Integración de Cisco Threat Response (CTR) y ESA

Contenido

Introducción

Este documento describe el proceso para integrar Cisco Threat Response (CTR) con Email Security Appliance (ESA) y cómo verificarlo para realizar algunas investigaciones de CTR.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Threat Response
- Aplicación de seguridad de correo electrónico

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Cuenta CTR
- Intercambio de servicios de seguridad de Cisco
- ESA C100V en la versión de software 13.0.0-392

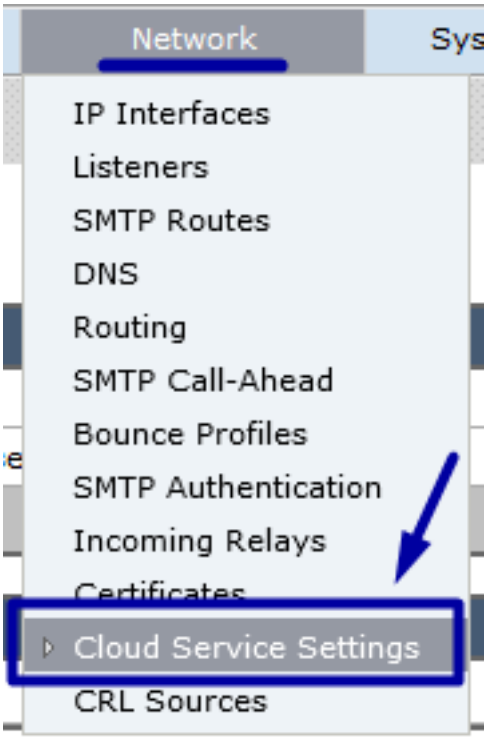
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Para configurar el CTR de integración y el ESA, inicie sesión en su dispositivo virtual de seguridad de correo electrónico y siga estos pasos rápidos:

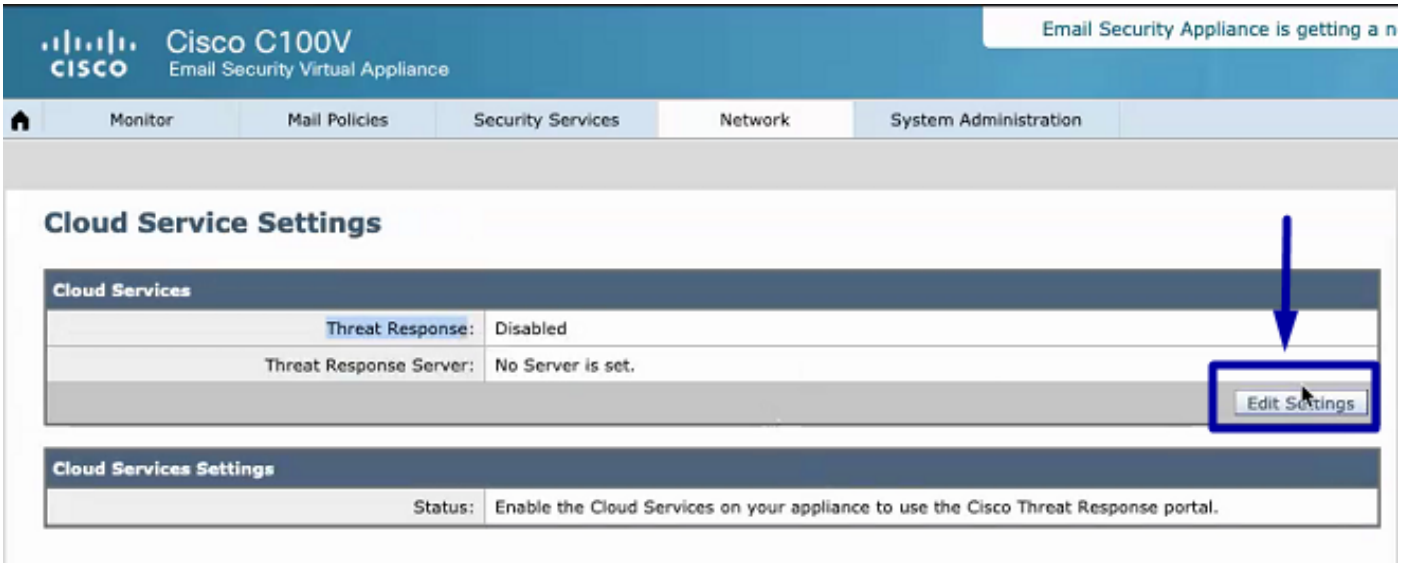
Paso 1. Vaya a Red > Configuración de servicios en la nube

Una vez en el ESA, navegue hasta el menú contextual Network > Cloud Service Settings, para ver el estado de respuesta de amenaza actual (Desactivado / Activado) como se muestra en la imagen.



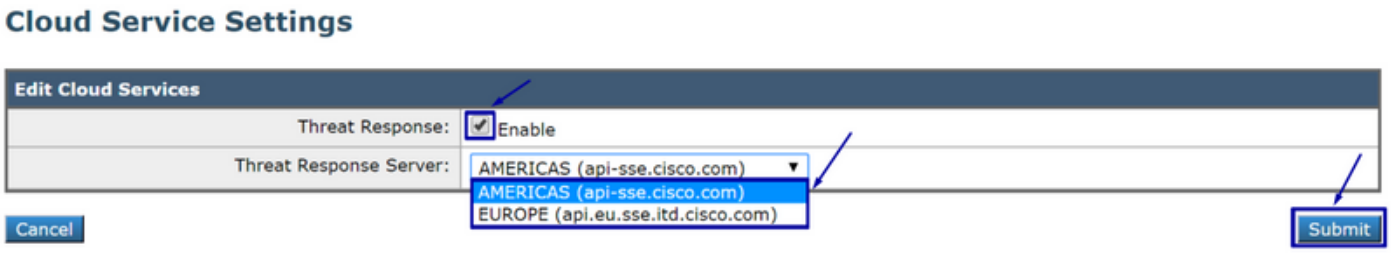
Paso 2. Haga clic en Edit Settings (Editar parámetros)

Hasta ahora, la función Threat Response en el ESA está desactivada, para habilitar la función, haga clic en Edit Settings (Editar configuración), como se muestra en la imagen:



Paso 3. Active la casilla de verificación Enable (Activar) y Threat Response Server (Servidor de respuesta a amenazas).

