

Integration von Cisco Threat Response (CTR) und ESA

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Schritt 1: Navigieren Sie zu Netzwerk > Cloud Service Settings.](#)

[Schritt 2: Klicken Sie auf Einstellungen bearbeiten.](#)

[Schritt 3: Aktivieren Sie das Kontrollkästchen Enable \(Aktivieren\) und Threat Response Server.](#)

[Schritt 4: Änderungen senden und bestätigen](#)

[Schritt 5: Melden Sie sich beim CTR-Portal an, und generieren Sie das in der ESA angeforderte Registrierungs-Token.](#)

[Schritt 6: Fügen Sie das Registrierungstoken \(vom CTR-Portal generiert\) in die ESA ein.](#)

[Schritt 7: Überprüfen Sie, ob sich Ihr ESA-Gerät im SSE-Portal befindet.](#)

[Schritt 8: Navigieren Sie zum CTR-Portal, und fügen Sie ein neues ESA-Modul hinzu.](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[ESA-Gerät wird nicht im CTR-Portal angezeigt.](#)

[CTR-Untersuchungen zeigen keine Daten von der ESA.](#)

[Die ESA fordert das Registrierungstoken nicht an.](#)

[Die Registrierung ist aufgrund eines ungültigen oder abgelaufenen Tokens fehlgeschlagen.](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird der Prozess zur Integration von Cisco Threat Response (CTR) mit E-Mail Security Appliance (ESA) beschrieben. Außerdem wird erläutert, wie Sie dies überprüfen können, um CTR-Untersuchungen durchzuführen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Reaktion auf Bedrohungen von Cisco
- E-Mail Security Appliance

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CTR-Konto
- Cisco Security Services Exchange
- ESA C100V auf Softwareversion 13.0.0-392

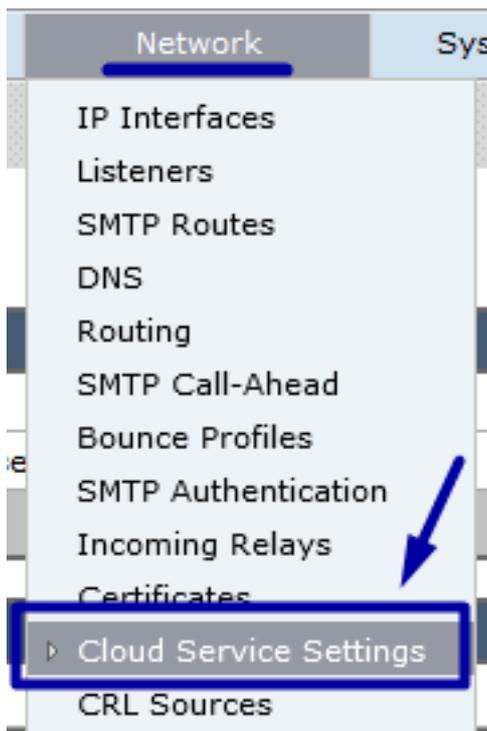
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Um die Integration CTR und ESA zu konfigurieren, melden Sie sich bei Ihrer E-Mail Security Virtual Appliance an und befolgen Sie die folgenden Schritte:

Schritt 1: Navigieren Sie zu Netzwerk > Cloud Service Settings.

Navigieren Sie in der ESA zum Kontextmenü Netzwerk > Cloud Service Settings, um den aktuellen Bedrohungsreaktionsstatus (Deaktiviert/Aktiviert) anzuzeigen, wie im Bild gezeigt.



Schritt 2: Klicken Sie auf Einstellungen bearbeiten.

Die Funktion "Threat Response" in der ESA ist bisher deaktiviert. Klicken Sie zum Aktivieren der Funktion auf "Edit Settings" (Einstellungen bearbeiten), wie im Bild gezeigt:



Schritt 3: Aktivieren Sie das Kontrollkästchen Enable (Aktivieren) und Threat Response Server.

