

Integración de Cisco Threat Response (CTR) y ESA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Paso 1. Vaya a Red > Configuración de servicios en la nube](#)

[Paso 2. Haga clic en Edit Settings \(Editar parámetros\)](#)

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

[Paso 4. Enviar y registrar cambios](#)

[Paso 5. Inicie sesión en el portal CTR y genere el token de registro solicitado en el ESA](#)

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

[Paso 7. Verifique que su dispositivo ESA esté en el portal SSE](#)

[Paso 8. Acceda al portal CTR y agregue un nuevo módulo ESA](#)

[Verificación](#)

[Troubleshoot](#)

[El dispositivo ESA no se muestra en el portal CTR](#)

[La investigación de CTR no muestra datos de la ESA](#)

[El ESA no solicita el token de registro](#)

[Error de registro debido a un token no válido o caducado](#)

[Información Relacionada](#)

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

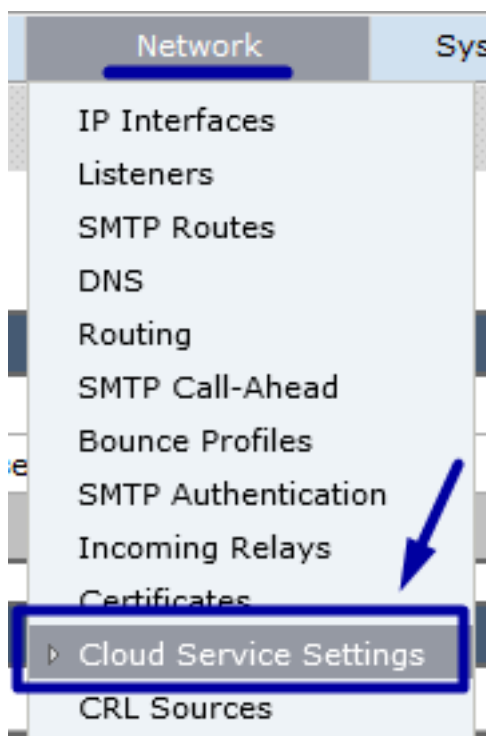
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

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:

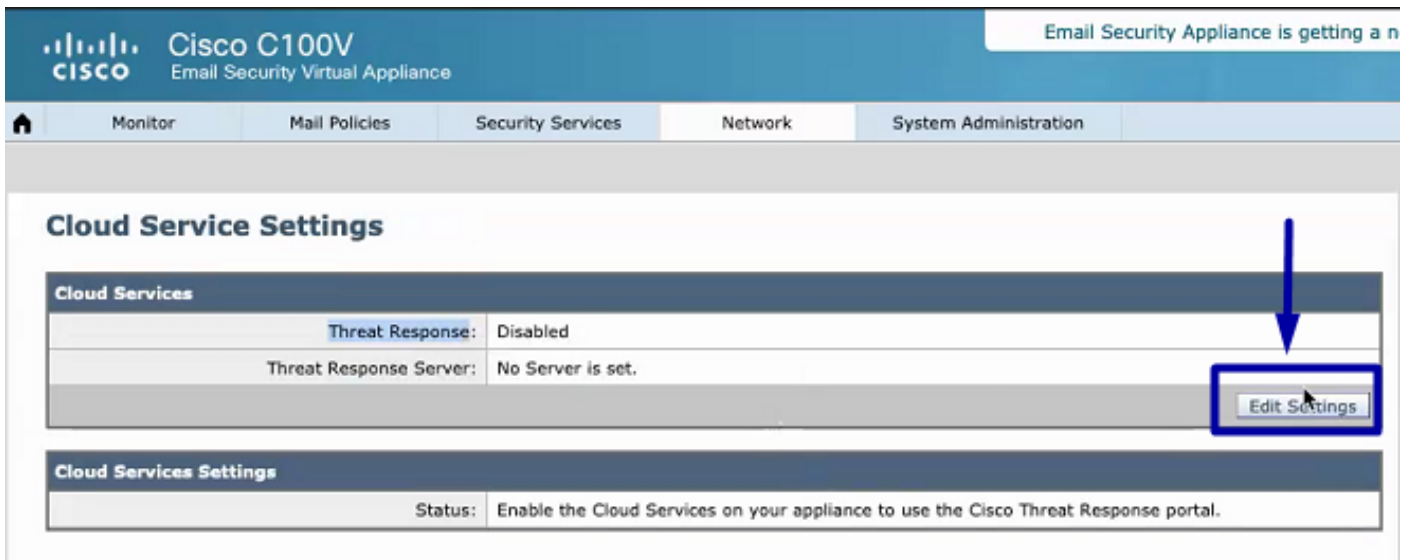
Paso 1. Vaya a Red > Configuración de servicios en la nube

