción	Fecha
Requisitos actualizados para el logotipo de la consola	Se actualizaron las pautas del logotipo y el manifiesto de socios para indicar que los socios deben proporcionar una versión del logotipo en modo claro y en modo oscuro para que se muestre en la consola de Security Hub. Los logotipos deben estar en formato SVG.	10 de mayo de 2021
Se actualizaron los requisitos previos para los nuevos socios de integración	Security Hub ahora también permite a los socios que se han unido alAWSLa trayectoria de los socios ISV y quienes utilizan un producto de integración que ha completado unAWSRevisión técnica fundamental (FTR). Anteriormente, todos los socios de integración tenían que serAWSSeleccione Socios de nivel.	29 de abril de 2021
NuevoFindingProviderFields objeto en ASFF	Se actualizó la información sobre el mapeo de hallazgos a ASFF. ParaConfidence ,Criticality ,RelatedFindings ,Severity, yTypes, los socios asignan sus valores	18 de marzo de 2021

	a los campos de`FindingProviderFields` .	
Nuevos principios para crear y actualizar los hallazgos	Se agregó un nuevo conjunto de pautas para crear nuevos hallazgos y actualizar los hallazgos existentes en Security Hub.	4 de diciembre de 2020
Versión inicial de esta guía	EstoGuía de integración de sociosproporcionaAWSsocios con información sobre cómo establecer una integración conAWS Security Hub.	23 de junio de 2020

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.