Active la casilla de verificación Enable (Activar) y, a continuación, seleccione Threat Response Server (Servidor de respuesta ante amenazas). Consulte la imagen siguiente:

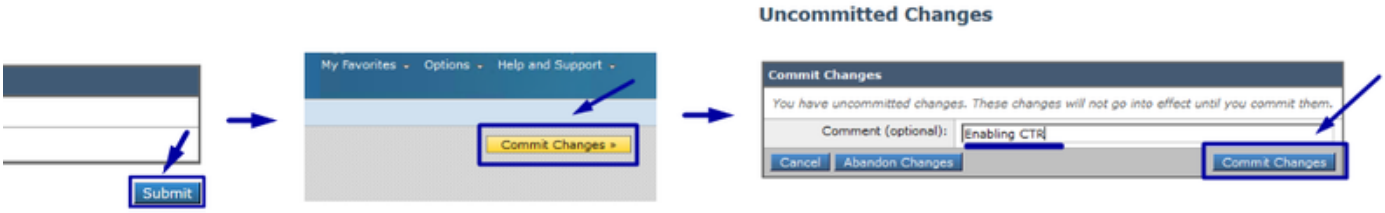


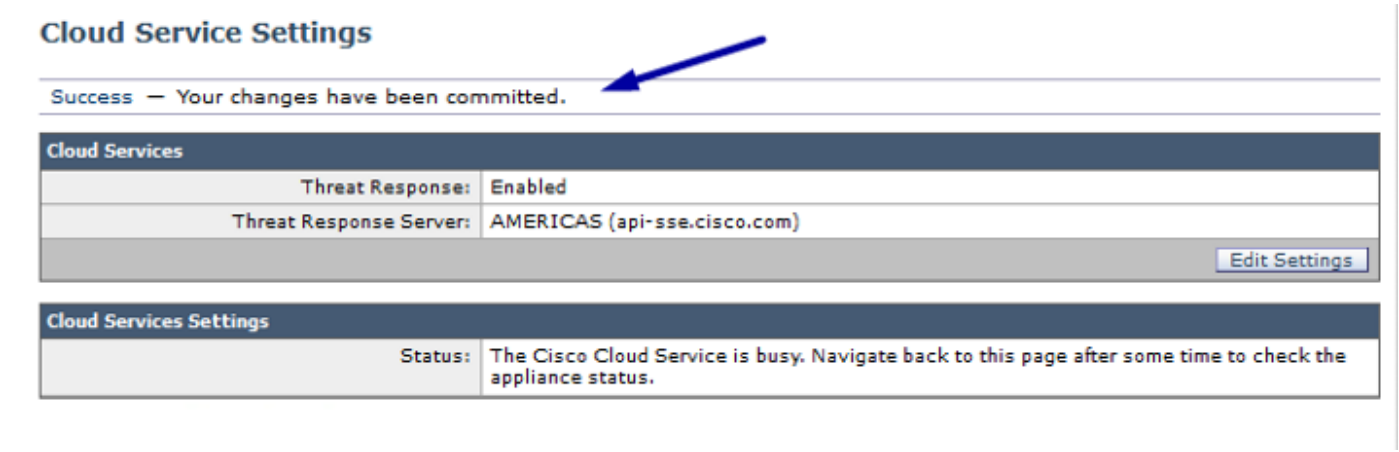
Nota: La selección predeterminada para la URL de Threat Response Server es AMERICAS (api-sse.cisco.com). Para las empresas de EUROPA, haga clic en el menú desplegable y seleccione EUROPE (api.eu.sse.itd.cisco.com)

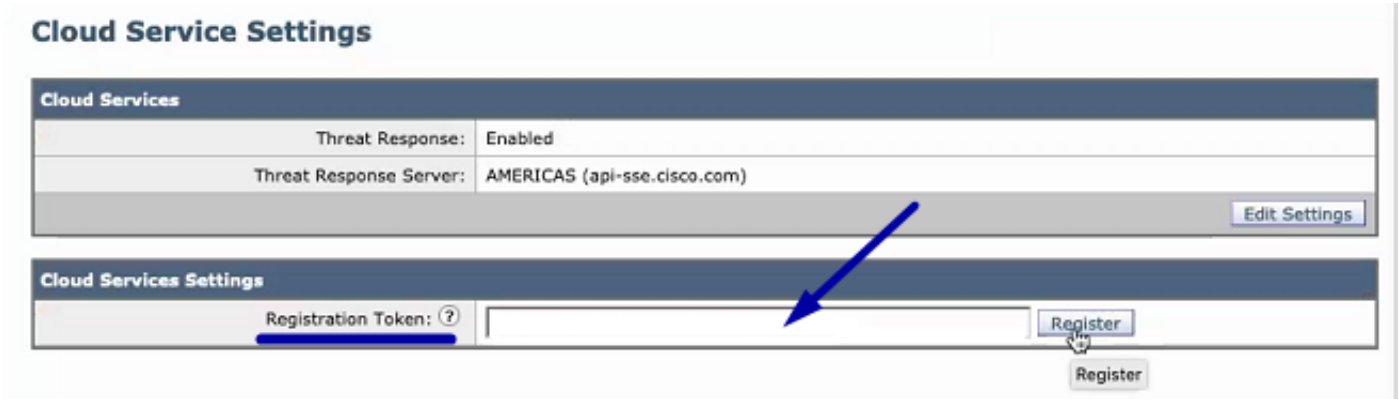
Paso 4. Enviar y registrar cambios

Se requiere enviar y registrar los cambios para guardar y aplicar cualquier cambio. Ahora, si se actualiza la interfaz ESA, se solicita un token de registro para registrar la integración, como se muestra en la siguiente imagen.

