Guía de integración de socios

AWS Security Hub CSPM

AWS Security Hub CSPM: Guía de integración de socios

Table of Contents

Descripción general de la integración de terceros con AWS Security Hub CSPM

Esta guía está destinada a los AWS socios de Partner Network (APN) con los que deseen crear una integración. AWS Security Hub CSPM

Como socio de APN, puede realizar la integración con Security Hub CSPM de una o varias de las siguientes maneras.

- Envíe los resultados a Security Hub (CSPM)
- Consume las conclusiones de Security Hub (CSPM)
- Ambos envían y consumen los hallazgos de Security Hub (CSPM).
- Utilice Security Hub CSPM como el centro de la oferta de un proveedor de servicios de seguridad gestionados (MSSP)
- Consulte a los AWS clientes sobre cómo implementar y usar Security Hub (CSPM)

Esta guía de incorporación se centra principalmente en los socios que envían las conclusiones a Security Hub (CSPM).

Temas

¿Por qué integrarse con? AWS Security Hub CSPM

AWS Security Hub CSPMproporciona una visión completa de las alertas de seguridad de alta prioridad y el estado de seguridad en todas las cuentas CSPM de Security Hub. Security Hub CSPM permite a socios como usted enviar las conclusiones de seguridad a Security Hub CSPM para ofrecer a sus clientes información sobre las conclusiones de seguridad que usted genera.

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

- Satisface a sus clientes que han solicitado una integración de Security Hub (CSPM)

- Proporciona a sus clientes una visión única de sus hallazgos relacionados con la seguridad AWS
- Permite que clientes nuevos descubran su solución cuando buscan socios que les proporcionen resultados relacionados con tipos específicos de eventos de seguridad

Antes de crear una integración con Security Hub CSPM, examine los motivos de la integración. Es más probable que una integración tenga éxito si sus clientes desean una integración de Security Hub CSPM con su producto. Puede crear una integración únicamente por motivos de marketing o bien para captar nuevos clientes. Sin embargo, si crea la integración sin conocer la opinión de sus clientes actuales y no tiene en cuenta sus necesidades, es posible que la integración no arroje los resultados esperados.

Preparándose para enviar las conclusiones a AWS Security Hub CSPM

Como socio de APN, no puede enviar información a Security Hub CSPM para sus clientes hasta que el equipo de CSPM de Security Hub lo autorice como proveedor de búsqueda. Para poder ser habilitado como proveedor de resultados, debe seguir estos pasos de incorporación. De este modo, se garantiza una experiencia positiva (Security Hub CSPM) para usted y sus clientes.

A medida que vaya completando los pasos de incorporación, asegúrese de seguir las pautas de the section called “Fundamentos para crear y actualizar los resultados”, the section called “Directrices para la asignación de ASFF” y the section called “Directrices para el uso de la API de `BatchImportFindings`”.

1. Asigne sus hallazgos de seguridad al formato de búsqueda AWS de seguridad (ASFF).
2. Cree su arquitectura de integración para llevar los hallazgos al punto final CSPM del Regional Security Hub correcto. Para ello, debe definir si va a enviar los resultados desde su propia AWS cuenta o desde las cuentas de sus clientes.
3. Haga que sus clientes suscriban el producto a sus cuentas. Para ello pueden utilizar la consola o la operación de la API de `EnableImportFindingsForProduct`. Consulte Administración de integraciones de productos en la Guía del usuario de AWS Security Hub.

   También puede suscribirles usted mismo al producto. Para ello, use un rol entre cuentas para acceder a la operación de la API `EnableImportFindingsForProduct` en nombre del cliente.

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

En las siguientes entradas del blog se analizan algunas de las integraciones de socios existentes con Security Hub CSPM.

- Anunciamos la integración de Cloud Custodian con AWS Security Hub CSPM
- Utilice AWS Fargate Ant Prowler para enviar los resultados de la configuración de seguridad sobre los AWS servicios a Security Hub (CSPM)
- Cómo importar AWS Config las evaluaciones de reglas como hallazgos en Security Hub (CSPM)

Preparándose para recibir las conclusiones de AWS Security Hub CSPM

Para recibir los resultadosAWS Security Hub CSPM, utilice una de las siguientes opciones:

- Haz que tus clientes envíen automáticamente todos los resultados a CloudWatch Events. Un cliente puede crear reglas de CloudWatch eventos específicas para enviar las conclusiones a objetivos específicos, como un SIEM o un bucket de S3.
- Haga que sus clientes seleccionen hallazgos específicos o grupos de hallazgos desde la consola CSPM de Security Hub y, a continuación, tomen medidas al respecto.

Por ejemplo, sus clientes pueden enviar los resultados a un SIEM, un sistema de ticketing, 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 en Security Hub CSPM.

Estas acciones se denominan acciones personalizadas. Cuando un usuario realiza una acción personalizada, se crea un CloudWatch evento para esos hallazgos específicos. Como socio, puede aprovechar esta capacidad y crear reglas u objetivos de CloudWatch eventos para que un cliente los utilice como parte de una acción personalizada. Tenga en cuenta que esta función no envía automáticamente todos los resultados de un tipo o clase en particular a CloudWatch Events. Esta función permite al usuario tomar medidas en relación con resultados concretos.

Las siguientes publicaciones del blog describen las soluciones que utilizan la integración con Security Hub, CSPM y CloudWatch Events para realizar acciones personalizadas.

- Cómo integrar acciones AWS Security Hub CSPM personalizadas con PagerDuty
- Cómo habilitar las acciones personalizadas en AWS Security Hub CSPM
- Cómo importar AWS Config las evaluaciones de reglas como hallazgos en Security Hub (CSPM)

Recursos para aprender sobre AWS Security Hub CSPM

Los siguientes materiales pueden ayudarle a comprender mejor la AWS Security Hub CSPM solución y cómo AWS los clientes pueden utilizar el servicio.

- Vídeo de introducción a AWS Security Hub CSPM
- Guía del usuario de Security Hub
- Referencia de la API de Security Hub
- Seminario web de incorporación

También le recomendamos que habilite Security Hub CSPM en una de sus AWS cuentas y adquiera experiencia práctica con el servicio.

Requisitos previos para los socios

Para poder iniciar una integración conAWS Security Hub CSPM, debe cumplir uno de los siguientes criterios:

- Es un socio de nivel AWS selecto o superior.
- Se ha unido a AWSISV Partner Path y el producto que utiliza para la integración de Security Hub CSPM ha superado una revisión técnica AWS fundamental (FTR). A continuación, el producto recibe el distintivo «Revisado por». AWS

También debe tener un acuerdo de confidencialidad mutua conAWS.

Casos de uso de integración y permisos necesarios

AWS Security Hub CSPM permite a AWS los clientes recibir las conclusiones de los socios de APN. Los productos del socio pueden estar disponibles dentro o fuera de la AWS cuenta del cliente. La configuración de permisos en la cuenta del cliente varía en función del modelo que utilice el producto del socio asociado.

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

Para permitir que un socio envíe las comprobaciones de seguridad a su cuenta, el cliente primero se suscribe al producto del socio en Security Hub CSPM. El paso de suscripción es necesario para todos los casos de uso que se describen a continuación. Para obtener más información sobre cómo los clientes administran las integraciones de productos, consulte Administración de integraciones de productos en la Guía del usuario de AWS Security Hub .

Cuando un cliente se suscribe a un producto asociado, Security Hub CSPM crea automáticamente una política de recursos gestionados. La política otorga al producto asociado permiso para usar la operación de la `BatchImportFindings`API para enviar los resultados a Security Hub CSPM para la cuenta del cliente.

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

Alojado por un socio: los resultados se envían desde la cuenta del socio

Este caso de uso incluye a los socios que alojan un producto en su propia cuenta. AWS Para enviar las comprobaciones de seguridad a un AWS cliente, el socio llama a la operación de la `BatchImportFindings`API desde la cuenta del producto del socio.

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

En la cuenta del socio, la entidad principal de IAM que llama a la operación de la API de `BatchImportFindings` debe tener una política de IAM que permita a dicha entidad realizar llamadas a `BatchImportFindings`.

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

1. El cliente crea una suscripción a un producto asociado en Security Hub CSPM.
2. Security Hub CSPM genera la política de recursos gestionados correcta con la confirmación del cliente.

Para enviar los resultados de seguridad relacionados con la cuenta del cliente, el producto del socio utiliza su propia credencial para llamar a la operación de la API de `BatchImportFindings`.

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

JSON

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

Alojado por un socio: los resultados se envían desde la cuenta del cliente

Este caso de uso se aplica a los socios que alojan un producto en su propia AWS cuenta, pero utilizan una función multicuenta para acceder a la cuenta del cliente. Llaman a la operación de la API de `BatchImportFindings` desde la cuenta del cliente.

En este caso de uso, para llamar a la operación de la API de `BatchImportFindings`, la cuenta del 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 en la llamada se utilice el ARN del producto para la cuenta del producto del socio. La política de recursos gestionados CSPM de Security Hub concede permisos para la cuenta del producto del socio y el ARN del producto asociado. El ARN del producto es el identificador único del socio como proveedor. Como la llamada no proviene de la cuenta del producto asociado, el cliente debe conceder permiso explícito para que el producto asociado envíe las conclusiones a Security Hub CSPM.

Lo más conveniente para los roles entre cuentas de los socios y las de los clientes es utilizar un identificador externo que proporcione el socio. Este identificador externo forma parte de la definición de la política entre cuentas de la cuenta del cliente. El socio debe proporcionar el identificador cuando asuma el rol. Un identificador externo proporciona un nivel de seguridad adicional a la hora de conceder acceso a la AWS cuenta a un socio. El identificador único garantiza que el socio utilice la cuenta de cliente correcta.

La activación de un producto asociado para enviar las conclusiones al cliente en Security Hub CSPM con una función multicuenta se realiza en cuatro pasos:

1. El cliente, o el socio que utiliza funciones multicuentas que trabajan en nombre del cliente, inicia la suscripción a un producto en Security Hub CSPM.
2. Security Hub CSPM genera la política de recursos gestionados correcta con la confirmación del cliente.
3. El cliente configura la función multicuenta de forma manual o mediante. CloudFormation Para obtener información sobre las funciones multicuenta, consulte Proporcionar acceso a AWS cuentas propiedad de terceros en la Guía del usuario de IAM.
4. El producto almacena de forma segura el rol del cliente y el identificador externo.

A continuación, el producto envía los resultados al Security Hub CSPM:

1. El producto llama a AWS Security Token Service (AWS STS) para asumir el rol de cliente.
2. El producto llama CSPM a la operación de la `BatchImportFindings`API en Security Hub con las credenciales temporales del rol asumido.

A continuación, se muestra un ejemplo de una política de IAM que concede los permisos CSPM de Security Hub necesarios para el rol multicuenta del socio.

JSON

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

En la sección `Resource` de la política se identifica la suscripción del producto específico. Esto garantiza que el socio solo pueda enviar los resultados del producto de socio al que está suscrito el cliente.

Alojado por el cliente: los resultados se envían desde la cuenta del cliente

Este caso de uso se refiere a los socios que tienen un producto implementado en la cuenta de AWS del cliente. Se llama a la API de `BatchImportFindings` desde la solución que se ejecuta en la cuenta del cliente.

En este caso de uso, se deben conceder permisos adicionales al producto del socio para llamar a la API de `BatchImportFindings`. La forma en que se concede este permiso varía según la solución del socio y la forma en que esté configurada en la cuenta del cliente.