Aktivieren Sie das Kontrollkästchen Enable (Aktivieren), und wählen Sie dann den Threat Response Server aus. Weitere Informationen finden Sie in der Abbildung unten:

Cloud Service Settings

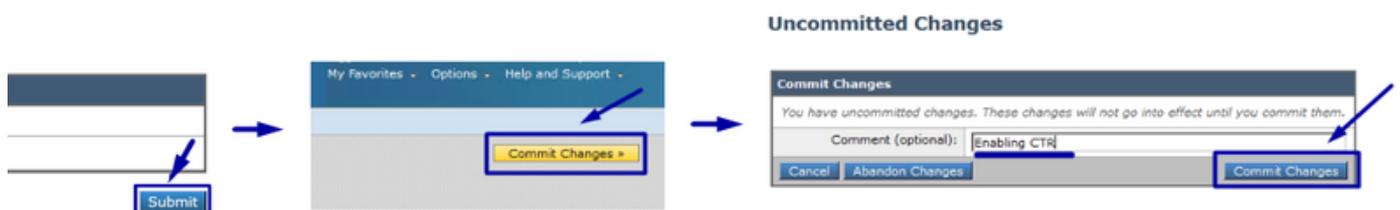


Hinweis: Die Standardauswahl für die URL des Threat Response-Servers lautet AMERICAS (api-sse.cisco.com). Klicken Sie für EUROPE-Unternehmen auf das Dropdown-Menü, und wählen Sie EUROPE (api.eu.sse.itd.cisco.com).

Schritt 4: Änderungen senden und bestätigen

Die Änderungen müssen eingesendet und bestätigt werden, um sie zu speichern und anzuwenden. Wenn nun die ESA-Schnittstelle aktualisiert wird, wird ein Registrierungstoken angefordert, um die Integration zu registrieren, wie in der Abbildung unten gezeigt.

Hinweis: Sie sehen eine Erfolgsmeldung: Ihre Änderungen wurden übernommen.



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	

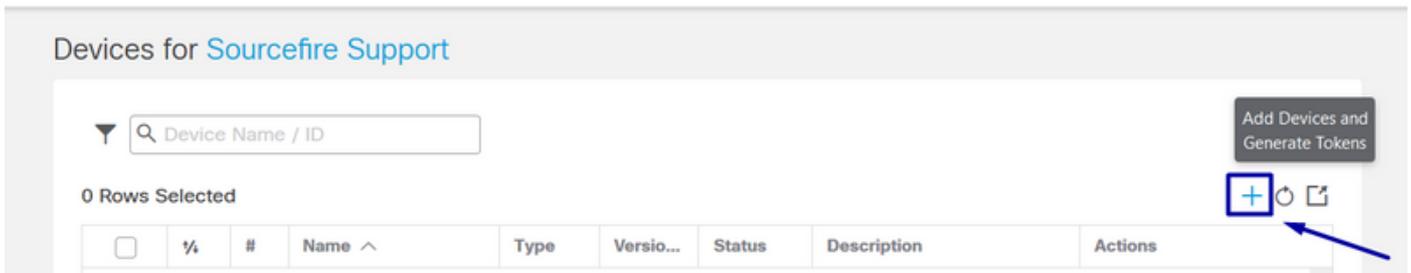
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	

Schritt 5: Melden Sie sich beim CTR-Portal an, und generieren Sie das in der ESA angeforderte Registrierungs-Token.

1.- Navigieren Sie im CTR-Portal zu Modules > Devices > Manage Devices (Module > Geräte > Geräte verwalten), sehen Sie das nächste Bild.