Nota: Puede ver un mensaje de éxito: Se han confirmado los cambios.

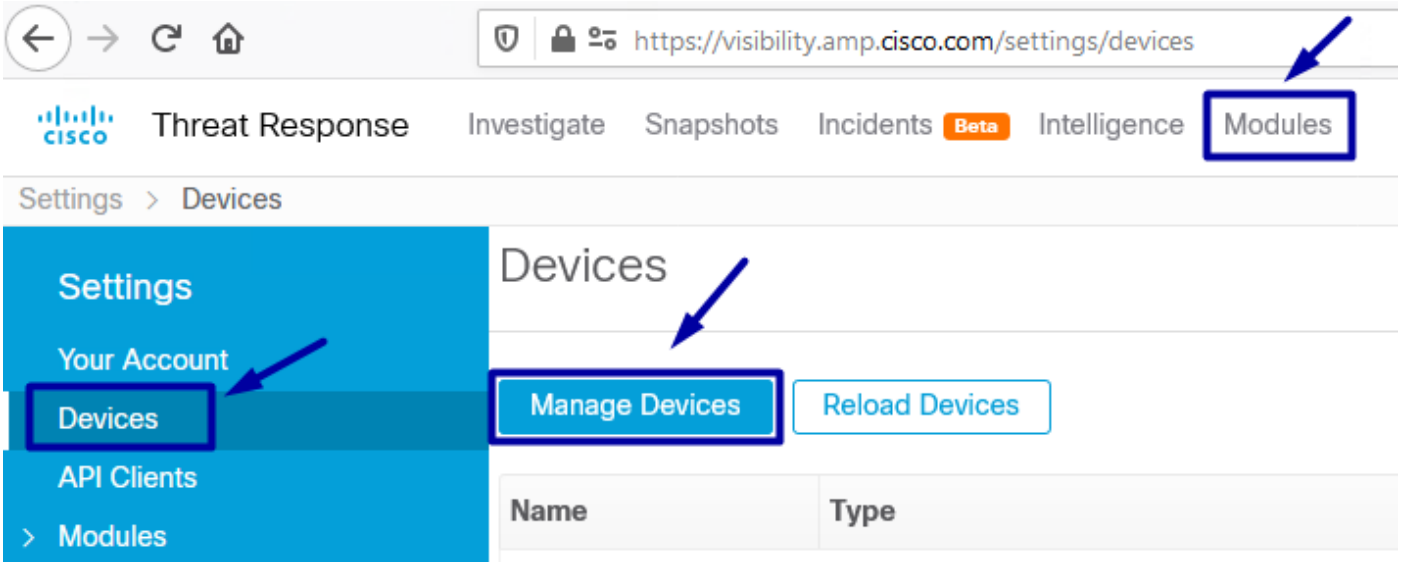




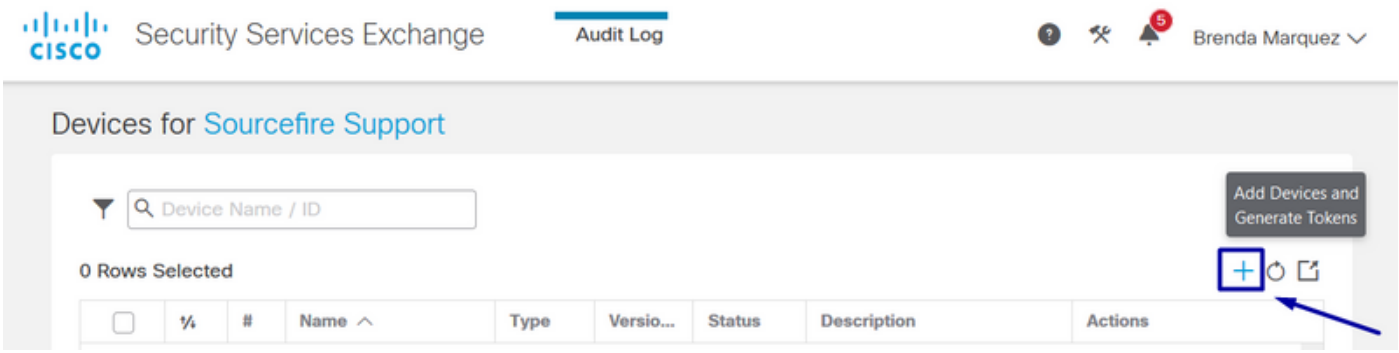


Paso 5. Inicie sesión en el portal CTR y genere el token de registro solicitado en el ESA

1.- Una vez en el portal CTR, navegue hasta Módulos > Dispositivos > Administrar dispositivos, vea la siguiente imagen.