Un ejemplo de este enfoque es el producto de un socio que se ejecuta en una instancia de EC2 en la cuenta del cliente. Esta instancia de EC2 debe tener asociado un rol de instancia de EC2 que le permita llamar a la operación de la API de `BatchImportFindings`. Esto permite que la instancia de EC2 envíe los resultados de seguridad a la cuenta del cliente.

Este caso de uso es funcionalmente equivalente a un escenario en el que un cliente carga en su cuenta los resultados de un producto que le pertenece.

El cliente permite que el producto asociado envíe las conclusiones de la cuenta del cliente al cliente en Security Hub CSPM:

1. El cliente implementa el producto del socio en su AWS cuenta de forma manual o mediante otra CloudFormation herramienta de implementación.
2. El cliente define la política de IAM necesaria para que el producto del socio la utilice cuando envíe las conclusiones a Security Hub CSPM.
3. El cliente adjunta la política a los componentes necesarios del producto del socio, como una instancia de EC2, un contenedor o una función de Lambda.

Ahora el producto puede enviar los resultados al Security Hub CSPM:

1. El producto asociado utiliza el AWS SDK o llama AWS CLI a la operación `BatchImportFindings`API en Security Hub CSPM. Realiza la llamada desde el componente de la cuenta del cliente al que se adjunta la política.
2. Durante la llamada a la API, se genera la credencial provisional necesaria para que la llamada de `BatchImportFindings` se realice correctamente.

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

JSON

```
{
    "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, tendrá que seguir varios pasos de alto nivel como parte de su proceso de incorporación. Debe completar estos pasos antes de poder enviar las comprobaciones de seguridad aAWS Security Hub CSPM.

1. Inicia una relación con el equipo de socios de APN o el equipo de CSPM del Security Hub y expresa su interés en convertirse en socio del Security Hub CSPM. Identifica las direcciones de correo electrónico que desea añadir a los canales de comunicación CSPM de Security Hub.
2. AWSIe proporciona los materiales de incorporación de socios de CSPM de Security Hub.
3. Te invitamos al canal Slack, socio de CSPM de Security Hub, donde podrás hacer preguntas relacionadas con tu integración.
4. Entregue a los contactos de los socios de APN un borrador del manifiesto de integración del producto para que lo revisen.

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

   Proporciona al equipo de CSPM de Security Hub la información que aparece en la página del proveedor asociado en la consola de CSPM de Security Hub. También se utiliza para proponer nuevos conocimientos gestionados relacionados con la integración para añadirlos a la biblioteca de conocimientos de CSPM de Security Hub.

   No es necesario que esta versión inicial del manifiesto de integración del producto incluya todos los detalles. Sin embargo, debe contener al menos el caso de uso y la información del conjunto de datos.

   Para obtener más información sobre el manifiesto y la información requerida, consulte Manifiesto de integración de producto.
5. El equipo de CSPM de Security Hub le proporciona un ARN de producto para su producto. El ARN se utiliza para enviar los resultados al Security Hub CSPM.
6. La integración se crea para enviar o recibir las conclusiones de Security Hub (CSPM).

   Asignación de resultados al ASFF

   Para enviar los resultados al Security Hub CSPM, debe asignarlos al AWS Security Finding Format (ASFF).

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

El ASFF es el formato de protocolo de conexión obligatorio que se debe utilizar para enviar resultados a AWS Security Hub CSPM. Los resultados se representan como documentos JSON que siguen el esquema JSON de ASFF y el RFC-7493, el formato de mensaje I-JSON. Si desea más información sobre el esquema ASFF, consulte Formato de resultados de seguridad de AWS (ASFF) en la Guía del usuario de AWS Security Hub.

Consulte the section called “Directrices para la asignación de ASFF”.

Creación y prueba de la integración

Puede completar todas las pruebas de la integración con una AWS cuenta de su propiedad. Si lo hace, obtendrá una visibilidad total de cómo aparecen los hallazgos en Security Hub CSPM. Esto también le ayudará a comprender la experiencia del cliente con sus resultados de seguridad.

La operación de `BatchImportFindings`API se utiliza para enviar los resultados nuevos y actualizados a Security Hub CSPM.

Durante la creación de una integración de Security Hub CSPM, le AWS anima a mantener informados a sus contactos de socios de APN sobre el progreso de la integración. También puede pedir ayuda a sus contactos de socios de APN con las preguntas sobre la integración.

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

7. Demuestra la integración al equipo de producto CSPM de Security Hub. Esta integración debe demostrarse mediante una cuenta que sea propiedad del equipo CSPM de Security Hub.

   Si se sienten cómodos con la integración, el equipo de CSPM de Security Hub da su aprobación para pasar a incluirlo como proveedor.
8. Usted AWS proporciona un manifiesto final para su revisión.
9. El equipo de CSPM de Security Hub crea la integración del proveedor en la consola CSPM de Security Hub. A continuación, los clientes pueden empezar a descubrir y habilitar la integración.
10. (Opcional) Realiza esfuerzos de marketing adicionales para promover la integración de Security Hub CSPM. Consulte Go-to-market actividades.

Como mínimo, Security Hub CSPM recomienda proporcionar los siguientes recursos.

- Un vídeo de demostración (de tres minutos como máximo) del funcionamiento de la integración. El vídeo se utiliza con fines de marketing y se publica en el AWS YouTube canal.
- Un diagrama de arquitectura de una sola diapositiva para añadir al conjunto de diapositivas de primera llamada del Security Hub CSPM.

Go-to-market actividades

Los socios también pueden participar en actividades de marketing opcionales para explicar y promocionar su integración de AWS Security Hub CSPM.

Si desea crear su propio contenido de marketing relacionado con Security Hub CSPM, antes de publicarlo, envíe un borrador al administrador de socios de APN para que lo revise y apruebe. De este modo se garantiza una coordinación total en cuanto a la mensajería.

AWSLos socios de la Red de Socios (APN) pueden utilizar la Central de Marketing para Socios de APN y el programa Market Development Funds (MDF) para crear campañas y obtener financiación. Para obtener más información sobre estos programas, póngase en contacto con su administrador de socios.

Entrada en la página de socios de Security Hub CSPM

Una vez que se le apruebe como socio de CSPM de Security Hub, su solución podrá mostrarse en la página de AWS Security Hub CSPMsocios.

Para aparecer en esta página, proporcione los siguientes detalles a sus contactos de socios de APN. Dichos contactos pueden ser el administrador de desarrollo de socios (PDM) o el arquitecto de soluciones de socios (PSA), o bien puede escribir un correo electrónico a `<securityhub-pms@amazon.com>`.

- Una breve descripción de su solución, su integración con Security Hub CSPM y el valor que la integración con Security Hub CSPM proporciona a los clientes. La descripción tiene un límite de 700 caracteres, incluidos los espacios.
- La URL de una página que describe su solución. Este sitio debe ser específico para su AWS integración y, más específicamente, para su integración con Security Hub CSPM. Debe estar centrado 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 los logotipos, consulte the section called “Logotipo para la página de socios”.

Nota de prensa

Como socio autorizado, si lo desea puede publicar un comunicado de prensa en su sitio web y en sus canales de relaciones públicas. El comunicado de prensa debe ser aprobado por. AWS

Antes de publicar el comunicado de prensa, debe enviarlo AWS para que lo revisen los socios de marketing de APN, los líderes de CSPM de Security Hub y los Servicios de Seguridad AWS Externos (ESS). El comunicado de prensa puede incluir una propuesta de presupuesto para el vicepresidente de ESS.

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

AWSBlog de Partner Network (APN)

También podemos ayudarle a publicar una entrada compuesta por usted en el blog de APN. La entrada del blog debe centrarse en una historia del cliente y en un caso de uso. No se puede publicar únicamente por ser el socio de lanzamiento de una integración.

Si le interesa, póngase en contacto con su PDM o PSA para iniciar el proceso. La aprobación final y la publicación de los blogs de APN pueden tardar ocho o más semanas.

Aspectos clave que debe saber sobre el blog de APN

Cuando cree una publicación para el blog, tenga en cuente lo siguiente.

¿Qué contenido se admite en una entrada de blog?

- Las publicaciones de los socios deben ser didácticas y proporcionar una experiencia detallada sobre un tema relevante para los clientes de AWS.
- La longitud ideal es de menos de 1500 palabras. Los lectores valoran el contenido profundo y educativo que les enseña lo que es posible hacer realidad. AWS
- El contenido debe ser original del blog de APN. No reutilice contenido de fuentes como publicaciones de blogs o documentos técnicos existentes.

¿Qué otros límites existen para la publicación en el blog de APN?

- Solo los socios de nivel avanzado o premier pueden publicar en el blog de APN. Puede haber excepciones con los socios de nivel selecto que cuentan con una designación de programa APN, como la entrega de servicios.

Existe un límite de tres publicaciones por año por socio. Dado que hay decenas de miles de socios de APNAWS debe proporcionar una cobertura igualitaria para todos.

Cada publicación debe contar con un patrocinador técnico que valide la solución o el caso de uso.

¿Cuánto tiempo se tarda en editar una publicación del blog antes de publicarla?

Una vez recibido el primer borrador completo de la entrada de blog, la edición tardará entre cuatro y seis semanas.

¿Qué interés tiene publicar en el blog de APN?

Una publicación en el blog de APN puede ofrecer los siguientes beneficios.

- Credibilidad: para los socios de APN, el hecho de que una historia sea publicada por una persona AWS puede influir en los clientes de todo el mundo.
- Visibilidad: el blog de APN es uno de los blogs más leídos, AWS con 1,79 millones de páginas vistas en 2019, incluido el tráfico influido.
- Negocios: las publicaciones de los socios de APN tienen botones de conexión que pueden generar clientes potenciales a través del programa Interacciones con los Clientes de APN (ACE) de APN.

¿Qué tipo de contenido es el más adecuado?

Los siguientes tipos de contenido son los más adecuados para las entradas en el blog de APN.

- El contenido técnico es el tipo de historia más leído. Esto incluye soluciones destacadas e información de procedimientos. Más del 75 % de los lectores consultan este contenido técnico.
- Los clientes valoran las historias de nivel 200 o superior con demostraciones del funcionamiento de un producto en AWS o cómo un socio de APN ha resuelto un problema empresarial para sus clientes.
- Las publicaciones de los expertos técnicos o expertos en la materia son, con diferencia, las más valoradas.

Hoja de ventas u hoja de marketing

Una hoja de ventas es un documento de una página en el que se resume un producto, su arquitectura de integración y casos de uso conjuntos con los clientes.

Si crea una hoja detallada para su integración, envíe una copia al equipo de CSPM de Security Hub. Ellos la añadirán a la página de socios.

Documento técnico o libro electrónico

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

Seminario web

Si realiza un seminario web sobre su integración, envíe una grabación del seminario web al equipo de CSPM de Security Hub. El equipo creará un enlace al seminario desde la página de socios.

El equipo también puede proporcionarle un experto en la materia CSPM de Security Hub para que participe en su seminario web.

Vídeo de demostración

Puede producir un vídeo de demostración del funcionamiento de la integración para fines de marketing. Publique un vídeo de este tipo en su cuenta de plataforma de vídeo y el equipo de CSPM de Security Hub lo vinculará desde la página de socios.

Manifiesto de integración de producto

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

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

- Para crear el listado de su sitio web
- Para crear la tarjeta de producto para la consola CSPM 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 CSPM de Security Hub utiliza el. the section called “Lista de verificación de disponibilidad del producto” Esta lista de verificación determina si su integración está lista para su lanzamiento.

Toda la información técnica que proporcione también debe estar reflejada en la documentación.

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

Contenido

  - Línea directa
  - Resultados de latidos
- AWS Security Hub CSPM información de la consola
  - Información de la empresa
  - Información del producto

Casos de uso e información de marketing

Los siguientes casos de uso pueden ayudarle a AWS Security Hub CSPM configurarlo para distintos fines.

Caso de uso para encontrar proveedores y consumidores de resultados

Es necesario para los proveedores de software independientes (ISV).

Para describir su caso de uso en torno a su integración con AWS Security Hub CSPM, responda a las siguientes preguntas. Si no tiene previsto enviar ni recibir resultados, anótelo en esta sección y, a continuación, complete la siguiente.

La siguiente información debe estar reflejada en su documentación.

- ¿Enviará resultados, los recibirá o las dos cosas?
- Si tiene pensado enviar resultados, ¿qué tipos de resultados enviará? ¿Enviará todos los resultados o un subconjunto específico de ellos?
- Si tiene previsto recibir resultados, ¿qué hará con ellos? ¿Qué tipos de resultados recibirá? Por ejemplo, ¿recibirá todos los resultados, los de un tipo determinado o solo los resultados concretos que seleccione un cliente?
- ¿Planea actualizar los resultados? Si es así, ¿qué campos actualizará? Security Hub CSPM recomienda actualizar los hallazgos en lugar de crear siempre nuevos. La actualización de los resultados existentes ayuda a reducir el ruido que generan los resultados para los clientes.

  Para actualizar un resultado, envíelo con un identificador de resultado asignado a un resultado que ya haya enviado.

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

Caso de uso de socio de consultoría (CP)

Obligatorio si es socio consultor de CSPM de Security Hub.

Proporcione dos casos de uso de clientes para su trabajo con Security Hub CSPM. Pueden ser casos de uso privados. El equipo de CSPM de Security Hub no los anuncia en ningún sitio. Deberían describir una o ambas de las siguientes acciones.

- ¿Cómo puede ayudar a los clientes a iniciar Security Hub CSPM? Por ejemplo, ¿ha ayudado a los clientes a utilizar servicios profesionales, un módulo de Terraform o una plantilla? CloudFormation
- ¿Cómo ayuda a los clientes a poner en funcionamiento y ampliar el Security Hub CSPM? 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 CSPM.

Para las conclusiones que va a enviar a Security Hub CSPM, proporcione la siguiente información.

- Los resultados en su formato nativo, como JSON o XML
- Un ejemplo de cómo va a convertir los resultados al formato de búsqueda de AWS seguridad (ASFF)

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

Arquitectura

Obligatorio si envía o recibe las conclusiones de Security Hub (CSPM).

Describa cómo se integrará con Security Hub CSPM. Esta información 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:

- ¿Qué AWS servicios, agentes del sistema operativo, etc. va a utilizar?

- Si va a enviar los resultados a Security Hub CSPM, ¿los enviará desde la AWS cuenta del cliente o desde la suya propia? AWS
- Si va a recibir las conclusiones, ¿cómo utilizará la integración de CloudWatch eventos?
- ¿Cómo convertirá los resultados en ASFF?
- ¿Cómo agrupará los resultados, realizará un seguimiento de su estado y evitará las limitaciones controladas?

Configuración

Obligatorio si envía o recibe las conclusiones de Security Hub (CSPM).

Describa cómo un cliente configurará su integración con Security Hub.

Como mínimo, debe utilizar 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 resultados por día y cliente

Obligatorio si envía los resultados a Security Hub CSPM.

¿Cuántas actualizaciones de búsqueda al mes (media y máxima) espera enviar a Security Hub CSPM en toda su base de clientes? Las estimaciones de órdenes de magnitud son aceptables.

Latencia

Obligatorio si envía los resultados a Security Hub CSPM.

¿Con qué rapidez agrupará y enviará los resultados a Security Hub CSPM? En otras palabras, ¿cuál es la latencia desde que se crea el hallazgo en su producto hasta que se envía a Security Hub CSPM?

Esta información debe estar reflejada en la documentación de integración de su producto. Es una pregunta frecuente de los clientes.

Descripción de la empresa y del producto

Necesario para todas las integraciones con Security Hub CSPM.

Describa brevemente su empresa y su producto, haciendo especial hincapié en la naturaleza de su integración con el Security Hub CSPM. Lo utilizamos en nuestra página de socios de CSPM de Security Hub.

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

La descripción no puede tener más de 700 caracteres, espacios incluidos.

Activos del sitio web de socios

Necesario para todas las integraciones con Security Hub CSPM.

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

Si integra varios productos con Security Hub CSPM, puede tener una única página de inicio para ellos. Security Hub CSPM recomienda que esta página de inicio 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 CSPM también incluirá enlaces a los de su página de socios.

Logotipo para la página de socios

Necesario para todas las integraciones de Security Hub CSPM.

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

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

Logotipos para la consola Security Hub CSPM

Obligatorio para todas las integraciones.

Proporcione logotipos URLs al modo claro y al modo oscuro para que se muestren en la consola CSPM de Security Hub.

Los logotipos deben cumplir los siguientes requisitos:

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

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

Tipos de resultados

Obligatorio si envía los resultados a Security Hub CSPM.

Proporcione una tabla donde se documenten los tipos de resultados con formato ASFF que utiliza y cómo se alinean con sus tipos de resultados nativos. Para obtener información detallada sobre los tipos de resultados en ASFF, consulte Taxonomía de tipos de ASFF en la Guía del usuario de AWS Security Hub .

Le recomendamos que también incluya esta información en la documentación del producto.

Línea directa

Necesario para todas las integraciones con Security Hub CSPM.

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

Proporcione también un punto de contacto activo las 24 horas de los 7 días de la semana, para problemas técnicos muy graves.

Resultados de latidos

Se recomienda si envía los resultados a Security Hub CSPM.

¿Puede enviar a Security Hub CSPM un aviso cada cinco minutos que indique que su integración con el Security Hub CSPM es funcional?

Si puede, hágalo con el tipo de resultado `Heartbeat`.

AWS Security Hub CSPM información de la consola

Proporcione al AWS Security Hub CSPM equipo un texto en formato JSON que contenga la siguiente información. El CSPM de 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 CSPM de Security Hub.

Información de la empresa

Esta información 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.",
}
```