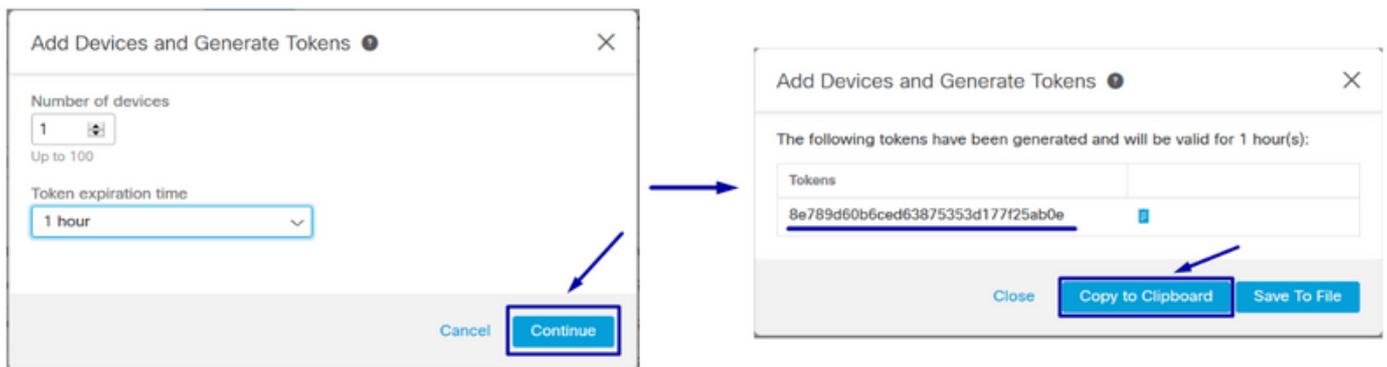
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the menu, the breadcrumb 'Settings > Devices' is shown. The 'Devices' section contains a 'Manage Devices' button (highlighted with a blue box and arrow) and a 'Reload Devices' button. A sidebar on the left lists 'Settings', 'Your Account', 'Devices' (highlighted with a blue box and arrow), 'API Clients', and '> Modules'.

2.- Der Link "Geräte verwalten" leitet Sie zur Security Services Exchange (SSE) um. Wenn Sie dort sind, klicken Sie auf das Symbol "Geräte hinzufügen" und "Token generieren", wie im Bild gezeigt.



3.- Klicken Sie auf Weiter, um das Token zu generieren. Wenn das Token generiert wurde, klicken Sie auf Kopieren in die Zwischenablage, wie im Bild gezeigt.

Tipp: Sie können die Anzahl der hinzuzufügenden Geräte auswählen (von 1 bis zu 100) und außerdem die Ablaufzeit für Token auswählen (1 Stunde, 2 Stunden, 4 Stunden, 6 Stunden, 8 Stunden, 12 Stunden, 01 Tage, 02 Tage, 03 Tage, 04 Tage und 05 Tage).



Schritt 6: Fügen Sie das Registrierungstoken (vom CTR-Portal generiert) in die ESA ein.

Nachdem das Registrierungstoken generiert wurde, fügen Sie es wie unten abgebildet im Abschnitt "Cloud Services Settings" der ESA ein.

Hinweis: Sie sehen eine Erfolgsmeldung: Es wird eine Anfrage zur Registrierung Ihrer Appliance beim Cisco Threat Response-Portal gestellt. Navigieren Sie nach einiger Zeit wieder zu dieser Seite, um den Status der Appliance zu überprüfen.



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.
---------	--

Schritt 7: Überprüfen Sie, ob sich Ihr ESA-Gerät im SSE-Portal befindet.

Sie können zum SSE-Portal (CTR > Module > Devices > Manage Devices) navigieren und auf der Registerkarte Search (Suchen) Ihr ESA-Gerät anzeigen, wie im Bild gezeigt.

Security Services Exchange Audit Log Brenda Marquez

Devices for Sourcefire Support

Search:

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	▼	1	esa03.mex-amp.inl...	ESA	13.0.0	Registere ESA		/ 🗑️ 📄

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

Schritt 8: Navigieren Sie zum CTR-Portal, und fügen Sie ein neues ESA-Modul hinzu.

