Integration der WSA mit CTR

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Integration von Web Security Appliance (WSA) in das Cisco Threat Response (CTR)-Portal.

Verfasst von Shikha Grover und herausgegeben von Yeraldin Sanchez Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- WSA-Zugriff
- CTR-Portalzugriff
- Cisco Security Account

Verwendete Komponenten

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

- Async Operating System, Version 12.x oder höher

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

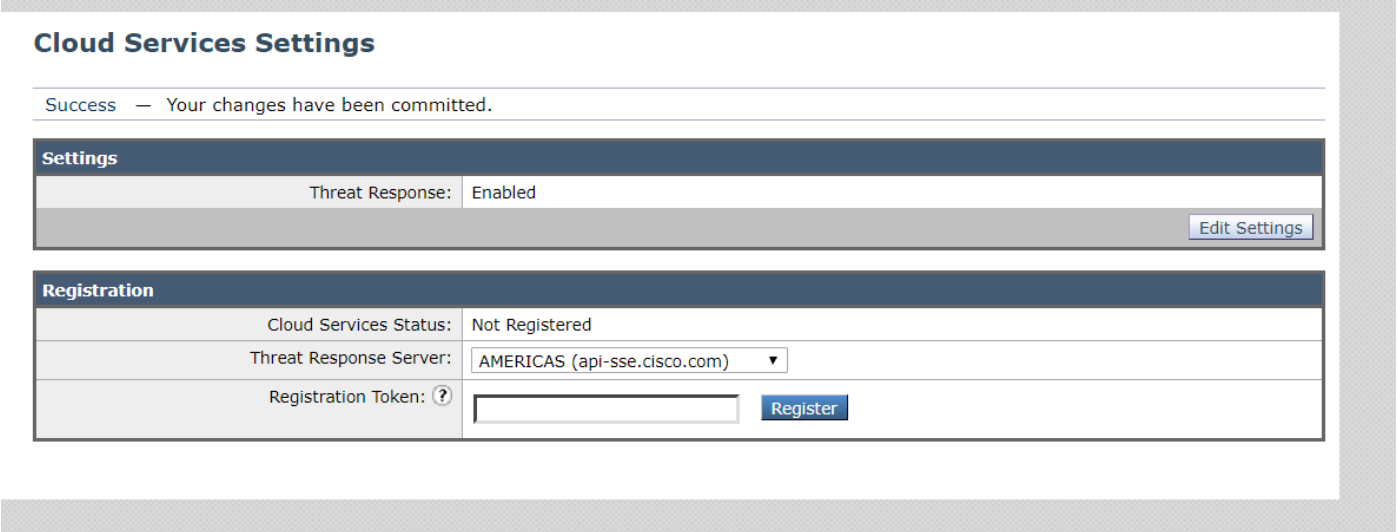
> **Vorsicht**: Wenn Sie über eine regionale URL für den Asien-Pazifik-Raum, Japan und China (https://visibility.apjc.amp.cisco.com/) auf CTR zugreifen, wird die Integration mit Ihrer Appliance derzeit nicht unterstützt.

Schritt 1: Aktivieren Sie **CTROBSERVABLE** unter REPORTINGCONFIG in der CLI, und bestätigen Sie die Änderungen, wie im Bild gezeigt.

```
WSA-12-0-1-173.COM> reportingconfig


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings
alculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
]> ctrobservable

TR observable indexing currently Enabled.
re you sure you want to change the setting? [N]> y


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
```

Schritt 2: Konfigurieren Sie das Cloud-Portal von Security Service Exchange (SSE), navigieren Sie zu **Network > Cloud Services Settings > Edit settings**, und klicken Sie auf **Enable** and **Submit** (**Netzwerk > Cloud Services Settings > Edit settings**), wie im Bild gezeigt.