Esta tabla de información de la empresa contiene los siguientes campos:

Campo	Obligatorio	Descripción
`id`	Sí	El identificador único de la empresa. El identificador de la empresa debe ser único en todas las empresas. Es probable que sea igual o parecido a `name`. Tipo: cadena 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 en un número o una letra minúscula.
`name`	Sí	El nombre de la empresa del proveedor que se mostrará en la consola CSPM de Security Hub. Tipo: cadena Longitud máxima: 16 caracteres
`description`	Sí	La descripción de la empresa del proveedor que se mostrará en la consola CSPM de Security Hub. Tipo: cadena Longitud máxima: 200 caracteres

Información del producto

En esta sección se proporciona información relativa a 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 las conclusiones al Security Hub CSPM, las recibe del Security Hub CSPM o las envía y recibe a la vez. Un socio de consultoría debe dejar este campo en blanco. Tipo: matriz de cadenas 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 entre todas las empresas. Es probable que sea igual o parecido a `name`. Tipo: cadena Longitud mínima: 5 caracteres Longitud máxima: 24 caracteres Caracteres permitidos: letras minúsculas, números y guiones Debe comenzar con una letra minúscula. Debe terminar en un número o una letra minúscula.
`regionsNotSupported`	Sí	¿Cuál de las siguientes AWS regiones no es compatible? En otras palabras, ¿en qué

Campo	Obligatorio	Descripción
		regiones no debería mostrarte Security Hub CSPM como opción en nuestra página de socios en la consola de Security Hub CSPM? Tipo: cadena Proporcione únicamente el código de región. Por ejemplo, `us-west-1` . Para ver una lista de regiones, consulte Puntos de conexión regionales en la Referencia general de AWS. Los códigos de región AWS GovCloud (US) son `us-gov-west-1` (para (EE. UU. Oeste) y AWS GovCloud (para (EE. UU. Esteus-gov-east-1)). AWS GovCloud Los códigos de región para las regiones de China son `cn-north-1` (para China (Pekín)) y `cn-northwest-1` (para China (Ningxia)).

Campo	Obligatorio	Descripción
`commercialAccountNumber`	Sí	El número de AWS cuenta principal del producto para las AWS regiones. Si envías las conclusiones a Security Hub CSPM, la cuenta que proporciones dependerá del lugar desde el que envíes las conclusiones. • Desde tu cuenta. AWS En este caso, proporcione el número de cuenta que utilizó para enviar los resultados. • Desde la AWS cuenta del cliente. En este caso, Security Hub CSPM recomienda proporcionar el número de cuenta principal que se utiliza para probar la integración. Lo ideal es que use la misma cuenta para todos sus productos en todas las regiones. Si esto no es posible, póngase en contacto con el equipo de CSPM de Security Hub. Si solo recibe los resultados de Security Hub CSPM, este número de cuenta no es obligatorio. Tipo: cadena

Campo	Obligatorio	Descripción
`govcloudAccountNumber`	No	El número de AWS cuenta principal del producto para AWS GovCloud (US) las regiones (si su producto está disponible en AWS GovCloud (US)). Si envías las conclusiones a Security Hub CSPM, la cuenta que proporciones dependerá del lugar desde el que envíes las conclusiones. • Desde tu cuenta. AWS En este caso, proporcione el número de cuenta que utilizó para enviar los resultados. • Desde la AWS cuenta del cliente. En este caso, Security Hub CSPM recomienda proporcionar el número de cuenta principal que se utiliza para probar la integración. Lo ideal es que use la misma cuenta para todos sus productos en todas las regiones de AWS GovCloud (US) . Si esto no es posible, póngase en contacto con el equipo de CSPM de Security Hub. Si solo recibe los resultados de Security Hub CSPM, este número de cuenta no es obligatorio. Tipo: cadena

Campo	Obligatorio	Descripción
`chinaAccountNumber`	No	El número de AWS cuenta principal del producto para las regiones de China (si el producto está disponible en las regiones de China). Si envías las conclusiones a Security Hub CSPM, la cuenta que proporciones dependerá del lugar desde el que envíes las conclusiones. • Desde tu cuenta. AWS En este caso, proporcione el número de cuenta que utilizó para enviar los resultados. • Desde la AWS cuenta del cliente. En este caso, Security Hub CSPM recomienda que proporcione el número de cuenta principal que utilice para probar la integración del producto. Lo ideal es que use la misma cuenta para todos sus productos en todas las regiones de China. Si esto no es posible, póngase en contacto con el equipo de CSPM de Security Hub. Si solo recibes información de Security Hub CSPM, puede ser cualquier cuenta que tengas en una región de China. Tipo: cadena
`name`	Sí	El nombre del producto del proveedor que se mostrará en la consola CSPM de Security Hub. Tipo: cadena Longitud máxima: 24 caracteres

Campo	Obligatorio	Descripción
`description`	Sí	La descripción del producto del proveedor que se mostrará en la consola CSPM de Security Hub. Tipo: cadena Longitud máxima: 200 caracteres
`importType`	Sí	El tipo de política de recursos del socio. Durante el proceso de incorporación de socios, puede especificar una de las siguiente s políticas de recursos o bien puede especificar `NEITHER`. • Con `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` , solo puede enviar los resultados a Security Hub desde la cuenta que figura en el ARN de su producto. • Con `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` , solo puede enviar los resultados desde la cuenta de cliente que se ha suscrito a su producto. Tipo: cadena Valores válidos: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` | `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` | `NEITHER`

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

Campo	Obligatorio	Descripción
		• Data Classification • Data Loss Prevention • Data Masking and Tokenization • Database Activity Monitoring • DDoS Protection • Deception • Device Control • Dynamic Application Security Testing • Data Encryption • Email Gateway • Encrypted Search • Endpoint Detection and Response (EDR) • Endpoint Forensics • Forensics Toolkit • Fraud Detection • Governance, Risk, and Compliance (GRC) • Host-based Intrusion Detection (HIDs) • 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 de destino del producto AWS Marketplace . La URL se muestra en la consola CSPM de Security Hub. Tipo: cadena Debe ser una AWS Marketplace URL. Si no tienes ningún AWS Marketplace anuncio, deja este campo en blanco.