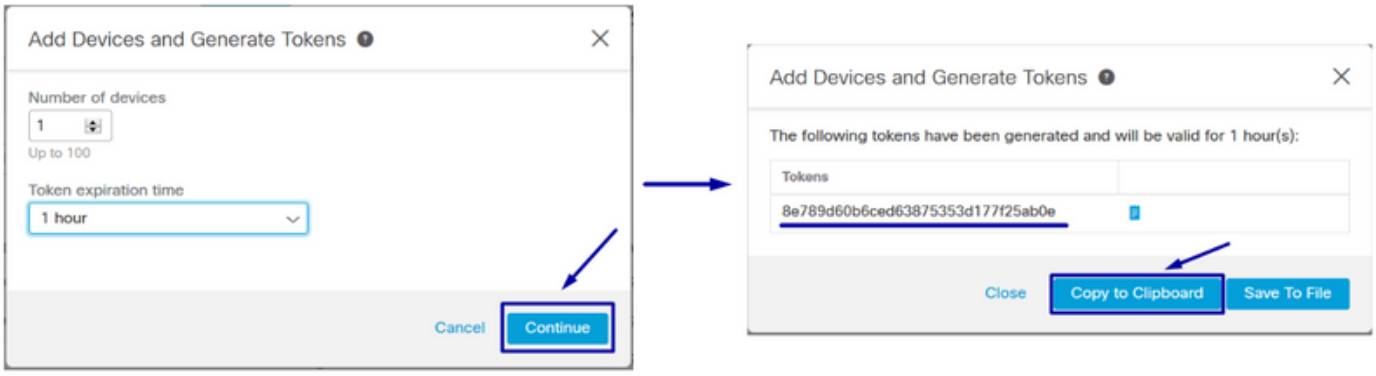


2.- El enlace Administrar dispositivos le redirige al Security Services Exchange (SSE), una vez que esté allí, haga clic en el icono Agregar dispositivos y generar tokens, como se muestra en la imagen.



3.- Haga clic en Continuar para generar el token, una vez que se genere el token, haga clic en Copiar al portapapeles, como se muestra en la imagen.

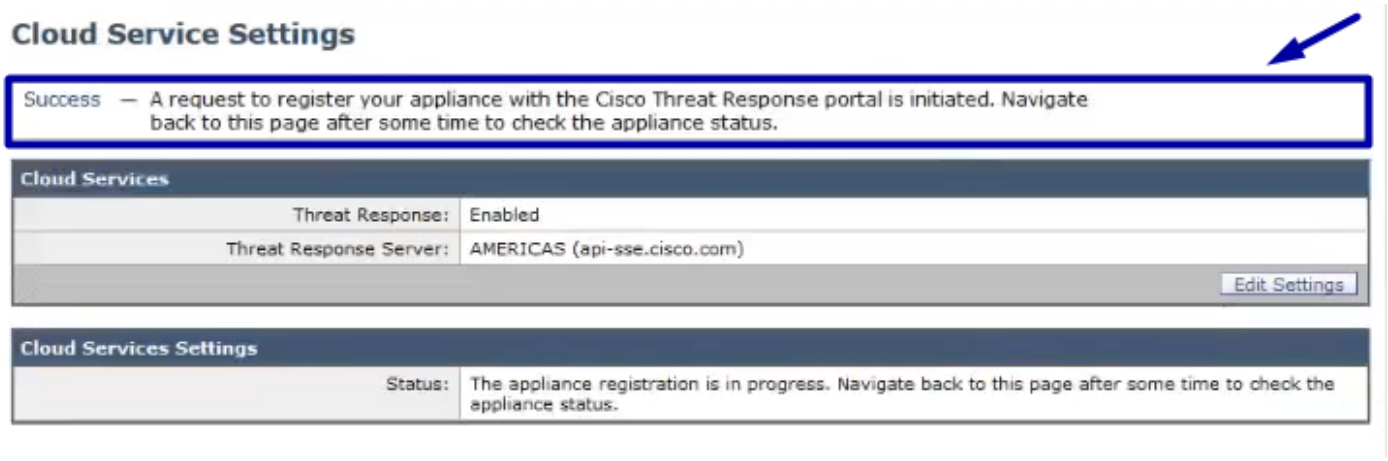
> **Consejo:** Puede seleccionar el número de dispositivos que desea agregar (de 1 a 100) y también la hora de caducidad del token (1h, 2hrs, 4hrs, 6hrs, 8hrs, 12hrs, 01 days, 02 days, 03 days, 04 days y 05 days).



Paso 6. Pegue el token de registro (generado desde el portal CTR) en el ESA

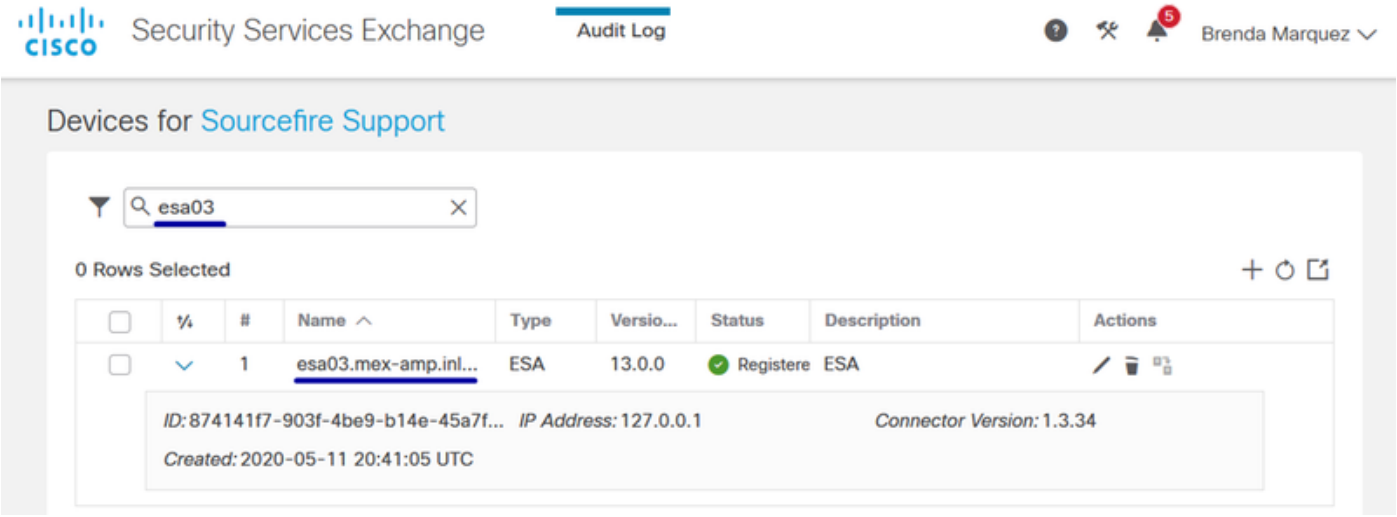
Una vez que se genere el token de registro, péguelo en la sección Cloud Services Settings en el ESA, como se muestra a continuación en la imagen.