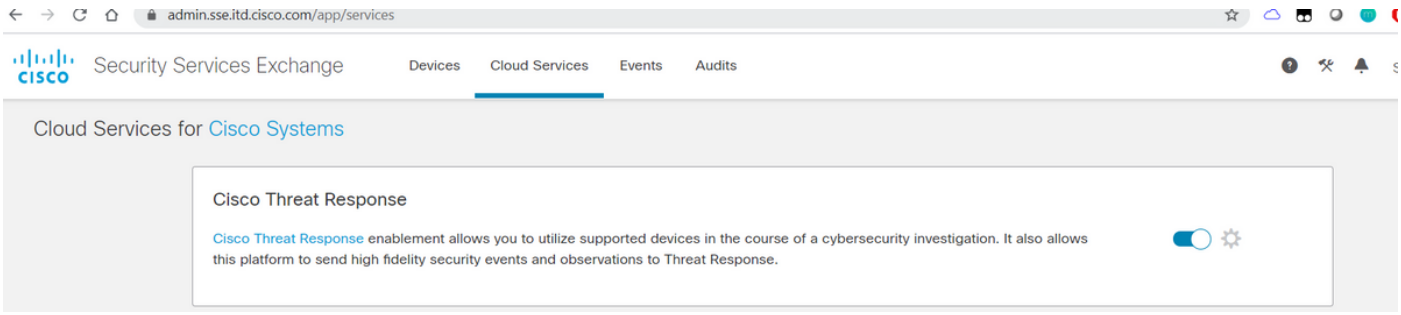
Wählen Sie die Cloud nach Ihrem Standort aus, wie im Bild gezeigt.



Schritt 3: Wenn Sie kein Cisco Security-Konto haben, können Sie im Cisco Threat Response-Portal ein Benutzerkonto mit Administratorrechten erstellen.

Um ein neues Benutzerkonto zu erstellen, navigieren Sie zur Anmeldeseite des Cisco Threat Response-Portals.

Schritt 4: Aktivieren Sie Cisco Threat Response unter Cloud-Services im SSE-Portal, wie im Bild gezeigt.



Schritt 5: Stellen Sie sicher, dass die WSA für Port 443 zum SSE-Portal erreichbar ist:

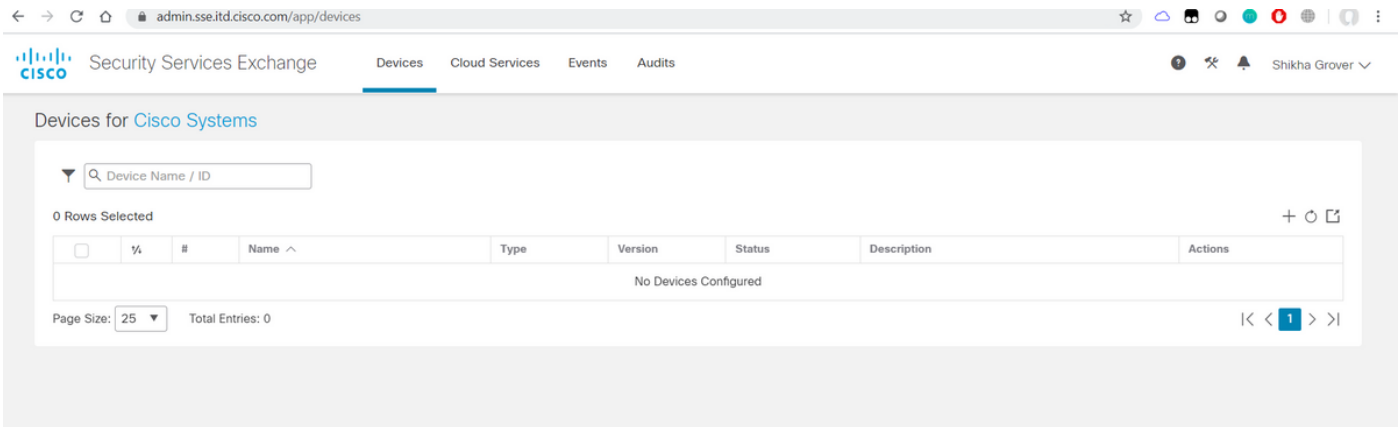
- api.eu.sse.itd.cisco.com (Europa)
- api-sse.cisco.com (Amerika)