Campo	Obligatorio	Descripción
`configurationUrl`	Sí	La URL de la documentación del producto sobre la integración con Security Hub CSPM. Este contenido está alojado en su sitio web o en una página web que usted administre, como una GitHub página. Tipo: cadena La documentación debe incluir la siguiente información. • Instrucciones de configuración • Enlaces a CloudFormation plantillas (si es necesario) • Información sobre su caso de uso para la integración • Latencia • Asignación de ASFF • Tipos de resultados incluidos • Arquitectura

Directrices y listas de verificación

Al preparar los materiales necesarios para la AWS Security Hub CSPM integración, utilice estas pautas.

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

Temas

Directrices para la visualización del logotipo en la consola AWS Security Hub CSPM

Para que el logotipo aparezca en la AWS Security Hub CSPM consola, sigue estas pautas.

Modos claro y oscuro

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

Formato

Formato de archivo SGV

Color de fondo

Transparente

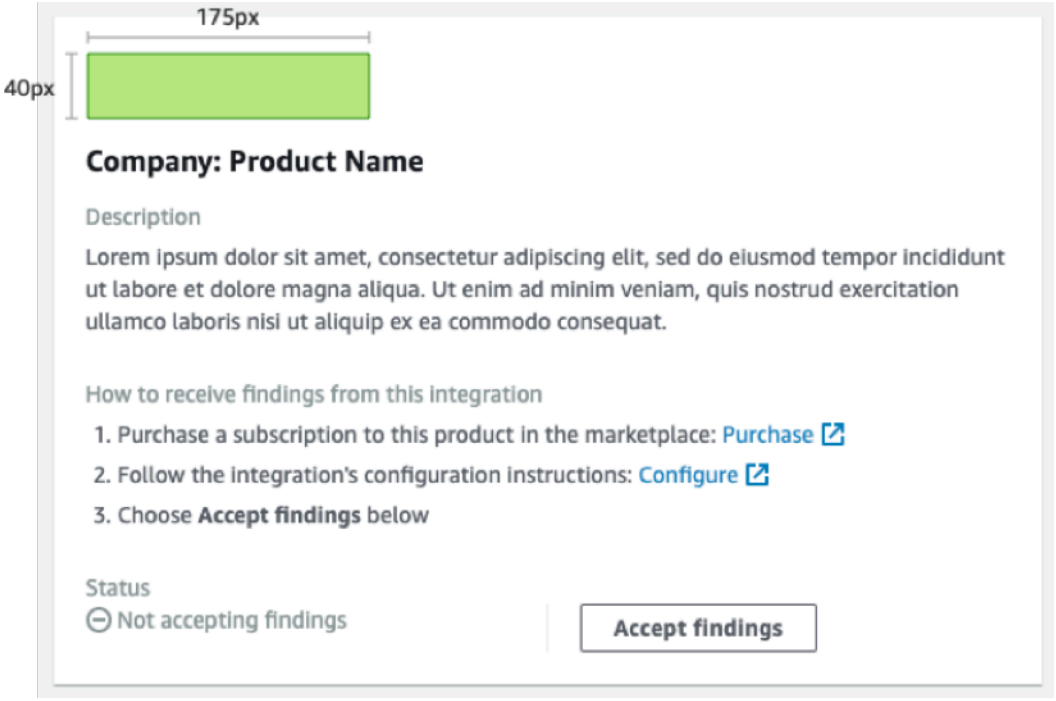
Tamaño

El tamaño ideal es de 175 px de ancho por 40 px de alto.

La altura mínima es de 40 px.

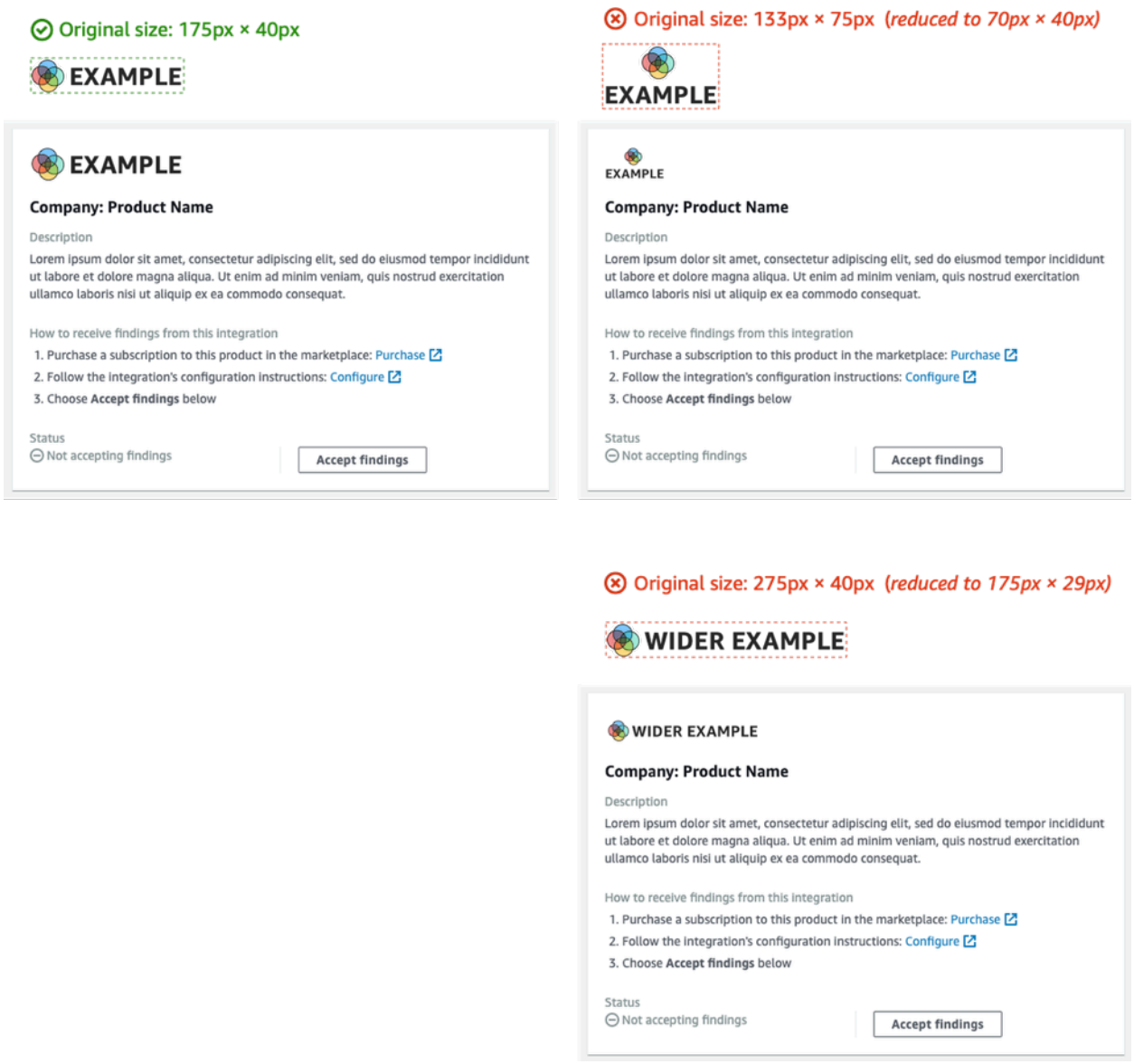
La forma óptima de los logotipos es la rectangular.

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



Si su logotipo no tiene estas dimensiones, Security Hub reducirá su tamaño a una altura máxima de 40 px y una anchura máxima de 175 px. Esto afecta a la forma en que se muestra el logotipo en la consola CSPM de Security Hub.

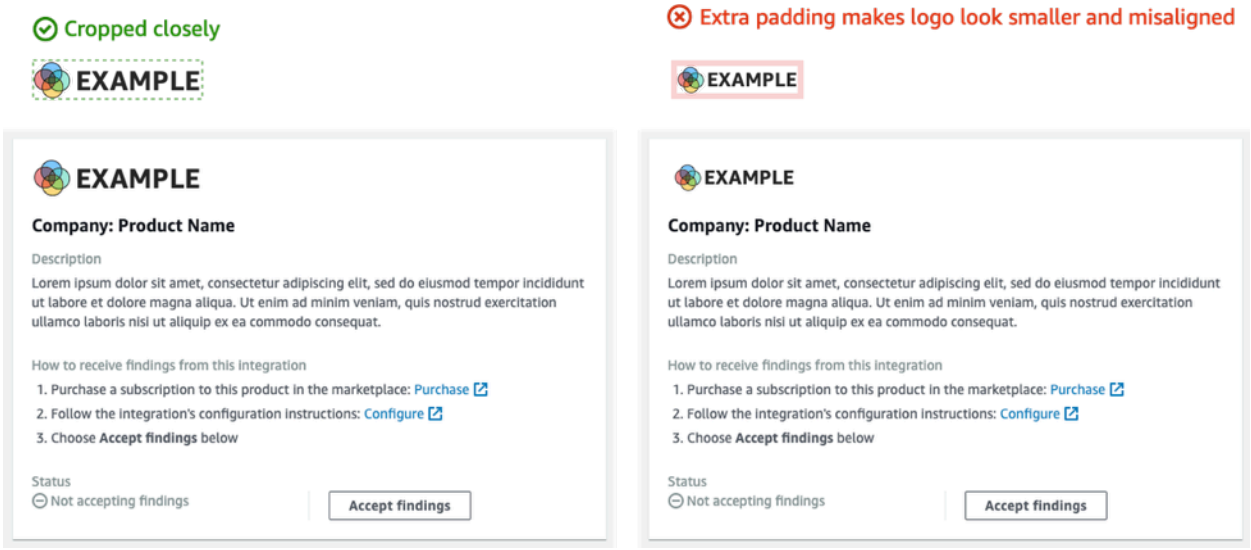
La siguiente imagen compara la visualización de un logotipo que tenía el tamaño ideal con la de logotipos más anchos o más altos.



Recortar

Recorte la imagen del logotipo tanto como pueda. No ponga relleno adicional.

La siguiente imagen muestra la diferencia entre un logotipo bien recortado y un logotipo que tiene un relleno adicional.



Fundamentos para crear y actualizar los resultados

Al planificar la forma en que va a crear y actualizar los hallazgos AWS Security Hub CSPM, tenga en cuenta los siguientes principios.

Los resultados deber ser tan específicos como sea posible para que los clientes puedan tomar las medidas apropiadas con facilidad.

> Los clientes prefieren las acciones de respuesta y corrección automatizadas y correlacionar los resultados con otros resultados. Para ello, los resultados deben tener las siguientes características:
>
> - Por lo general, deben referirse a un recurso único o primario.
> - Deben tener un único tipo de resultados.
> - Deben referirse a un único evento de seguridad.
>
> Si un resultado contiene datos de varios eventos de seguridad, a los clientes les resultará más difícil tomar medidas al respecto.

Asigne todos los campos de búsqueda al formato de búsqueda AWS de seguridad (ASFF). Permita que los clientes confíen en Security Hub CSPM como fuente de información fiable.

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

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

Minimice la redundancia en los resultados. No abrume a los clientes con grandes cantidades de resultados.