> **Nota:** Puede ver un mensaje de éxito: Se inicia una solicitud para registrar su dispositivo en el portal de Cisco Threat Response. Vuelva a esta página después de un tiempo para comprobar el estado del dispositivo.



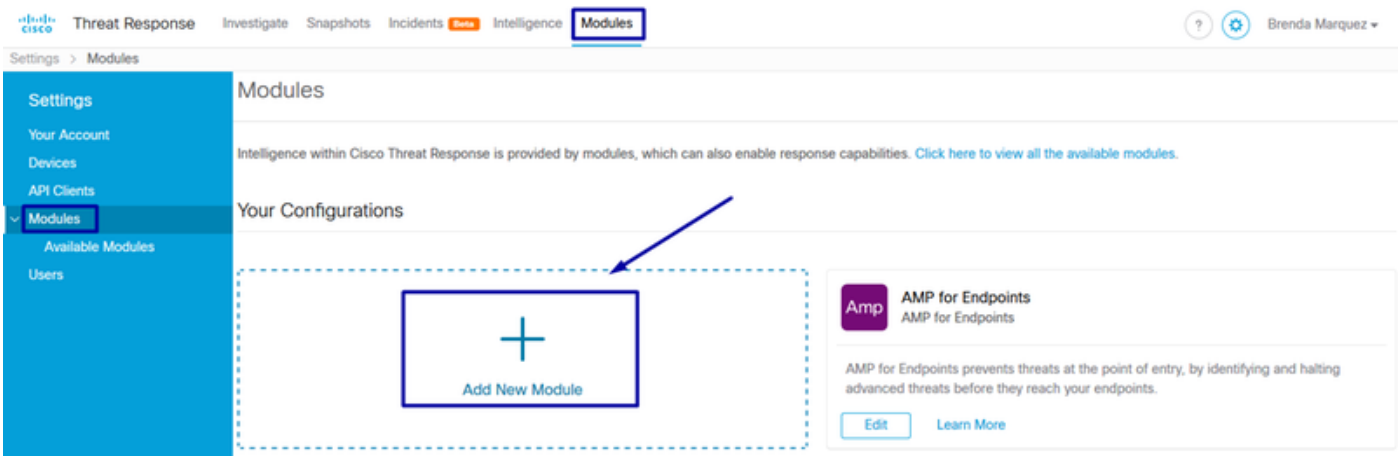
Paso 7. Verifique que su dispositivo ESA esté en el portal SSE

Puede navegar hasta el portal SSE (CTR > Módulos > Dispositivos > Administrar dispositivos), y en la pestaña Buscar (Search) mire su dispositivo ESA, como se muestra en la imagen.