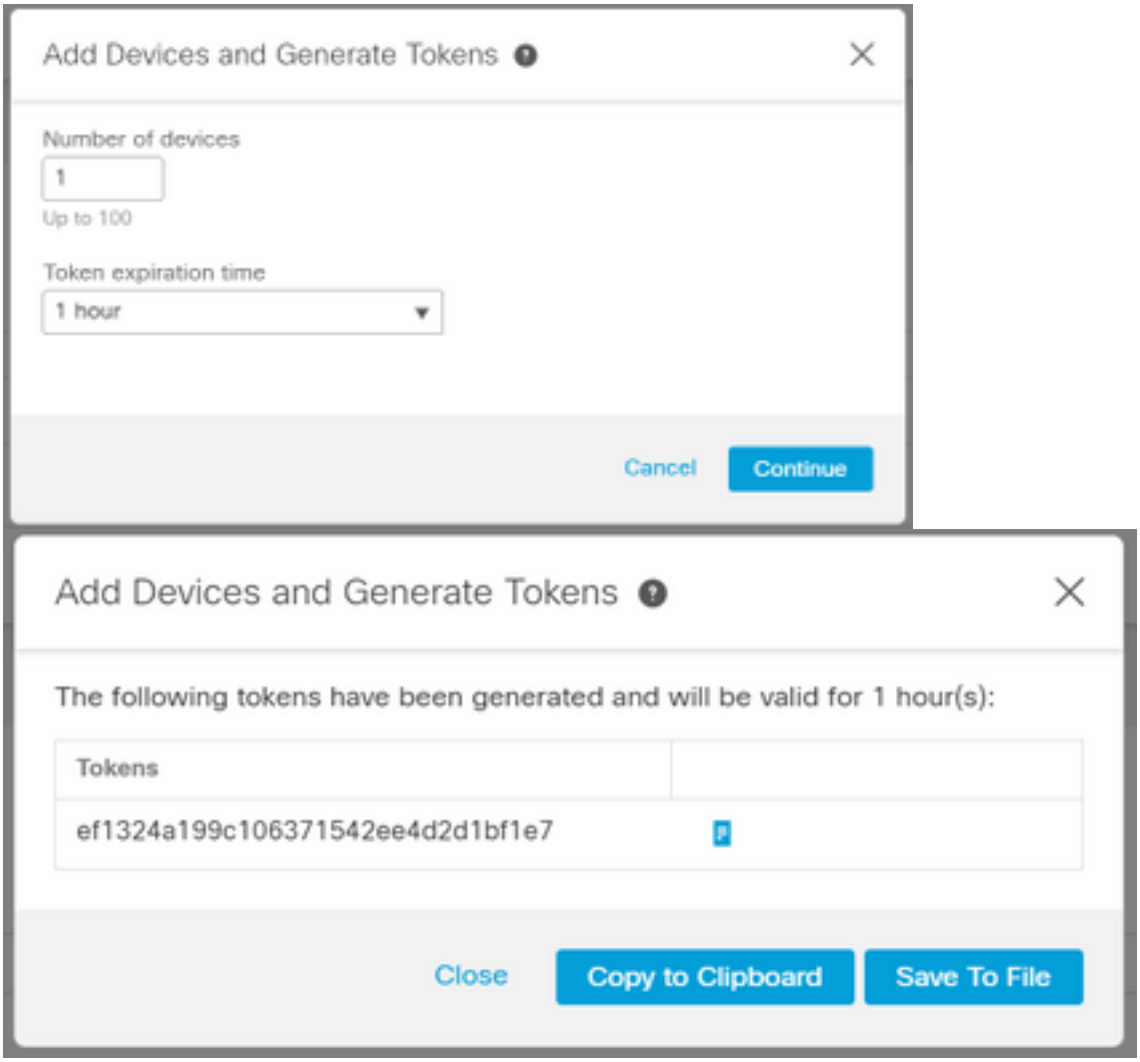
Appliance registrieren

Schritt 1: Rufen Sie ein Registrierungstoken vom Security Services Exchange-Portal (SSE) ab, um Ihre Appliance beim Exchange-Portal für Sicherheitsdienste zu registrieren.