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

Si solo se produce un cambio menor en el resultado, actualícelo en lugar de crear uno nuevo.

Si el cambio producido en el resultado es importante, por ejemplo, se da en la puntuación de gravedad o en el identificador del recurso, cree un resultado nuevo.

Por ejemplo, crear resultados para los escaneos de puertos individuales en tiempo real no es muy práctico. Dado que el escaneo de puertos puede realizarse de forma continua, generaría una gran cantidad de resultados. Resulta mucho más convincente y preciso sencillamente actualizar la hora del último escaneo y el recuento de escaneos con un solo resultado para el escaneo de un puerto de MongoDB desde un nodo de TOR.

Permita que los clientes personalicen sus resultados para que sean más significativos.

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

Por ejemplo, los clientes desean poder añadir notas y etiquetas y ajustar las puntuaciones de gravedad en función del tipo de cuenta o el tipo de recurso al que esté asociado el resultado.

Directrices para mapear los hallazgos en el formato de búsqueda de AWS seguridad (ASFF)

Use las siguientes directrices para asignar sus resultados al ASFF. Para obtener descripciones detalladas de cada campo y objeto del ASFF, consulte Formato de resultados de seguridad de AWS (ASFF) en la Guía del usuario de AWS Security Hub .

Información de identificación

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

`ProductArn`es el ARN que se le AWS Security Hub CSPM asigna.

`Id`es el valor que utiliza Security Hub CSPM para indexar las conclusiones. El identificador de resultados debe ser único para garantizar que no se sobrescriban otros resultados. Para actualizar un resultado, vuelva a enviarlo con el mismo identificador.

`GeneratorId`puede ser igual `Id` o hacer referencia a una unidad lógica discreta, como un ID de GuardDuty detector de Amazon, un ID de AWS Config grabadora o un ID de IAM Access Analyzer.

Title y Description

`Title` debe contener alguna información sobre el recurso afectado. `Title` tiene un límite de 256 caracteres, incluidos los espacios.

Puede agregar información más larga y detallada en la `Description`. La `Description` tiene un límite de 1024 caracteres, espacios incluidos. Puede considerar la posibilidad de truncar 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 resultados

Proporcione la información del tipo de resultados en `FindingProviderFields.Types`.

`Types` debe coincidir con la taxonomía de tipos de ASFF.

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

Marcas de tiempo

El formato ASFF incluye algunas marcas temporales diferentes.

`CreatedAt` y `UpdatedAt`

Debe enviar `CreatedAt` y `UpdatedAt` cada vez que llame a `BatchImportFindings` para cada resultado.

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

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

`FirstObservedAt` y `LastObservedAt`

`FirstObservedAt` y `LastObservedAt` deben coincidir en el momento en que el sistema observó el resultado. Si esta información no se registra, no es necesario que envíe estas marcas temporales.

Los valores coinciden con el ISO8601 formato de Python 3.8.

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

Severity

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

`Original`

El valor de gravedad de su sistema. `Original` puede ser cualquier cadena, adaptada al sistema que utilice.

`Label`

El indicador CSPM de Security Hub requerido de la gravedad del hallazgo. Los valores permitidos son los siguientes:

- `INFORMATIONAL`: no se encontró ningún problema.
- `LOW`: el problema no requiere medidas por sí solo.
- `MEDIUM`: el problema debe abordarse, pero no es urgente.
- `HIGH`: el problema debe abordarse con prioridad.
- `CRITICAL`: el problema debe solucionarse de inmediato para evitar más daños.

Los resultados que cumplan con las normas siempre deben tener el valor de `Label` establecido en `INFORMATIONAL`. Algunos ejemplos de `INFORMATIONAL` hallazgos son los resultados de los controles de seguridad que se han superado y AWS Firewall Manager los que se han subsanado.

Los clientes suelen ordenar los resultados por su gravedad para ofrecer a sus equipos de operaciones de seguridad una lista de tareas pendientes. Establezca la gravedad del resultado en `HIGH` o `CRITICAL` con moderación.

La documentación de integración debe incluir la justificación de las asignaciones.

Remediation

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

`Remediation.Recommendation.Text` aparece en la sección Corrección de los detalles del resultado. Tiene un hipervínculo al valor de `Remediation.Recommendation.Url`.

Actualmente, solo los hallazgos de los estándares CSPM de Security Hub, IAM Access Analyzer y Firewall Manager muestran hipervínculos a la documentación sobre cómo corregir el hallazgo.

SourceUrl

Use `SourceUrl` solo si puede proporcionar una URL con un enlace profundo a su consola para ese resultado concreto. De lo contrario, omítalo de la asignación.

El CSPM de Security Hub no admite hipervínculos de este campo, pero está expuesto en la consola CSPM de Security Hub.

Malware, Network, Process, ThreatIntelIndicators

Cuando proceda, use `Malware`, `Network`, `Process` o `ThreatIntelIndicators`. Cada uno de estos objetos está expuesto en la consola CSPM de Security Hub. Utilice estos objetos en el contexto del resultado que va a enviar.

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

Malware

`Malware` es una lista que acepta hasta cinco conjuntos de información sobre malware. Haga que las entradas de malware sean relevantes para el recurso y el resultado.

Cada entrada cuenta con los siguientes campos:

`Name`

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

`Name` debe provenir de una fuente de investigación o de inteligencia sobre amenazas acreditada.

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

`State`

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

En el título y la descripción del resultado, asegúrese de incluir el contexto de lo que ha ocurrido con el malware.

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

Por ejemplo, si `Malware.State` es `OBSERVED`, el título y la descripción del resultado deberían reflejar que el producto ha encontrado el malware en la ruta.

`Type`

Indica el tipo de malware. Los valores permitidos son `ADWARE` | `BLENDED_THREAT` | `BOTNET_AGENT` | `COIN_MINER` | `EXPLOIT_KIT` | `KEYLOGGER` | `MACRO` | `POTENTIALLY_UNWANTED` | `SPYWARE` | `RANSOMWARE` | `REMOTE_ACCESS` | `ROOTKIT` | `TROJAN` | `VIRUS` | `WORM`.

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

Network

`Network` es un objeto único. No se pueden añadir varios detalles relacionados con la red. Aplique las siguientes directrices para asignar los campos.

Información sobre el destino y el origen

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

Por lo general, el origen es el lugar donde se origina el ataque, pero podría provenir de otros orígenes, como los que se indican a continuación. Debe explicar el origen en su documentación y también describirlo en el título y la descripción del resultado.

- En el caso de un ataque DDoS a una instancia de 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 de EC2. `Direction` es IN.
- En el caso de un malware al que se ha observado comunicándose desde una instancia de EC2 con un comando y nodo de control conocido, el origen es la dirección IPV4 de la instancia de EC2. El destino es el comando y nodo de control. `Direction` es `OUT`. También debe proporcionar `Malware` y `ThreatIntelIndicators`.

`Protocol`

`Protocol` siempre se asigna a un nombre registrado de la Internet Assigned Numbers Authority (IANA), a menos que pueda proporcionar un protocolo específico. Siempre debe usarlo y proporcionar la información del puerto.

`Protocol` es independiente de la información de origen y destino. Indíquelo solo cuando tenga sentido hacerlo.

`Direction`

`Direction`siempre es relativo a los límites de la AWS red.

- `IN`significa que está entrando AWS (VPC, servicio).
- `OUT`significa que está saliendo de los límites de la AWS red.

Process

`Process` es un objeto único. No se pueden añadir varios detalles relacionados con la red. Aplique las siguientes directrices para asignar los campos.

`Name`

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

`Path`

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

`Pid`, **`ParentPid`**

`Pid` y `ParentPid` deben coincidir con el identificador de proceso (PID) de Linux o el ID de evento de Windows. Para distinguirlos, utilice las imágenes de máquina de Amazon (AMI) de EC2 para proporcionar la información. Los clientes probablemente puedan distinguir entre Windows y Linux.

Marcas temporales (**`LaunchedAt`** y **`TerminatedAt`**)

Si no puede recuperar esta información de forma fiable, y no tienen una precisión de milisegundos, no las proporcione.

Si un cliente confía en las marcas temporales para realizar una investigación forense, es mejor no contar con dicha marca que tener una marca temporal incorrecta.

ThreatIntelIndicators

`ThreatIntelIndicators` acepta un conjunto de hasta cinco objetos de inteligencia 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_ADDRESS` | `MUTEX` | `PROCESS` | `URL`.

Estos son algunos ejemplos de cómo asignar los indicadores de inteligencia de amenazas:

- Ha encontrado un proceso que sabe que está asociado a Cobalt Strike. Lo has aprendido en FireEye su blog.

  Establece `Type` en `PROCESS`. Cree también un objeto `Process` para el proceso.

- Su filtro de correo detectó que alguien estaba enviando un paquete con hash reconocido desde un dominio malicioso conocido.

  Cree dos objetos `ThreatIntelIndicator`. Un objeto es para `DOMAIN`. El otro es para `HASH_SHA1`.
- Has encontrado un malware con una regla de Yara (Loki, Fenrir, VirusScan Awss3,). BinaryAlert

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

Resources

Para `Resources`, utilice los tipos de recursos y los campos de detalles que proporcionamos siempre que sea posible. Security Hub CSPM agrega constantemente nuevos recursos al ASFF. `<Para recibir un registro mensual de los cambios en el ASFF, póngase en contacto`

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

Para un recurso que no esté modelado en ASFF, establezca `Type` en `Other`. Para obtener información detallada, consulte `Details.Other`.

También puede utilizar el tipo de `Other` recurso para los casos en los que no se encuentre información.AWS

ProductFields

Use `ProductFields` solo si no puede usar otro campo mantenido para `Resources` o un objeto descriptivo como `ThreatIntelIndicators`, `Network` o `Malware`.

Si usa `ProductFields`, debe proporcionar una justificación estricta de esta decisión.

Conformidad

Use `Compliance` solo si sus resultados están relacionados con la conformidad.

Security Hub CSPM utiliza `Compliance` para los hallazgos que genera en función de los controles.

Firewall Manager usa `Compliance` para sus resultados porque están relacionados con la conformidad.

Campos que están restringidos

Estos campos están pensados para que los clientes realicen un seguimiento de su investigación de un resultado.

No asigne nada a estos campos u objetos.

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

Para estos campos, haga la asignación a los campos que están en el objeto `FindingProviderFields`. No los asigne a los campos de nivel superior.

- `Confidence`: incluya una puntuación de confianza (0-99) únicamente si su servicio tiene una funcionalidad similar o si confirma al 100 % su resultado.
- `Criticality`: la puntuación de importancia crítica (0-99) se usa para expresar la importancia del recurso asociado al resultado.
- `RelatedFindings`: proporcione los resultados relacionados únicamente si puede llevar un seguimiento de los resultados relacionados con el mismo recurso o tipo de resultado. Para identificar un hallazgo relacionado, debe consultar el identificador de hallazgo de un hallazgo que ya esté en el Security Hub CSPM.

Directrices para el uso de la API de **`BatchImportFindings`**

Cuando utilice la operación de `BatchImportFindings`API para enviar los resultados AWS Security Hub CSPM, siga las siguientes pautas.

- Debe llamar a `BatchImportFindings` a través de la cuenta asociada a los resultados. El identificador de la cuenta asociada es el valor del atributo `AwsAccountId` del resultado.
- Envíe el lote más grande que pueda. Security Hub CSPM acepta hasta 100 hallazgos por lote, hasta 240 KB por hallazgo y hasta 6 MB por lote.
- El límite de la tasa de limitación es de 10 TPS por cuenta y región, con una ráfaga de 30 TPS.
- Debe implementar un mecanismo para mantener el estado de los resultados en caso de que existan problemas de limitación o de red. También necesita el estado de los resultados para

poder enviar actualizaciones de resultados a medida que un resultado cumpla y deje de cumplir la normativa.