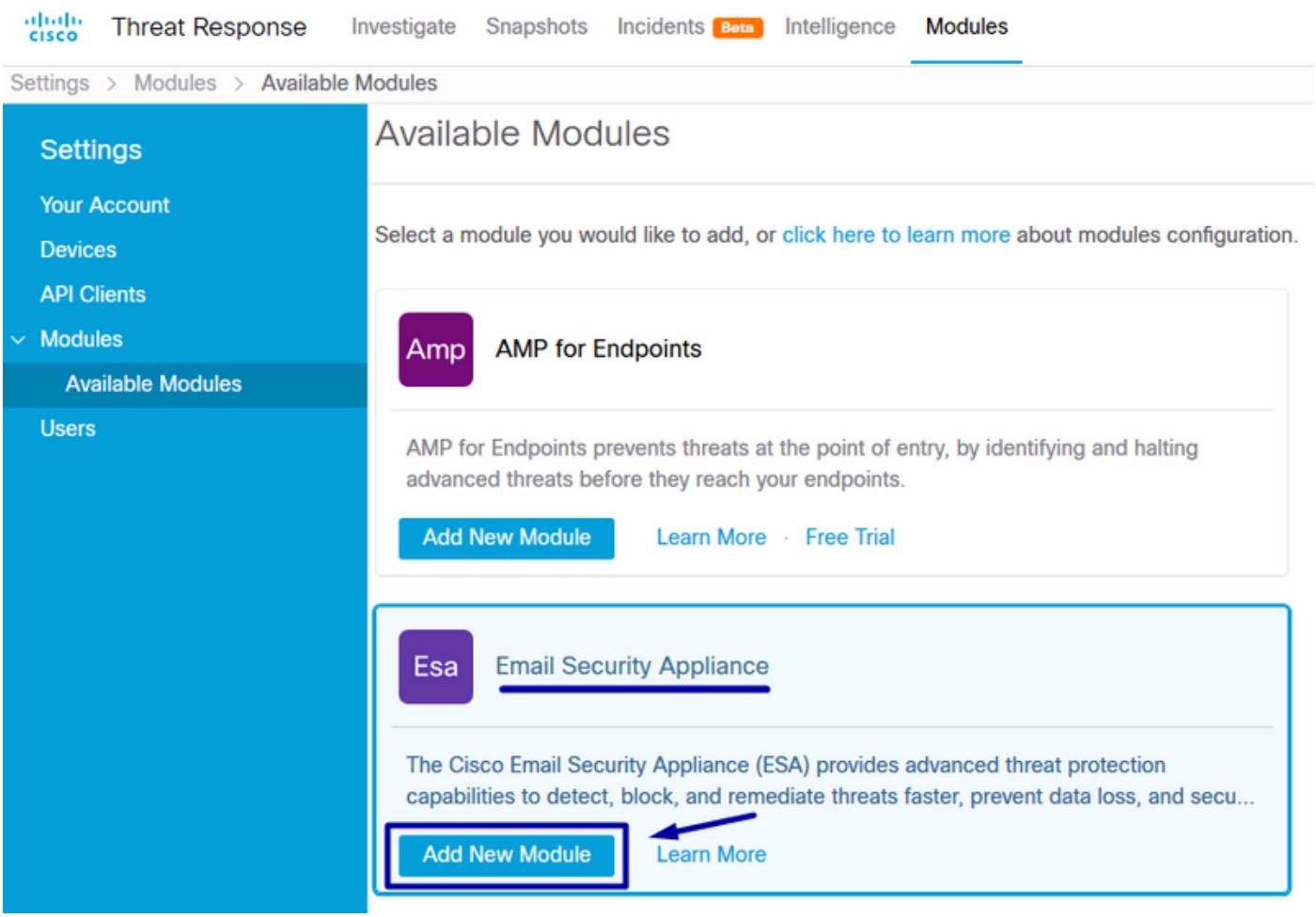


Paso 8. Acceda al portal CTR y agregue un nuevo módulo ESA

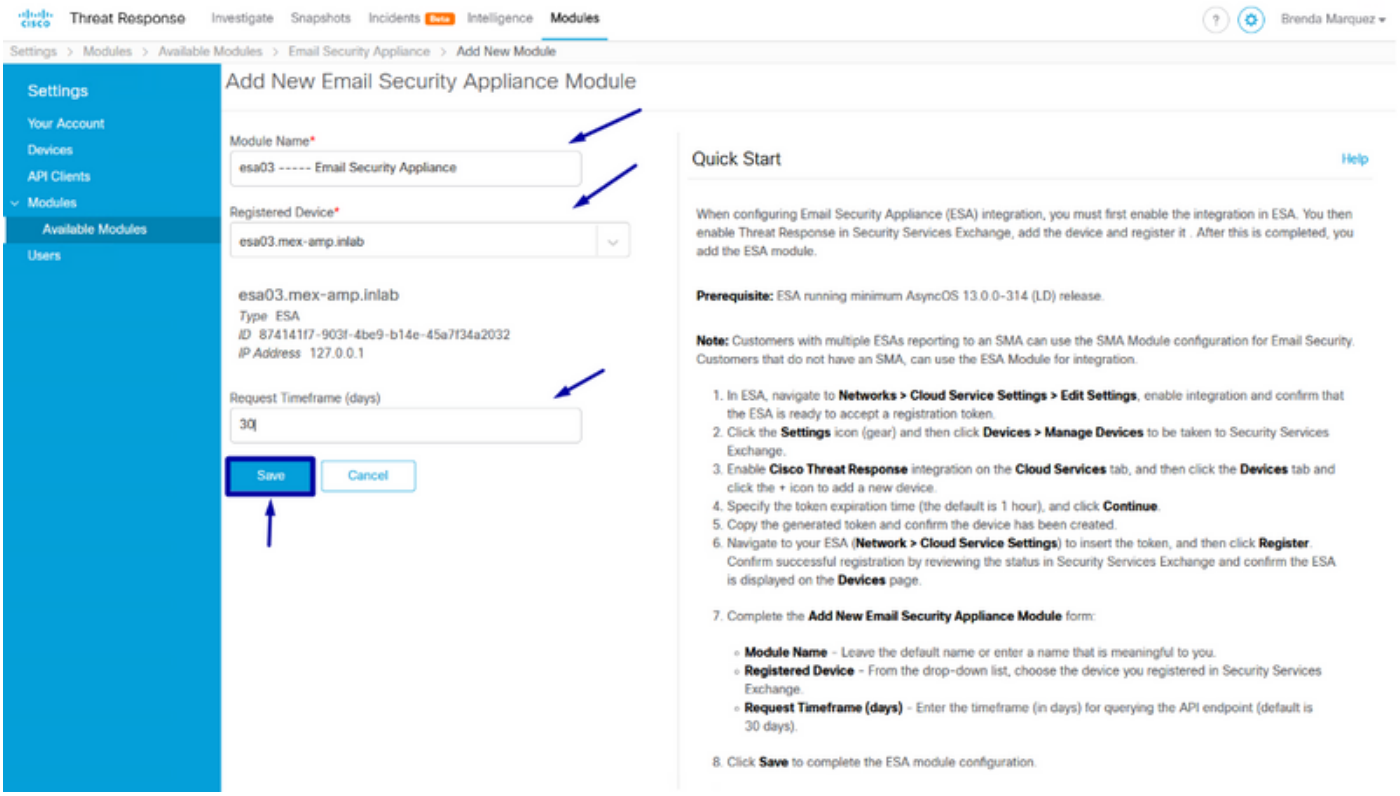
1.- Una vez que esté en el portal de CTR, navegue hasta Módulos > Agregar nuevo módulo, como se muestra en la imagen.



2.- Elija el tipo de módulo, en este caso, el módulo es un módulo Email Security Appliance como la imagen a continuación.