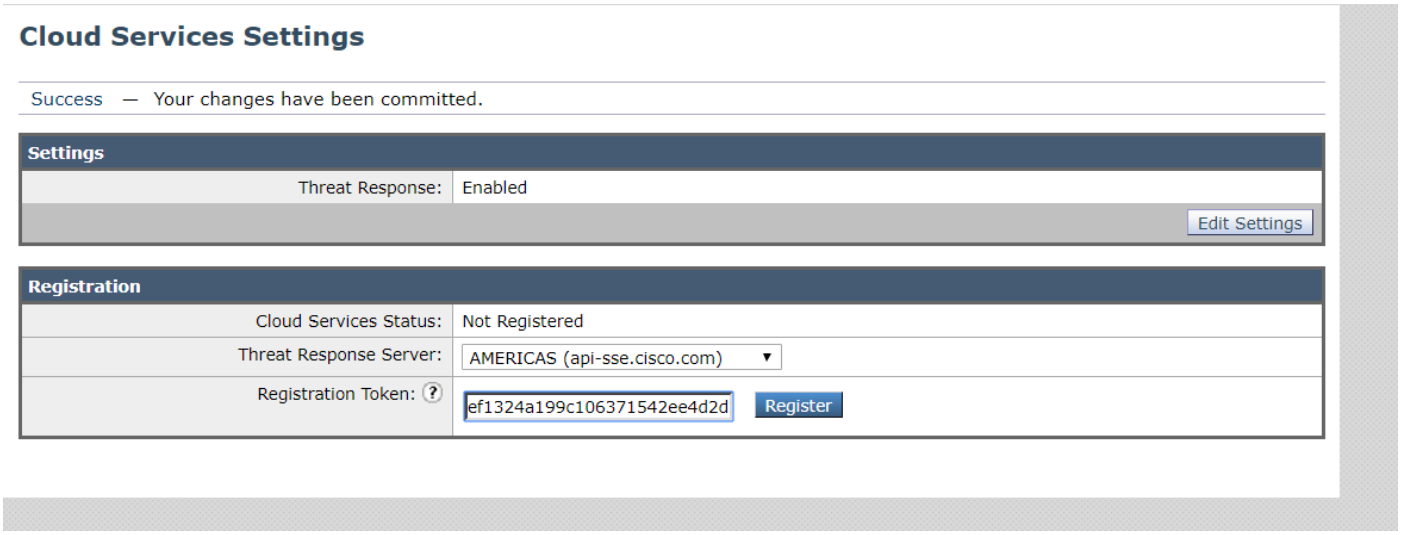
Der SSE-Portal-Link lautet https://admin.sse.itd.cisco.com/app/devices.

> **Hinweis**: Verwenden Sie CTR-Kontoanmeldeinformationen, um sich beim SSE-Portal anzumelden.



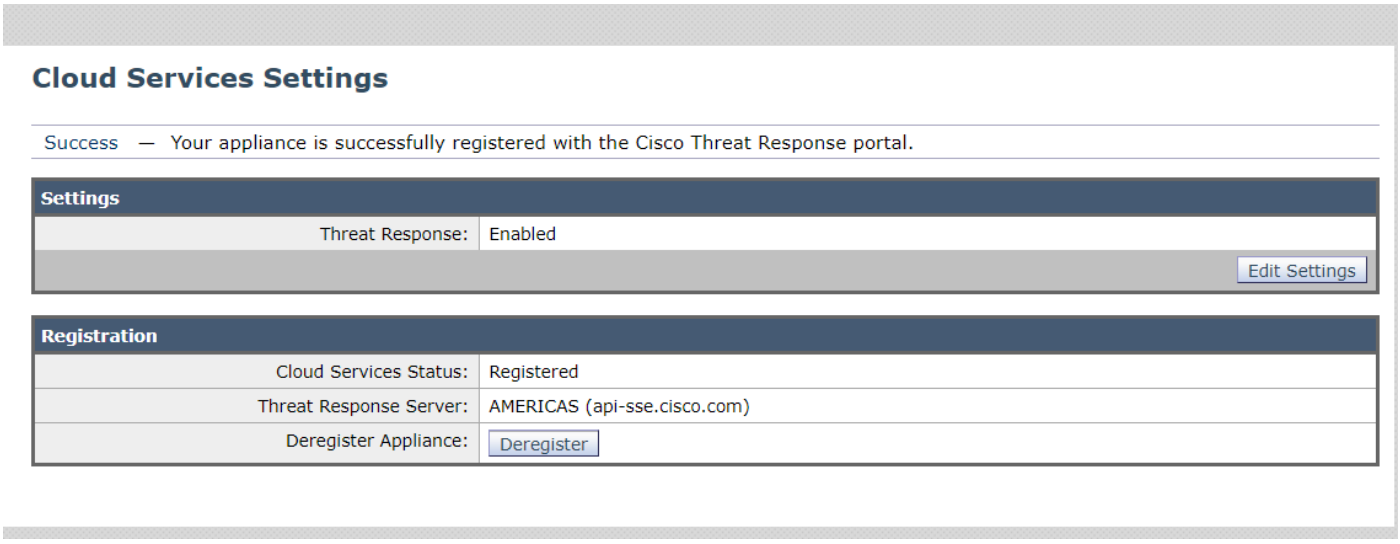


Schritt 2: Geben Sie das im Security Services Exchange-Portal in WSA abgerufene Registrierungstoken ein, und klicken Sie auf **Registrieren**, wie im Bild gezeigt.