1.- Navigieren Sie im CTR-Portal zu Module > Add New Module (Neues Modul hinzufügen), wie im Bild gezeigt.

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

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 for Endpoints
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.- Wählen Sie den Modultyp aus. In diesem Fall ist das Modul ein E-Mail-Security-Appliance-

Modul wie unten abgebildet.

Settings > Modules > Available Modules

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.- Geben Sie die Felder ein: Modulname, registriertes Gerät (wählen Sie das zuvor registrierte aus) und Anforderungszeitrahmen (Tage) sowie Speichern, wie im Bild gezeigt.

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

Add New Email Security Appliance Module

Module Name*
esa03 ----- Email Security Appliance

Registered Device*
esa03.mex-amp.inlab

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

Request Timeframe (days)
30

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

Quick Start

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.

Überprüfen

Um die CTR- und ESA-Integration zu überprüfen, können Sie eine Test-E-Mail senden, die Sie auch von der ESA aus sehen können. Navigieren Sie zu Monitor > Message Tracking (Überwachung > Nachrichtenverfolgung), und suchen Sie die Test-E-Mail. In diesem Fall habe ich nach E-Mail Betreff wie das Bild unten gefiltert.

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 main content area is titled 'Message Tracking' and contains a search form. The search form has the following fields and options:

- Search** section with 'Available Time Range: 14 May 2020 12:44 to 14 May 2020 13:41 (GMT +00:00)' and 'Data in time range: 100.0% complete'.
- Envelope Sender:** ? Begins With []
- Envelope Recipient:** ? Begins With []
- Subject:** Begins With [test test]
- Message Received:** Last Day Last Week Custom Range
- Start Date:** 05/13/2020 **Time:** 13:00 and **End Date:** 05/14/2020 **Time:** 13:42 (GMT +00:00)
- Advanced** Search messages using advanced criteria
- Clear** and **Search** buttons

Below the search form, it says 'Generated: 14 May 2020 13:42 (GMT +00:00)' and 'Export All... | Export...'. The **Results** section shows 'Items per page 20' and 'Displaying 1 — 1 of 1 items.' The single result is:

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

Message 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.

Im CTR-Portal können Sie jetzt eine Untersuchung durchführen, zu Investigate navigieren und einige E-Mail-Beobachtungsmaterialien verwenden, wie im Bild gezeigt.

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate (selected), Snapshots, Incidents, Intelligence, and Modules. Below the navigation, there are filters for 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The search bar contains the query 'email_subject:"test test"'. Below the search bar, there are buttons for 'Investigate', 'Clear', and 'Reset'. The main area is divided into three panels: 'Relations Graph' showing a network of nodes (IP, Domain, Email Address, Cisco Message ID, Target Email, Email Subject), 'Sightings' showing a graph of sightings over time, and 'Observables' showing details for the 'test test' observable. A table in the 'Observables' panel lists sightings, with one entry highlighted: 'esa03 - Email Security Appliance' observed 9 hours ago with a description of an incoming message.

Tip: Sie können die gleiche Syntax für andere E-Mail-Observables wie im Bild verwenden.