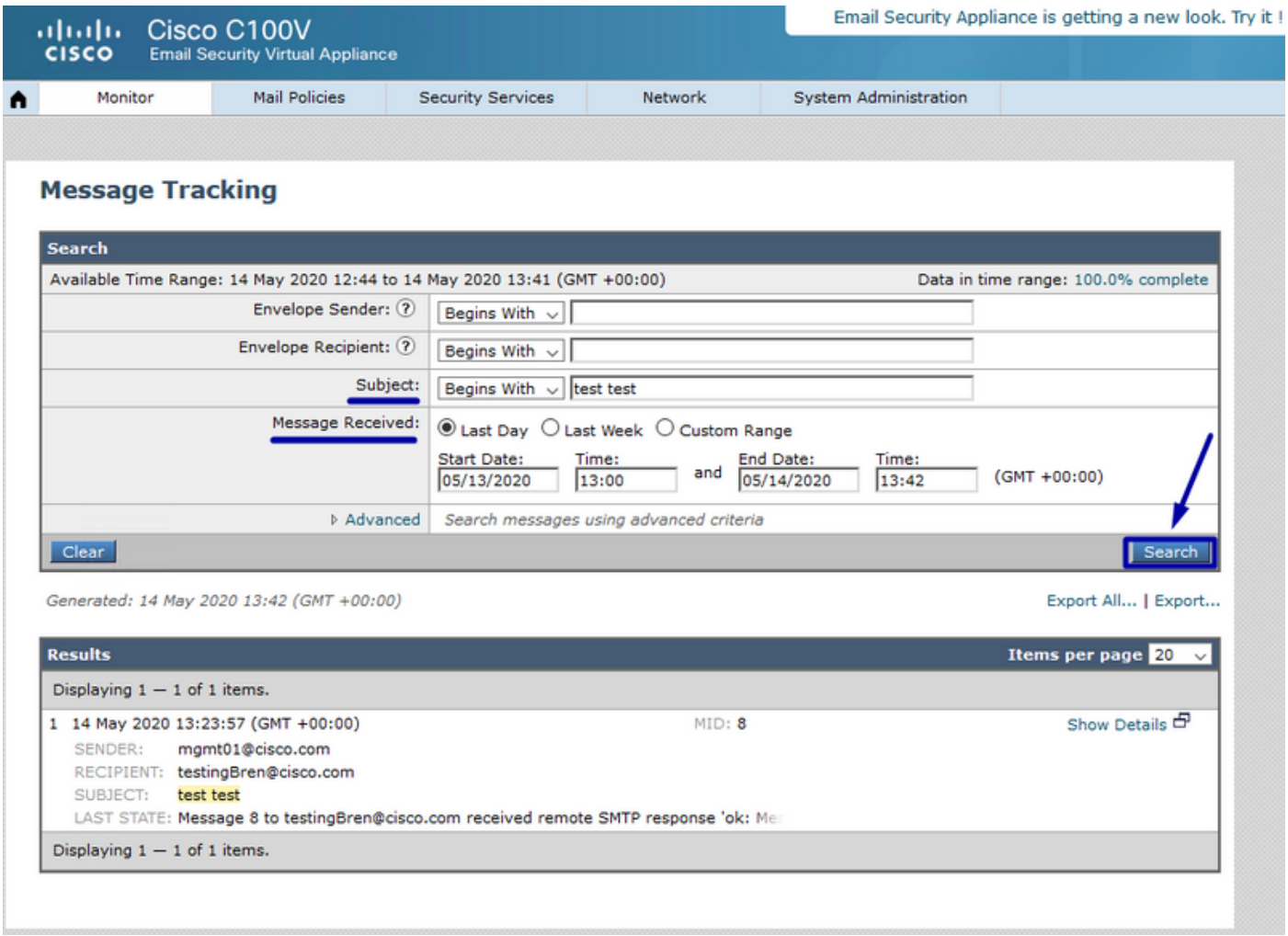


3.- Introduzca los campos siguientes: Module Name (Nombre de módulo), Registered Device (Dispositivo registrado) (seleccione el registrado anteriormente) y Request Timeframe (Días), y Save (Guardar), como se muestra en la imagen.