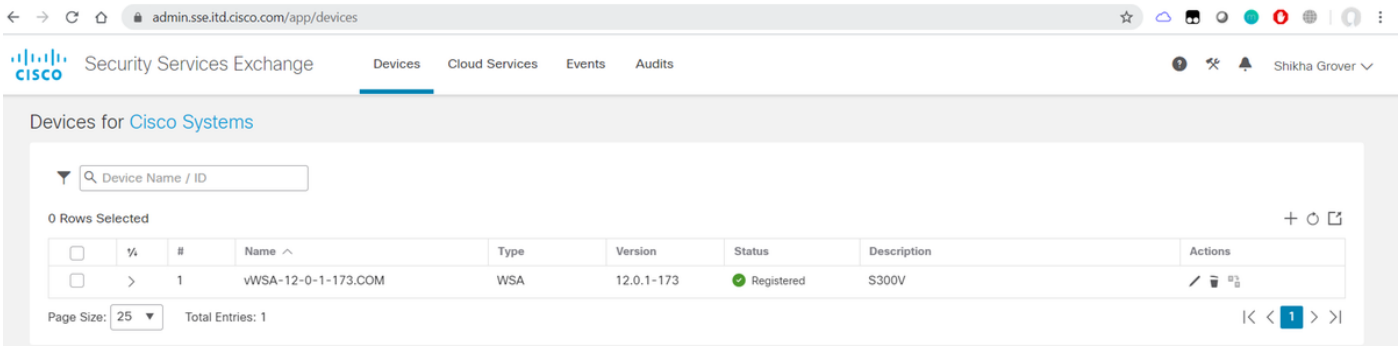


Schritt 3: Nach einigen Sekunden wird die Registrierung erfolgreich durchgeführt.

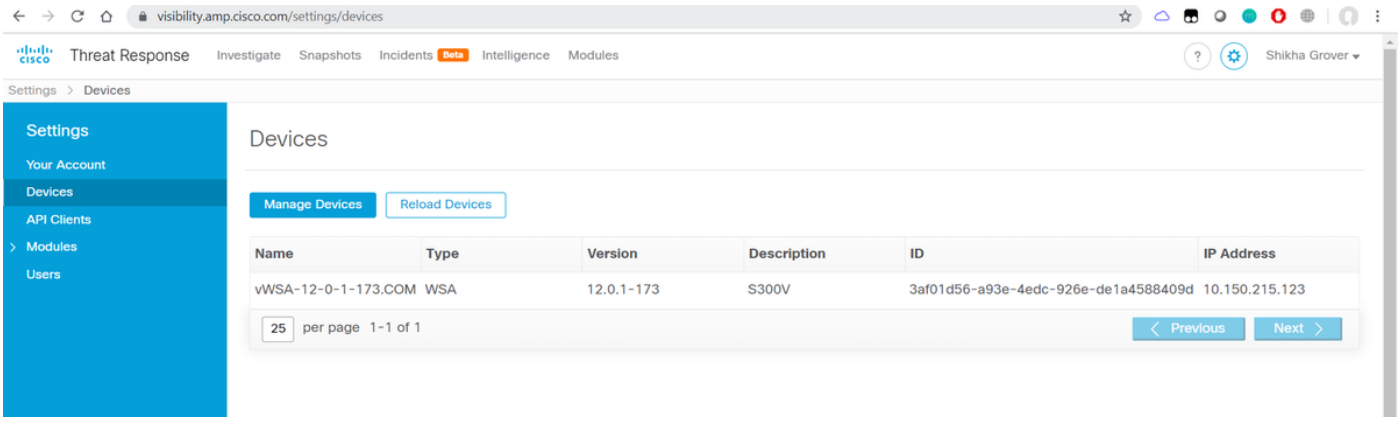
Vorsicht: Stellen Sie sicher, dass das generierte Token verwendet wird, bevor es abläuft.