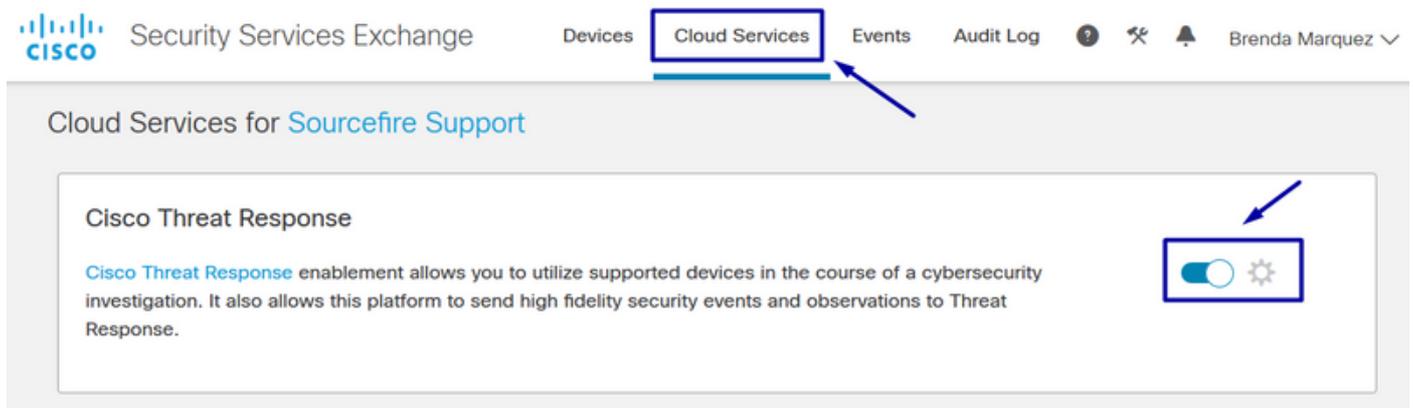
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

Fehlerbehebung

Wenn Sie ein CES-Kunde sind oder Ihre ESA-Geräte über eine SMA verwalten, können Sie nur über Ihre SMA eine Verbindung mit Threat Response herstellen. Stellen Sie sicher, dass Ihre SMA AsyncOS 12.5 oder höher ausführt. Wenn Sie Ihre ESA nicht mit einer SMA verwalten und die ESA direkt integrieren, stellen Sie sicher, dass die ESA ab AsyncOS Version 13.0 verfügbar ist.

ESA-Gerät wird nicht im CTR-Portal angezeigt.

Wenn Ihr ESA-Gerät nicht im Dropdown-Menü für registrierte Geräte angezeigt wird, während das ESA-Modul im CTR-Portal hinzugefügt wird, stellen Sie sicher, dass CTR in SSE aktiviert ist. Navigieren Sie im CTR zu Module > Devices > Manage Devices (Geräte > Geräte verwalten), und navigieren Sie im SSE-Portal zu Cloud Services, und aktivieren Sie CTR (siehe unten):



CTR-Untersuchungen zeigen keine Daten von der ESA.

Stellen Sie sicher, dass

- Die Syntax der Untersuchung ist korrekt. Die E-Mail-Beobachtungen sind oben im Abschnitt Überprüfen aufgeführt.
- Sie haben den richtigen Threat Response Server oder die richtige Cloud (Nord- und Südamerika/Europa) ausgewählt.

Die ESA fordert das Registrierungstoken nicht an.

Stellen Sie sicher, dass Sie die Änderungen bestätigen, wenn die Bedrohungsantwort aktiviert wurde. Andernfalls werden die Änderungen nicht auf den Abschnitt "Bedrohungsantwort" der ESA angewendet.

Die Registrierung ist aufgrund eines ungültigen oder abgelaufenen Tokens fehlgeschlagen.

Stellen Sie sicher, dass der Token aus der richtigen Cloud generiert wird:

Wenn Sie Europa (EU) Cloud für ESA verwenden, erstellen Sie das Token aus:

<https://admin.eu.sse.itd.cisco.com/>

Wenn Sie Americas (NAM) Cloud für ESA verwenden, generieren Sie das Token aus:

<https://admin.sse.itd.cisco.com/>

Denken Sie auch daran, dass das Registrierungstoken eine Ablaufzeit hat (wählen Sie den für den rechtzeitigen Abschluss der Integration günstigsten Zeitpunkt aus).

Zugehörige Informationen

- Die Informationen in diesem Artikel finden Sie im Video [zur Cisco Threat Response- und ESA-Integration](#).

- [Technischer Support und Dokumentation - Cisco Systems](#)