- Para obtener información sobre las longitudes de cadena máximas y otras limitaciones, consulte Formato de resultados de seguridad de AWS (ASFF) en la Guía del usuario de AWS Security Hub .

Lista de verificación de disponibilidad del producto

Los equipos de socios de APN AWS Security Hub CSPM y los de los socios de APN utilizan esta lista de verificación para validar que la integración esté lista para su lanzamiento.

Asignación de ASFF

Estas preguntas están relacionadas con la asignación de su hallazgo al formato de búsqueda de AWS seguridad (ASFF).

¿Todos los datos de resultados del socio están asignados al ASFF?

Asigne todos sus resultados al ASFF de alguna manera.

Utilice campos mantenidos, como los tipos de recursos modelados, `Network`, `Malware` o `ThreatIntelIndicators`.

Asigne todo lo demás a `Resource.Details.Other` o `ProductFields` según corresponda.

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

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

Asigne otra información relacionada con los recursos a `Resource.Details.Other` únicamente cuando no haya una coincidencia directa.

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

No utilice `UserDefinedFields`.

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

¿El socio asigna información a **`ProductFields`** que podría asignarse en otros campos de ASFF?

Use `ProductFields` únicamente para la información específica del producto, como información sobre el control de versiones, resultados de gravedad específicos del producto u otra información que no se pueda asignar a un campo mantenido o `Resources.Details.Other`.

¿El socio importa sus propias marcas temporales para **`FirstObservedAt`**?

La marca temporal `FirstObservedAt` se utiliza para registrar el momento en que se observó un resultado en el producto. Si es posible, asigne este campo.

¿El socio proporciona valores únicos generados para cada identificador de resultado, excepto para los resultados que desea actualizar?

Todos los resultados del CSPM de Security Hub se indexan en el identificador de búsqueda (atributo)`Id`. Este valor debe ser siempre único para garantizar que los resultados no se actualicen por accidente.

También debe mantener el estado del identificador de resultado para actualizar los resultados.

¿El socio proporciona un valor que asigna los resultados a un identificador de generador?

`GeneratorID` no debe tener el mismo valor que el identificador del resultado.

`GeneratorID` debe poder vincular lógicamente los resultados con lo que los generó.

Puede ser un subcomponente de un producto (producto A: vulnerabilidad o producto A: EDR) o algo por el estilo.

¿Utiliza el socio los espacios de nombres de los tipos de resultados requeridos de una manera que es pertinente para su producto? ¿Utiliza el socio las categorías de tipos de resultados o los clasificadores recomendados en sus tipos de resultados?

La taxonomía del tipo de resultados debe ajustarse estrechamente a los resultados que genera el producto.

Se requieren los espacios de nombres de primer nivel descritos en el AWS formato de búsqueda de seguridad.

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

¿El socio capta la información del flujo de red en los campos **`Network`**, si tiene datos de red?

Si su producto captura NetFlow información, asígnela al campo. `Network`

¿El socio capta la información del proceso (PID) en los campos **`Process`**, si tiene datos de proceso?

Si su producto capta información de proceso, asígnela al campo `Process`.

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

Si su producto capta información de malware, asígnela al campo `Malware`.

¿El socio capta información de inteligencia sobre amenazas en el campo **`ThreatIntelIndicators`**, si tiene datos de inteligencia sobre amenazas?

Si su producto capta información de inteligencia sobre amenazas, asígnela al campo `ThreatIntelIndicators`.

¿El socio proporciona una calificación de confianza para los resultados? Si lo hace, ¿se proporciona una justificación?

Siempre que use este campo, proporcione una justificación en la documentación y el manifiesto.

¿Utiliza el socio un identificador canónico o un ARN como identificador del recurso en el resultado?

Al identificar AWS los recursos, la mejor práctica es utilizar el ARN. Si no hay un ARN disponible, use el ID de recurso canónico.

Configuración y funcionamiento de la integración

Estas preguntas están relacionadas con la configuración y el day-to-day funcionamiento de la integración.

¿El socio proporciona una plantilla infrastructure-as-code (IaC) para implementar la integración con Security Hub CSPM, como Terraform, o? CloudFormation AWS Cloud Development Kit (AWS CDK)

En el caso de las integraciones que envíen los resultados desde la cuenta del cliente o utilicen CloudWatch Events para consumir los resultados, se requiere algún tipo de plantilla de IaC.

CloudFormation se prefiere, pero también AWS CDK se puede utilizar Terraform.

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

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

¿El socio solo envía los resultados de valor?

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

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

¿Proporcionó el socio una estimación de la cantidad de datos que enviaría al día por cliente y con qué frecuencia (media y ráfaga)?

Se utilizan números de hallazgos únicos para calcular la carga en el Security Hub CSPM. Un resultado único se define como un resultado con una asignación a ASFF diferente a la de otro resultado.

Por ejemplo, si un resultado solo rellena `ThreatIntelIndicators` y otro solo rellena `Resources.Details.AWSEc2Instance`, son dos resultados únicos.

¿Tiene el socio una forma correcta de gestionar los errores 4xx y 5xx de tal manera que no tengan limitaciones y puedan enviarse todos los resultados en otro momento?

Actualmente, la API de `BatchImportFindings` tiene una velocidad de ráfaga de 30 a 50 TPS. Si se devuelven errores 4xx o 5xx, debe conservar el estado de esos resultados fallidos para poder volver a intentarlos en su totalidad más adelante. Puede hacerlo a través de una cola de cartas muertas u otros servicios de AWS mensajería, como Amazon SNS o Amazon SQS.

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

Si planea actualizar los resultados sobrescribiendo el identificador de resultados original, debe disponer de un mecanismo para conservar el estado, de modo que se actualice la información correcta del resultado correcto.

Si proporciona resultados, no utilice la operación `BatchUpdateFindings` para actualizarlos. Esta operación solo debe ser utilizada por los clientes. Solo se utiliza `BatchUpdateFindings` cuando se investigan los resultados y se toman medidas al respecto.

¿El socio gestiona los reintentos de una forma en que no comprometen los resultados satisfactorios enviados anteriormente?

Debería disponer de un mecanismo para conservar la conclusión original IDs en caso de errores, a fin de no duplicar ni sobrescribir las conclusiones correctas por error.

¿El socio actualiza los resultados llamando a la operación **`BatchImportFindings`** con el identificador de resultado de los resultados existentes?

Para actualizar un resultado debe sobrescribir el resultado existente enviando el mismo ID de resultado.

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

¿El socio actualiza los resultados mediante la API de **`BatchUpdateFindings`**?

Si toma medidas con los resultados, puede usar la operación `BatchUpdateFindings` para actualizar campos concretos.

¿El socio proporciona 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 al Security Hub CSPM?

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

Esta información es obligatoria en el manifiesto.

Si la arquitectura del socio consiste en enviar las conclusiones a Security Hub CSPM desde una cuenta de cliente, ¿lo han demostrado satisfactoriamente? Si la arquitectura del socio consiste en enviar las conclusiones al Security Hub CSPM desde su propia cuenta, ¿lo ha demostrado satisfactoriamente?

Durante las pruebas, los resultados deben enviarse correctamente desde una cuenta de su propiedad que sea diferente de la cuenta proporcionada para el ARN del producto.

Al enviar un resultado desde la cuenta del propietario del ARN del producto, se pueden omitir determinadas excepciones de error de las operaciones de la API.

¿El socio proporciona una conclusión rápida al Security Hub CSPM?

Para demostrar que su integración funciona correctamente, debe enviar resultados de latidos. Los resultados de latidos se envían cada cinco minutos y utilizan el tipo de resultados `Heartbeat`.

Esto es importante si se envían los resultados desde una cuenta de producto.

¿El socio se integró con la cuenta del equipo de producto CSPM de Security Hub durante las pruebas?

Durante la validación previa a la producción, debe enviar los ejemplos de búsqueda a la cuenta del equipo de producto CSPM de Security Hub. AWS Estos ejemplos demuestran que los resultados se envían y asignan correctamente.

Documentación

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

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

La documentación debe estar alojada en su sitio web como una página web estática, wiki, Read the Docs u otro formato específico.

El alojamiento de la documentación no GitHub cumple con el requisito de un sitio web específico.

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

Puede configurar la integración mediante una plantilla de IaC o una integración de “un solo clic” basada en una consola.

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

El caso de uso que proporcione en el manifiesto también deberá describirse en la documentación

¿La documentación del socio proporciona una justificación de los resultados que envía?

Debe explicar los motivos de los tipos de resultados que envíe.

Por ejemplo, su producto puede producir hallazgos de vulnerabilidades, malware y antivirus, pero solo envía los hallazgos de vulnerabilidades y malware a Security Hub CSPM. En ese caso, debe explicar los motivos por los que no envía los resultados de antivirus.

¿La documentación del socio proporciona una justificación de cómo asigna sus resultados a ASFF?

Debe proporcionar los motivos para asignar los resultados nativos de un producto al ASFF. Los clientes necesitan saber dónde buscar información específica sobre un producto.

¿La documentación del socio proporciona orientación sobre cómo el socio actualiza los resultados, en caso de que los actualice?

Proporcione a los clientes información sobre cómo conserva el estado, garantice la idempotencia y sobrescriba los resultados con información. up-to-date

¿En la documentación del socio se describe la latencia de los resultados?

Minimice la latencia para garantizar que los clientes vean los resultados lo antes posible en Security Hub CSPM.

Esta información es obligatoria en el manifiesto.

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

Proporcione información sobre cómo asignar `Severity.Original` a `Severity.Label`.

Por ejemplo, si su valor de gravedad se califica con letras (A, B, C), debe proporcionar información sobre cómo asignar las letras de calificación a la etiqueta de gravedad.

¿La documentación del socio proporciona una justificación para los índices de confianza?

Si proporciona puntuaciones de confianza, estas puntuaciones deben tener una clasificación.

Si utiliza puntuaciones de confianza rellenadas de forma estática o asignaciones derivadas de inteligencia artificial o machine learning, debe proporcionar un contexto adicional.

¿La documentación del socio indica qué regiones admite y cuáles no?

Anote las regiones que admite o no para que los clientes sepan en qué regiones no deben intentar una integración.

Información de la tarjeta del producto

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

¿El identificador de AWS cuenta proporcionado es válido y contiene 12 dígitos?

Los identificadores de cuenta tienen 12 dígitos. Si un identificador de cuenta tiene 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 del manifiesto no debe tener más de 200 caracteres, incluidos los espacios.

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

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

¿El enlace de compra (si se proporciona) lleva al AWS Marketplace listado del producto?

Si proporcionas un enlace de compra, debe ser para una AWS Marketplace entrada. Security Hub CSPM no acepta enlaces de compra que no estén alojados por. AWS

¿Las categorías de productos describen correctamente el producto?

En el manifiesto puede incluir hasta tres categorías de productos. Deben coincidir con el JSON y no pueden estar personalizadas. No se pueden proporcionar más de tres categorías de productos.

¿Los nombres de la empresa y de los productos son válidos y correctos?

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

Información de marketing

Estas preguntas están relacionadas con el marketing de la integración.

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

La página de socios de CSPM de Security Hub solo acepta un máximo de 700 caracteres, incluidos los espacios.

El equipo recortará las descripciones más largas.

¿El logotipo de la página de socios de CSPM de Security Hub no mide más de 600 x 300 px?

Proporcione una URL de acceso público con el logotipo de la empresa en PNG o JPG que no tenga más de 600 x 300 píxeles.