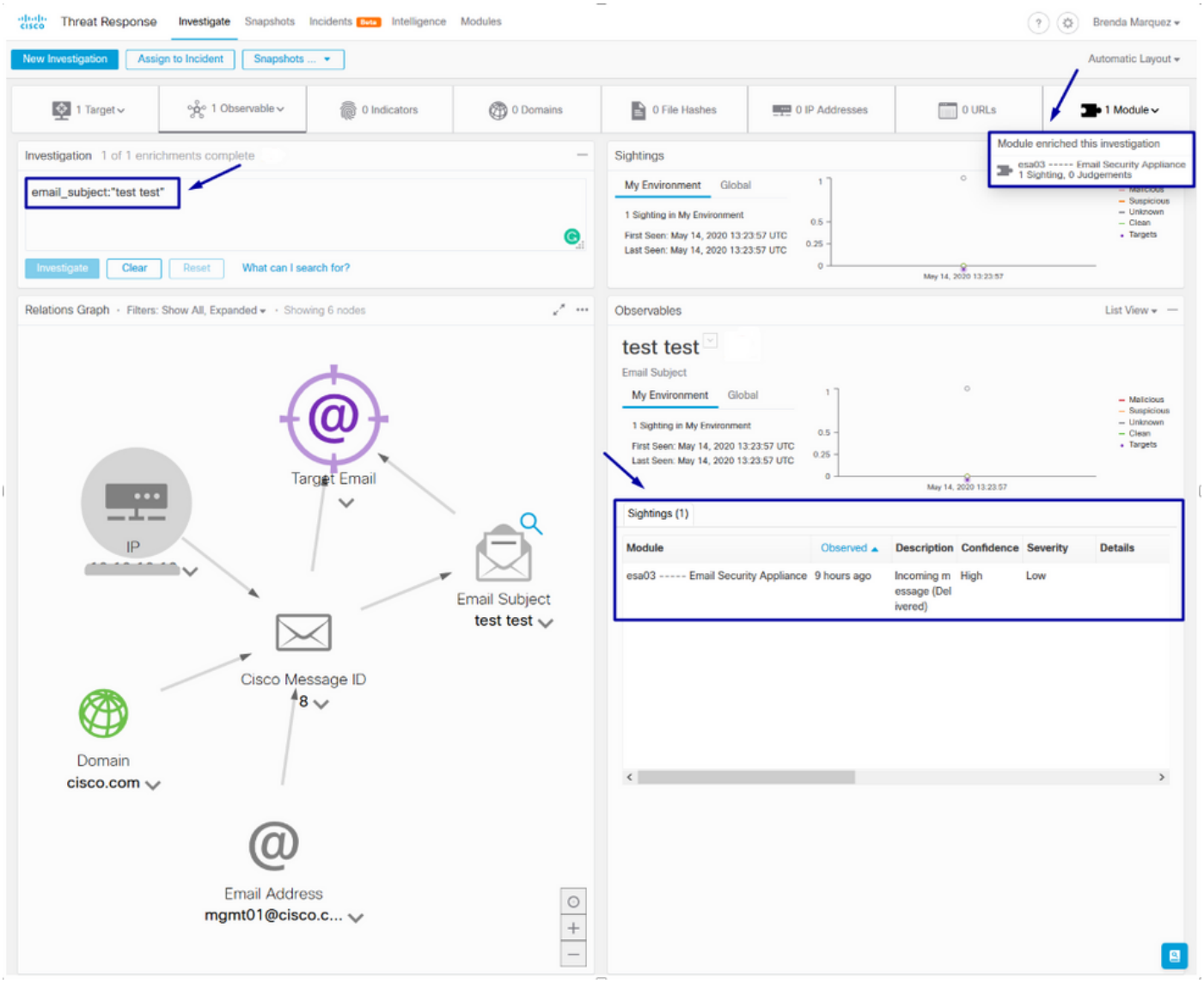


Verificación

Para verificar la integración de CTR y ESA, puede enviar un correo electrónico de prueba, que también puede ver desde su ESA, navegar hasta Monitor > Message Tracking y encontrar el correo electrónico de prueba. En este caso, filtré por Asunto del correo electrónico como la siguiente imagen.



Ahora, desde el portal de CTR, puede realizar una investigación, navegar hasta Investigar y utilizar algunos observables de correo electrónico, como se muestra en la imagen.



Consejo: Puede utilizar la misma sintaxis para otros observables de correo electrónico como se muestra a continuación en la imagen.

IP address	ip:"4.2.2.2"
Domain	domain:"cisco.com"
Sender email address	email:"noreply@cisco.com"
Email message header	email_messageid:"123-abc-456@cisco.com"

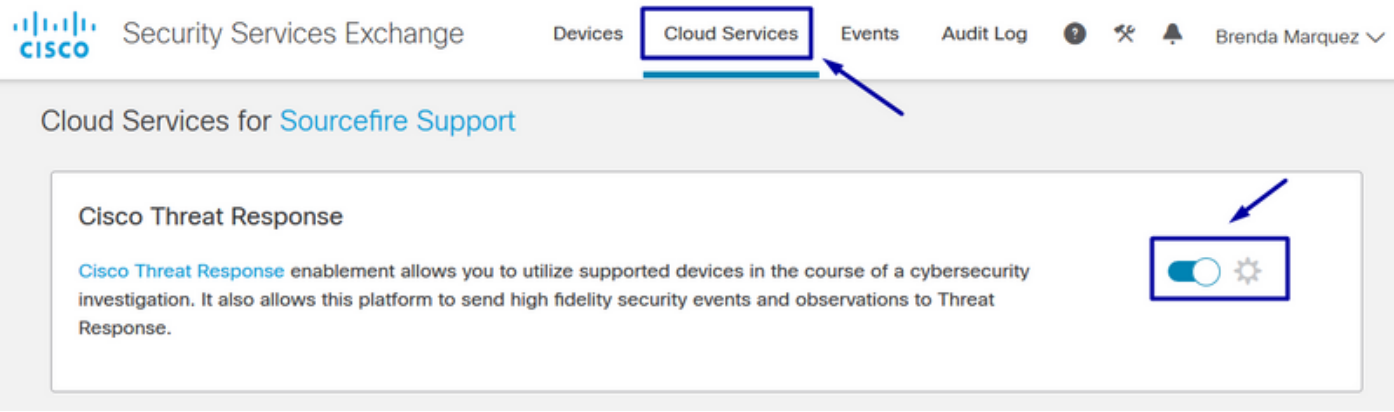
Email subject	email_subject:"Invoice Due"
Cisco Message ID (MID)	cisco_mid:"12345"
SHA256 filehash	sha256:"sha256filehash"
Email attachment file name	file_name:"invoice.pdf"

Troubleshoot

Si es cliente de CES o si gestiona sus dispositivos ESA a través de un SMA, sólo puede conectarse a Threat Response a través de su SMA. Asegúrese de que su SMA ejecuta AsyncOS 12.5 o superior. Si no gestiona su ESA con un SMA e integra el ESA directamente, asegúrese de que se encuentre en la versión 13.0 o posterior de AsyncOS.

El dispositivo ESA no se muestra en el portal CTR

Si su dispositivo ESA no se muestra en el dispositivo registrado desplegable mientras se agrega el módulo ESA en el portal CTR, asegúrese de haber habilitado CTR en SSE, en CTR navegue hasta Módulos > Dispositivos > Administrar dispositivos, luego en el portal SSE navegue hasta Servicios en la nube y habilite CTR, como se muestra a continuación en la imagen:



La investigación de CTR no muestra datos de la ESA

Asegúrese de que:

- La sintaxis de la investigación es correcta, los observables de correo electrónico se muestran arriba en la sección Verificación.
- Ha seleccionado el servidor de respuesta ante amenazas o la nube adecuados (América/Europa).

El ESA no solicita el token de registro

Asegúrese de registrar los cambios cuando se haya habilitado la respuesta a amenazas; de lo contrario, los cambios no se aplicarán a la sección Respuesta a amenazas del ESA.

Error de registro debido a un token no válido o caducado

Asegúrese de que el token se genere desde la nube correcta:

Si utiliza la nube de Europa (UE) para ESA, genere el token a partir de: https://admin.eu.sse.itd.cisco.com/

Si utiliza la nube de América (NAM) para ESA, genere el token a partir de: https://admin.sse.itd.cisco.com/

Además, recuerde que el token de registro tiene un tiempo de vencimiento (seleccione el tiempo más conveniente para completar la integración a tiempo).

Información Relacionada

- **Puede encontrar la información contenida en este artículo en el vídeo Respuesta ante amenazas de Cisco e Integración de ESA.**
- Soporte Técnico y Documentación - Cisco Systems