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:

Cloud Service Settings

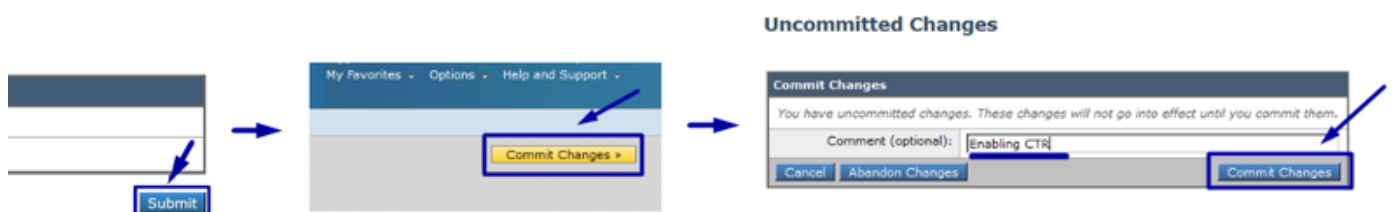


Nota: La selección predeterminada para la URL de Threat Response Server es AMERICAS (api-sse.cisco.com). Para las empresas de EUROPA, haga clic en el menú desplegable y seleccione EUROPE (api.eu.sse.itd.cisco.com)

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.



Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

Cloud Services Settings	
Status:	The Cisco Cloud Service is busy. Navigate back to this page after some time to check the appliance status.

Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

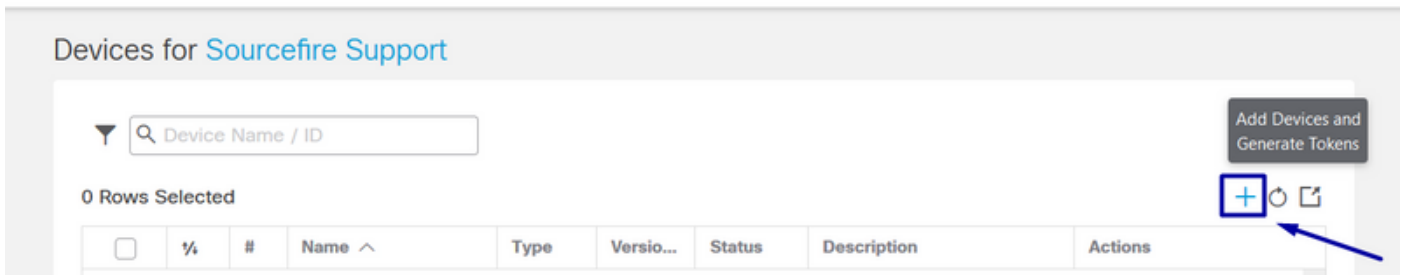
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	
Register	

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.