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

El enlace Más información no debe llevar al sitio web principal del socio ni a la información de la documentación.

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

¿El socio ofrece una demostración o un vídeo instructivo sobre cómo utilizar su integración?

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

¿Se publica una entrada de blog de AWS Partner Network con el socio y su gerente de desarrollo de socios o representante de desarrollo de socios?

AWS Las publicaciones del blog de Partner Network deben coordinarse previamente con el gerente de desarrollo de socios o el representante de desarrollo de socios.

Estos son independientes de cualquier publicación del blog que cree usted mismo.

Espere un tiempo de 4 a 6 semanas. Este esfuerzo debe iniciarse una vez finalizadas las pruebas con el ARN del producto privado.

¿Se publicará un comunicado de prensa dirigido por los socios?

Puede trabajar con el administrador de desarrollo de socios o el representante de desarrollo de socios para obtener un presupuesto del vicepresidente de servicios de seguridad externos. Puede utilizar este presupuesto en su comunicado de prensa.

¿Se publicará una entrada de blog dirigida por los socios?

Puede crear sus propias publicaciones de blog para mostrar la integración fuera del blog de la Red de socios de AWS .

¿Se publicará una seminario web dirigido por los socios?

Puede crear sus propios seminarios web para mostrar la integración.

Si necesita la ayuda del equipo de CSPM de Security Hub, trabaje con el equipo del producto después de completar las pruebas con el ARN del producto privado.

¿El socio solicitó asistencia en las redes sociales? AWS

Tras su liberación, puede trabajar con el responsable de marketing AWS de Seguridad para utilizar los canales AWS oficiales de las redes sociales y compartir información sobre sus seminarios web.

AWS Security Hub CSPMPreguntas frecuentes sobre socios

Las preguntas siguientes se formulan con frecuencia sobre la configuración y el mantenimiento de una integración con AWS Security Hub CSPM.

1. ¿Cuáles son las ventajas de la integración de Security Hub CSPM?
   - Satisfacción del cliente: la razón principal para integrarse con Security Hub CSPM es porque los clientes lo solicitan.

     Security Hub CSPM es el centro de seguridad y cumplimiento para AWS los clientes. Está diseñado como el primer lugar al que acuden los profesionales AWS de seguridad y cumplimiento todos los días para comprender su estado de seguridad y cumplimiento.

     Escuche a sus clientes. Ellos le dirán si quieren ver sus resultados en Security Hub.
   - Oportunidades de descubrimiento: promocionamos socios con integraciones certificadas dentro de la consola CSPM de Security Hub, incluidos enlaces a sus listados. AWS Marketplace Esto ofrece una forma estupenda para que los clientes descubran los nuevos productos de seguridad.
   - Oportunidades de marketing: los proveedores con integraciones aprobadas pueden participar en seminarios web, publicar comunicados de prensa, crear hojas informativas y mostrar sus integraciones a los clientes. AWS
2. ¿Qué tipos de socios existen?
   - Socios que envían las conclusiones a Security Hub (CSPM)
   - Socio que recibe las conclusiones de Security Hub (CSPM)
   - Socios que envían y reciben resultados
   - Socios consultores que ayudan a los clientes a configurar, personalizar y utilizar Security Hub (CSPM) en su entorno
3. ¿Cómo funciona a un alto nivel la integración de un socio con Security Hub CSPM?

   Usted recopila las conclusiones de una cuenta de cliente o de su propia AWS cuenta y transforma el formato de las conclusiones al formato de búsqueda de AWS seguridad (ASFF). A continuación, envía esos hallazgos al punto final regional CSPM de Security Hub correspondiente.

   También puede usar CloudWatch Events para recibir las conclusiones de Security Hub CSPM.
4. ¿Cuáles son los pasos básicos para completar una integración con Security Hub CSPM?

a. Envíe la información del manifiesto de socios.

b. Reciba el producto ARNs para usarlo con Security Hub CSPM, si va a enviar los resultados a Security Hub.

c. Asigne sus resultados al ASFF. Consulte the section called “Directrices para la asignación de ASFF”.

d. Defina su arquitectura para enviar y recibir las conclusiones de Security Hub (CSPM). Siga los principios descritos en the section called “Fundamentos para crear y actualizar los resultados”.

e. Cree un marco de implementación para los clientes. Por ejemplo, los CloudFormation scripts pueden servir para este propósito.

f. Documente su configuración y facilite instrucciones de configuración a los clientes.

g. Defina toda la información personalizada (reglas de correlación) que los clientes puedan usar con su producto.

h. Demuestre su integración al equipo de CSPM de Security Hub.

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

5. ¿Qué procedimiento se sigue para enviar el manifiesto de socios? ¿Y para que AWS los servicios envíen las conclusiones al Security Hub CSPM?

   `<Para enviar la información del manifiesto al equipo de CSPM de Security Hub,`

   Se le entregará el producto ARNs en un plazo de siete días naturales.

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

   Los precios del CSPM de Security Hub se basan en parte en la cantidad de hallazgos ingeridos. Por ello, debe abstenerse de enviar resultados que no aporten valor a los clientes.

   Por ejemplo, algunos proveedores de administración de vulnerabilidades solo envían los resultados que tienen una puntuación del Common Vulnerability Scoring System (CVSS) mayor o igual que 3 sobre un total de 10 puntos posibles.

7. ¿Cuáles son los diferentes enfoques para enviar mis conclusiones a Security Hub CSPM?

   Estos son los enfoques principales:

   - Los resultados se envían desde su propia AWS cuenta designada mediante la `BatchImportFindings`operación.

- Los resultados se envían desde la cuenta del cliente mediante la operación `BatchImportFindings`. Puede utilizar enfoques basados en la asunción de roles, aunque dichos enfoques no son obligatorios.

Para conocer las directrices generales sobre el uso de `BatchImportFindings`, consulte the section called “Directrices para el uso de la API de `BatchImportFindings`”.

8. ¿Cómo recopilo mis hallazgos y los envío a un punto final regional de Security Hub CSPM?

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

   Por ejemplo, algunos socios crean una aplicación de Python que se puede implementar como un CloudFormation script. El script recopila los hallazgos del socio del entorno del cliente, los transforma en ASFF y los envía al punto final regional CSPM de Security Hub.

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

9. ¿Cómo sé cuándo debo empezar a enviar las conclusiones a Security Hub CSPM?

   Security Hub CSPM admite la autorización parcial por lotes para el funcionamiento de la `BatchImportFindings`API, de modo que puede enviar todos sus hallazgos a Security Hub CSPM para todos sus clientes.

   Si algunos de sus clientes aún no se han suscrito a Security Hub CSPM, Security Hub CSPM no ingiere esos hallazgos. Solamente incorpora los resultados autorizados que están en el lote.

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

    a. Asegúrese de que se implementen las políticas de IAM correctas.
    b. Habilite una suscripción de producto (políticas de recursos) para las cuentas. Utilice la operación desde la API de `EnableImportFindingsForProduct` o la página de integraciones. Esto puede hacerlo el cliente o bien puede usar roles entre cuentas para actuar en nombre del cliente.
    c. Asegúrese de que el `ProductArn` del resultado sea el ARN público de su producto.
    d. Asegúrese de que el `AwsAccountId` del resultado sea el ID de la cuenta del cliente.
    e. Asegúrese de que sus hallazgos no contengan datos mal formados de acuerdo con el formato de búsqueda de AWS seguridad (ASFF). Por ejemplo, los campos obligatorios deben estar rellenados y no contener valores no válidos.

f. Envíe los resultados en lotes al punto de conexión regional correcto.

11 ¿De qué permisos de IAM se debe disponer para poder enviar resultados?

Las políticas de IAM deben estar configuradas para el rol o el usuario de IAM que realiza las llamadas a `BatchImportFindings` u otras llamadas a la API.

La prueba más sencilla consiste en hacerlo desde una cuenta de administrador. Puede restringirlas a `action: 'securityhub:BatchImportFindings'` y `resource: <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 con las políticas de IAM por parte del intermediario de `BatchImportFindings`, defina la política de IAM para dicho intermediario de la siguiente manera:

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

Asegúrese de comprobar que no haya políticas de `Deny` para el intermediario. Cuando consiga que de esta manera funcione, 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 a un producto?

Para recibir resultados del producto de un socio concreto, el cliente (o el socio con roles entre cuentas cuando trabaje en nombre del cliente) debe establecer una suscripción al producto. Para hacer esto desde la consola se utiliza la página de integraciones. Para hacerlo desde la API, se usa la operación de la API de `EnableImportFindingsForProduct`.

La suscripción al producto crea una política de recursos que autoriza al cliente a recibir o enviar los resultados del socio. Para obtener más información, consulte Casos de uso y permisos.

Security Hub CSPM tiene los siguientes tipos de políticas de recursos para los 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 puede enviar los resultados a Security Hub CSPM desde la cuenta que aparece en el ARN de su producto.

Con `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, solo puede enviar los resultados desde la cuenta de cliente que se ha suscrito a su producto.

13. Supongamos que un cliente ha creado una cuenta de administrador a la que agregó algunas cuentas de miembros. ¿Es necesario que el cliente suscriba cada cuenta de miembro a mi producto? ¿O el cliente solo se suscribe desde la cuenta de administrador y luego yo puedo enviar los resultados a los recursos de todas las cuentas de los miembros?

    Lo que se pregunta aquí es si los permisos se crean para todas las cuentas de los miembros en función del registro de la cuenta de administrador.

    El cliente debe crear una suscripción al producto para cada cuenta. Esto puede hacerse 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 CSPM genera para usted y que utiliza para enviar las conclusiones. Recibirá un ARN de producto por cada producto que integre con Security Hub CSPM. El ARN del producto correcto debe formar parte de cada hallazgo que envíe a Security Hub CSPM. Los resultados que no tienen un ARN de producto se descartan. El ARN del producto tiene 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 CSPM. El ID de cuenta, la empresa y los nombres de producto vienen determinados por los manifiestos enviados por su socio. Nunca deberá cambiar la información asociada al ARN de su producto, excepto el código de región. Dicho código debe coincidir con la región para la que envíe los resultados.

Un error común es cambiar el ID de la cuenta para que coincida con el de la cuenta desde la que trabaja actualmente. El ID de la cuenta no cambia. Debe enviar un identificador de cuenta "de inicio" como parte del envío del manifiesto. Este ID de cuenta está bloqueado en el ARN del producto.

Cuando Security Hub CSPM se lanza en nuevas regiones, utiliza automáticamente los códigos de región estándar para generar el producto ARNs para esas regiones.

Cada cuenta también recibe automáticamente un ARN de producto privado. Puede usar este ARN para hacer pruebas de importación de los resultados en su propia cuenta de desarrollo antes de recibir el ARN del producto oficial público.

15. ¿Qué formato se debe utilizar para enviar las conclusiones al Security Hub CSPM?

Los hallazgos deben proporcionarse en el formato de búsqueda AWS de seguridad (ASFF). Consulte Formato de resultados de seguridad de AWS (ASFF) en la Guía del usuario de AWS Security Hub.

Se espera que toda la información de sus resultados nativos se refleje plenamente en el ASFF. Los campos personalizados, por ejemplo, `ProductFields` y `Resource.Details.Other`, permiten asignar datos que no encajan perfectamente en los campos predefinidos.

16. ¿Cuál es el punto de conexión regional correcto que se debe utilizar?

Debe enviar los resultados al punto final regional CSPM de Security Hub que está asociado a la cuenta del cliente.

17. ¿Dónde se puede encontrar la lista de puntos de conexión regionales?

Consulte la lista de puntos finales CSPM de Security Hub.

18 ¿Se pueden enviar resultados de una región a otra?