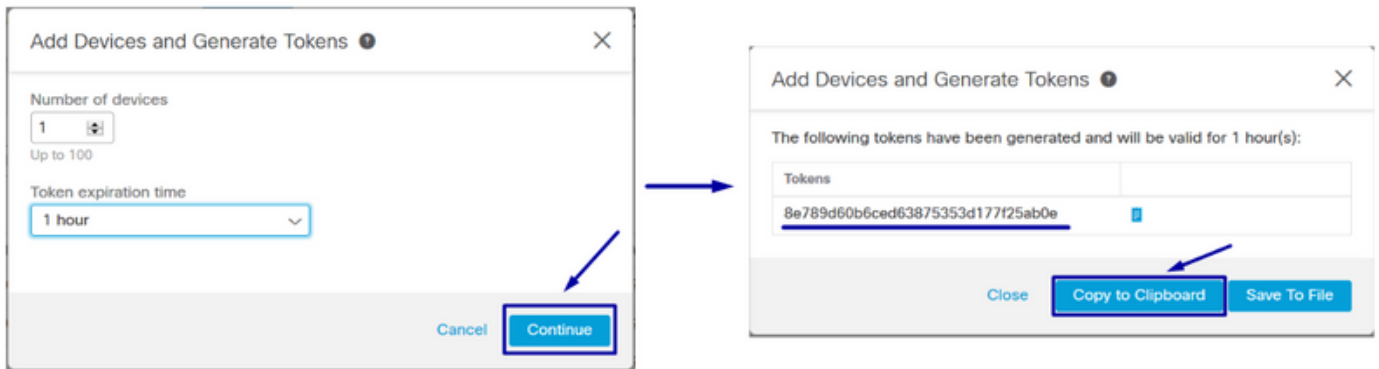
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu is expanded, showing Settings, Your Account, Devices, API Clients, and > Modules. The 'Devices' menu item is highlighted, and the 'Manage Devices' button is visible in the main content area. Below the buttons is a table with columns for Name and Type.

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.

Cloud Service Settings



Cloud Service Settings

Success — A request to register your appliance with the Cisco Threat Response portal is initiated. Navigate back to this page after some time to check the appliance status.

Cloud Services

Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

Cloud Services Settings

Status:	The appliance registration is in progress. Navigate back to this page after some time to check the appliance status.
---------	--

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.

Security Services Exchange Audit Log Brenda Marquez

Devices for Sourcefire Support

Search: esa03

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	▼	1	esa03.mex-amp.inl...	ESA	13.0.0	Registered	ESA	Edit Delete Refresh

ID: 874141f7-903f-4be9-b14e-45a7f... IP Address: 127.0.0.1 Connector Version: 1.3.34
Created: 2020-05-11 20:41:05 UTC

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.

Threat Response Investigate Snapshots Incidents Intelligence **Modules** Brenda Marquez

Settings > Modules

Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. [Click here to view all the available modules.](#)

Your Configurations

[Add New Module](#)

Amp AMP for Endpoints
AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.
[Edit](#) [Learn More](#)

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

Settings

Your Account

Devices

API Clients

▼ Modules

Available Modules

Users

Available Modules

Select a module you would like to add, or [click here to learn more](#) about modules configuration.

Amp **AMP for Endpoints**

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Add New Module](#) [Learn More](#) · [Free Trial](#)

Esa **Email Security Appliance**

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secu...

[Add New Module](#) [Learn More](#)

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.

Cisco Threat Response Investigate Snapshots Incidents Beta Intelligence Modules ? ⚙️ Brenda Marquez ▼

Settings > Modules > Available Modules > Email Security Appliance > Add New Module

Add New Email Security Appliance Module

Module Name*

Registered Device*

esa03.mex-amp.inlab
Type ESA
ID 874141f7-903f-4be9-b14e-45a7f34a2032
IP Address 127.0.0.1

Request Timeframe (days)

[Save](#) [Cancel](#)

Quick Start [Help](#)

When configuring Email Security Appliance (ESA) integration, you must first enable the integration in ESA. You then enable Threat Response in Security Services Exchange, add the device and register it. After this is completed, you add the ESA module.

Prerequisite: ESA running minimum AsyncOS 13.0 0-314 (LD) release.

Note: Customers with multiple ESAs reporting to an SMA can use the SMA Module configuration for Email Security. Customers that do not have an SMA, can use the ESA Module for integration.

- In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
- Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
- Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
- Specify the token expiration time (the default is 1 hour), and click **Continue**.
- Copy the generated token and confirm the device has been created.
- Navigate to your ESA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the ESA is displayed on the **Devices** page.
- Complete the **Add New Email Security Appliance Module** form:
 - Module Name** - Leave the default name or enter a name that is meaningful to you.
 - Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
 - Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
- Click **Save** to complete the ESA module configuration.