Security Hub CSPM aún no admite el envío de resultados entre regiones para los AWS servicios nativos, como Amazon, Amazon GuardDuty Macie y Amazon Inspector. Si su cliente lo permite, Security Hub CSPM no le impide enviar hallazgos desde diferentes regiones.

En este sentido, puede llamar a un punto de conexión regional desde cualquier lugar y la información sobre los recursos del ASFF no tiene por qué coincidir con la región del punto de conexión. Sin embargo, `ProductArn` debe coincidir con la región del punto de conexión.

19 ¿Qué normas y directrices rigen el envío de lotes de resultados?

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

Puede agrupar un conjunto de resultados de diferentes cuentas. Sin embargo, si alguna de las cuentas del lote no está suscrita a Security Hub CSPM, se produce un error en todo el lote. Esto es una limitación del modelo de autorización de referencia de API Gateway.

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

20 ¿Se pueden enviar actualizaciones de los resultados que he creado?

Sí, si envía un resultado con el mismo ARN de producto y el mismo ID de resultado, se sobrescribirán los datos anteriores de ese resultado. Tenga en cuenta que todos los datos se sobrescribirán, por lo que debe enviar un resultado completo.

La tarificación y facturación de los clientes se basa tanto en los nuevos resultados como en sus actualizaciones.

21 ¿Se pueden enviar actualizaciones de los resultados que ha creado otra persona?

Sí, si el cliente le concede acceso a la operación de la API de `BatchUpdateFindings`, puede actualizar ciertos campos mediante esa operación. Esta operación está diseñada para que la utilicen los clientes SIEMs, los sistemas de emisión de tickets y las plataformas de organización, automatización y respuesta de seguridad (SOAR).

22 ¿Cómo se eliminan los resultados obsoletos?

Security Hub CSPM caduca los resultados 90 días después de la fecha de la última actualización. Transcurrido este tiempo, los hallazgos obsoletos se eliminan del clúster CSPM de Security Hub. OpenSearch

Si actualizas un hallazgo con el mismo ID de hallazgo y ha caducado, se crea un nuevo hallazgo en Security Hub CSPM.

Los clientes pueden usar CloudWatch Events para sacar las conclusiones del Security Hub CSPM. De este modo se pueden enviar todos los resultados a los destinos que elija el cliente.

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

23 ¿Qué aceleradores instala Security Hub CSPM?

Security Hub CSPM limita las llamadas a las `GetFindings` API, ya que el enfoque recomendado para acceder a los hallazgos es utilizar eventos. CloudWatch

Security Hub CSPM no implementa ninguna otra limitación en los servicios internos, los socios o los clientes más allá de la que imponen las invocaciones a API Gateway y Lambda.

24 ¿Cuál es la puntualidad, la latencia SLAs o las expectativas de los hallazgos que se envían a Security Hub CSPM desde los servicios de origen?

El objetivo es que tanto los resultados iniciales como sus actualizaciones se publiquen lo más cerca posible al tiempo real. Debe enviar los resultados a Security Hub CSPM en un plazo de cinco minutos después de su creación.

25 ¿Cómo puedo recibir las conclusiones de Security Hub CSPM?

Para recibir resultados, utilice alguno de los métodos siguientes.

- Todos los hallazgos se envían automáticamente a CloudWatch Events. Un cliente puede crear reglas de CloudWatch eventos específicas para enviar los hallazgos a objetivos específicos, como un SIEM o un bucket de S3. Esta capacidad sustituyó a la antigua operación de la API de `GetFindings`.
- Usa CloudWatch Events para realizar acciones personalizadas. Security Hub CSPM permite a los clientes seleccionar hallazgos específicos o grupos de hallazgos desde la consola y tomar medidas al respecto. Por ejemplo, se pueden enviar los resultados a un SIEM, un sistema de ticketing, 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 en Security Hub CSPM. Estas acciones se denominan acciones personalizadas.

Cuando un usuario selecciona una acción personalizada, se crea un CloudWatch evento para esos hallazgos específicos. Puedes aprovechar esta capacidad y crear reglas y objetivos de CloudWatch eventos para que un cliente los 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 a CloudWatch Events. Corresponde al usuario tomar medidas en relación con resultados concretos.

Puedes usar las operaciones de la API de acciones personalizadas, por ejemplo`CreateActionTarget`, para crear automáticamente las acciones disponibles para tu producto (por ejemplo, mediante CloudFormation plantillas). También CloudWatch utilizaría las operaciones de la API de reglas de CloudWatch eventos para crear las reglas de eventos correspondientes asociadas a la acción personalizada. Mediante CloudFormation plantillas, también puede crear reglas de CloudWatch eventos para incorporar automáticamente desde Security Hub CSPM todos los hallazgos o todos los hallazgos con determinadas características.

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

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

Debe disponer de documentación de usuario que explique su uso del Security Hub CSPM.

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

Si el MSSP solo recibe las conclusiones del Security Hub CSPM, debe tener como mínimo una CloudFormation plantilla para configurar las reglas de eventos adecuadas. CloudWatch

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

Si es socio consultor de APN, puede convertirse en socio de CSPM de Security Hub. Debe enviar dos casos prácticos privados que evidencien cómo ayudó a un cliente concreto a hacer lo siguiente.

- Configure Security Hub CSPM con los permisos de IAM que necesite el cliente.

- Ayude a conectar las soluciones de proveedores de software independientes (ISV) ya integradas al Security Hub CSPM mediante las instrucciones de configuración de la página de socios de la consola.
- Ayudar a los clientes con integraciones de productos personalizadas.
- Crear información personalizada pertinente a las necesidades y los conjuntos de datos de los clientes.
- Crear acciones personalizadas.
- Crear manuales de corrección.
- Cree guías de inicio rápido que se ajusten a los estándares de cumplimiento CSPM de Security Hub. Estos deben ser validados por el equipo de CSPM de Security Hub.

No es necesario compartir públicamente los nombres de los casos prácticos.

28 ¿Cuáles son los requisitos en torno a la forma en que implemento mi integración con Security Hub CSPM con mis clientes?

Las arquitecturas de integración entre Security Hub CSPM y los productos de los socios varían de un socio a otro en cuanto al funcionamiento de la solución de cada socio. Debe asegurarse de que el proceso de configuración de la integración no dure más de 15 minutos.

Si va a implementar un software de integración en el AWS entorno del cliente, debería aprovechar las CloudFormation plantillas para simplificar la integración. Algunos socios han creado integraciones con un solo clic, algo que se recomienda encarecidamente.

29 ¿Qué requisitos debe cumplir la documentación?

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

Esta documentación también debe incluir información sobre su utilización de ASFF. En concreto, debe enumerar los tipos de resultados de ASFF que está utilizando para sus diferentes resultados. Si utiliza definiciones de información predeterminadas, le recomendamos que también las incluya aquí.

Considere la posibilidad de incluir otra posible información:

- Su caso de uso para la integración con Security Hub (CSPM)
- El volumen medio de resultados enviados

- Su arquitectura de integración
- Las regiones que son compatibles y las que no
- La latencia entre el momento en que se crean los resultados y el momento en que estos se envían a Security Hub
- Si los resultados se actualizan

30 ¿Qué son los conocimientos personalizados?

Le recomendamos que defina los conocimientos personalizados para sus resultados. Los conocimientos son reglas de correlación sencillas que ayudan al cliente a priorizar qué resultados y recursos requieren más atención y medidas.

Security Hub CSPM tiene una operación de `CreateInsight` API. Puedes crear información personalizada dentro de una cuenta de cliente como parte de tu CloudFormation plantilla. Esta información aparece en la consola del cliente.

31 ¿Se pueden enviar widgets de paneles?

De momento no. Solo se pueden crear conocimientos personalizados.

32 Qué modelo de precios se aplica?

Consulte la información de precios de CSPM de Security Hub.

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

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

No nos envíe ningún dato confidencial ni información de identificación personal. Estos datos se utilizan para demostraciones públicas. Al enviarnos estos datos, nos autoriza a utilizarlos en las demostraciones.

34 ¿Qué mensajes de error o de éxito proporciona **`BatchImportFindings`**?

Security Hub CSPM proporciona una respuesta para la autorización y una respuesta para. `BatchImportFindings` Se están desarrollando mensajes de éxito, fallo y error más claros.

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

Los servicios de origen son responsables de todo el control de errores. Se encargan de gestionar los mensajes de error, los reintentos, las limitaciones y las alarmas. También deben gestionar los comentarios o los mensajes de error enviados a través del mecanismo de comentarios CSPM de Security Hub.

36 ¿Puede citar algunas de las soluciones a los problemas más comunes?

Una `AuthorizerConfigurationException` es el resultado de un `AwsAccountId` o `ProductArn` incorrecto.

Durante la resolución de problemas, tenga en cuenta lo siguiente:

- `AwsAccountId` debe tener exactamente 12 dígitos.
- `ProductArn`debe tener el siguiente formato: arn:aws:securityhub: ::product//*<us-west-2 or us-east-1><accountId><company-id><product-id>*

  El ID de cuenta no cambia con respecto al que el equipo de CSPM de Security Hub incluyó en el producto ARNs que le proporcionaron.

`AccessDeniedException` se produce cuando un resultado se envía a una cuenta equivocada o desde ella, o cuando la cuenta no tiene una `ProductSubscription`. El mensaje de error contendrá un ARN con un tipo de recurso `product` o `product-subscription`. Este error solo se produce durante las llamadas entre cuentas. Si llama a `BatchImportFindings` con su propia cuenta para la misma cuenta en `AwsAccountId` y `ProductArn`, la operación utiliza las 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 realmente registradas. Algunos socios han utilizado un número de cuenta para el producto del ARN del producto, pero intentan usar una cuenta completamente diferente para llamar a `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 los resultados.

37 ¿Dónde se envían las preguntas, los comentarios y los errores?

`<securityhub-partners@amazon.com>`

38 ¿A qué región se envían los resultados de los elementos relacionados con los servicios globales de AWS? Por ejemplo, ¿dónde debo enviar los resultados relacionados con la IAM?

Envíe los resultados a la misma región en la que se detectaron los resultados. En el caso de un servicio como IAM, es probable que la solución detecte el mismo problema de IAM en varias regiones. En ese caso, el resultado se envía a todas las regiones en las que se detectó el problema.

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

Cuando resuelva un problema, envíe la actualización del resultado a todas las regiones a las que envió el resultado original.

Historial de revisiones de la Guía de integración de socios

En la tabla siguiente se explican las actualizaciones realizadas en la documentación de esta guía.

Cambio	Descripción	Fecha
Requisitos actualizados para el logotipo de la consola	Se actualizaron el manifiesto de socios y las directrices del logotipo 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 CSPM 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	El CSPM de Security Hub ahora también permite a los socios que se han unido a la ruta de socios AWS ISV y que utilizan un producto de integración que ha completado una revisión técnica AWS fundamental (FTR). Anteriormente, todos los socios de integración debían ser socios de nivel selecto. AWS	29 de abril de 2021
Nuevo objeto `FindingProviderFields` en ASFF	Se actualizó la información sobre la asignación de resultados al ASFF. Para `Confidence`, `Criticality`, `RelatedFindings`, `Severity` y `Types`, los socios asignan sus valores a	18 de marzo de 2021

	los campos en `FindingProviderFields` .	
Nuevos fundamentos para crear y actualizar los resultados	Se agregó un nuevo conjunto de pautas para crear nuevos hallazgos y actualizar los hallazgos existentes en Security Hub CSPM.	4 de diciembre de 2020
Versión inicial de esta guía	Esta guía de integración de AWS socios proporciona a los socios información sobre cómo establecer una integración con. AWS Security Hub CSPM	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.