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.

The screenshot shows the Cisco C100V Email Security Virtual Appliance interface. The top navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System Administration'. The 'Message Tracking' section is active, displaying a search form with the following fields:

- Envelope Sender: Begins With
- Envelope Recipient: Begins With
- Subject: Begins With test test
- Message Received: Last Day (selected), Last Week, Custom Range
- Start Date: 05/13/2020, Time: 13:00, and End Date: 05/14/2020, Time: 13:42 (GMT +00:00)

A blue arrow points to the 'Search' button. Below the search form, the results are displayed as follows:

Generated: 14 May 2020 13:42 (GMT +00:00) Export All... | Export...

Results Items per page 20

Displaying 1 — 1 of 1 items.

1	14 May 2020 13:23:57 (GMT +00:00)	MID: 8	Show Details
---	-----------------------------------	--------	--------------

SENDER: mgmt01@cisco.com
RECIPIENT: testingBren@cisco.com
SUBJECT: test test
LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:

Displaying 1 — 1 of 1 items.

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.

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate, Snapshots, Incidents, Intelligence, and Modules. The user is logged in as Brenda Marquez. The interface displays search filters for 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The search query is `email_subject:'test test'`. The Relations Graph shows a central node for 'Target Email' connected to 'IP', 'Domain', 'Cisco Message ID', and 'Email Address'. The Observables section shows a graph for 'test test' with a single sighting. The Sighting table below shows one entry:

Module	Observed	Description	Confidence	Severity	Details
esa03 ----- Email Security Appliance	9 hours ago	Incoming m essage (Del ivered)	High	Low	

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

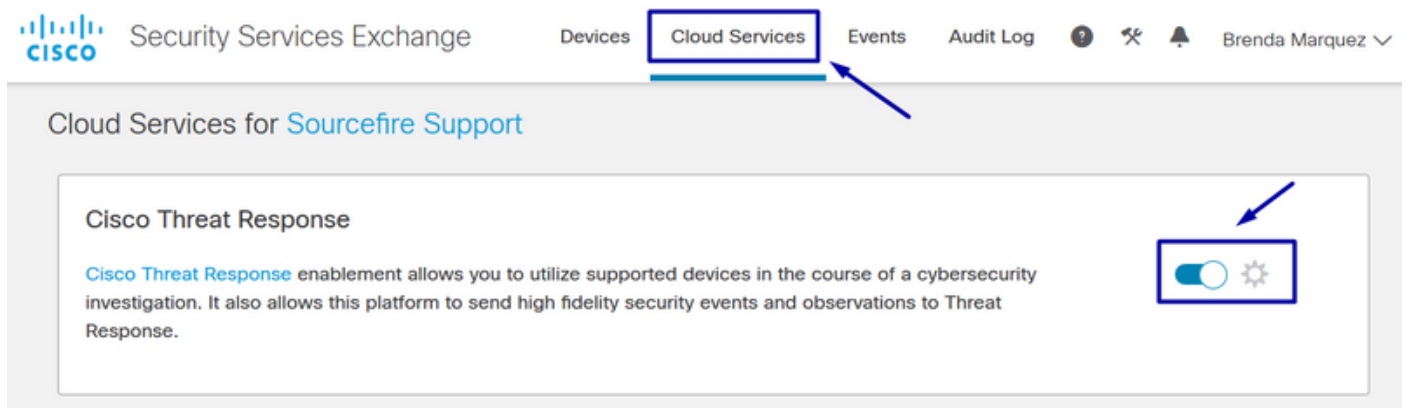
IP address	<code>ip:"4.2.2.2"</code>	Email subject	<code>email_subject:"Invoice Due"</code>
Domain	<code>domain:"cisco.com"</code>	Cisco Message ID (MID)	<code>cisco_mid:"12345"</code>
Sender email address	<code>email:"noreply@cisco.com"</code>	SHA256 filehash	<code>sha256:"sha256filehash"</code>
Email message header	<code>email_messageid:"123-abc-456@cisco.com"</code>	Email attachment file name	<code>file_name:"invoice.pdf"</code>

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](#)