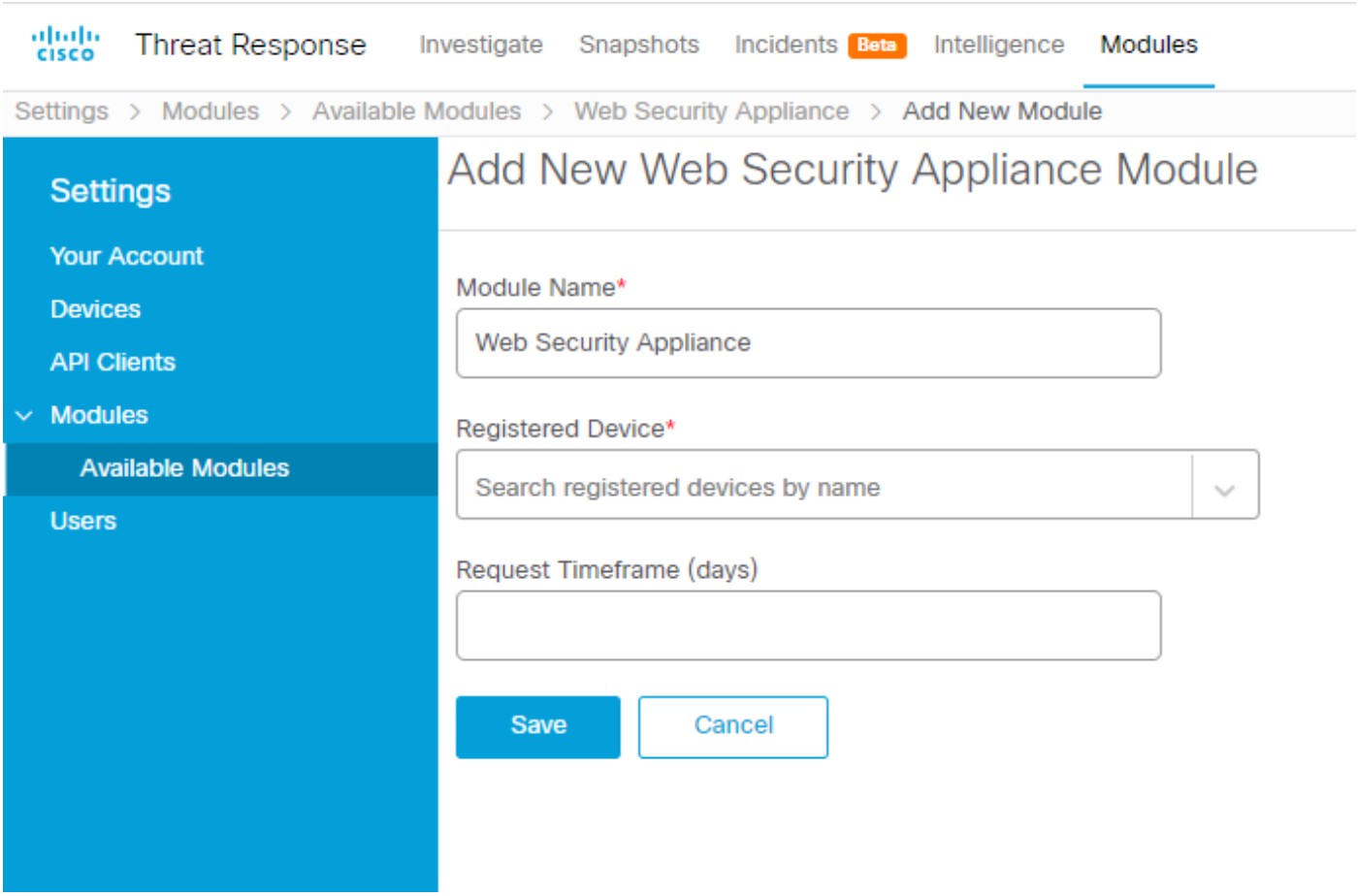
Schritt 4: Im SSE-Portal wird der Gerätestatus angezeigt.



Schritt 5: Im CTR-Portal wird das registrierte Gerät angezeigt.



Sie können dieses Gerät einem Modul zuordnen. Navigieren Sie zu **Module > Neues Modul hinzufügen > Websicherheits-Appliance**, wie im Bild gezeigt.



Das Gerät ist nun integriert. Sie können Datenverkehr von der WSA durchlaufen und Bedrohungen im CTR-Portal untersuchen.

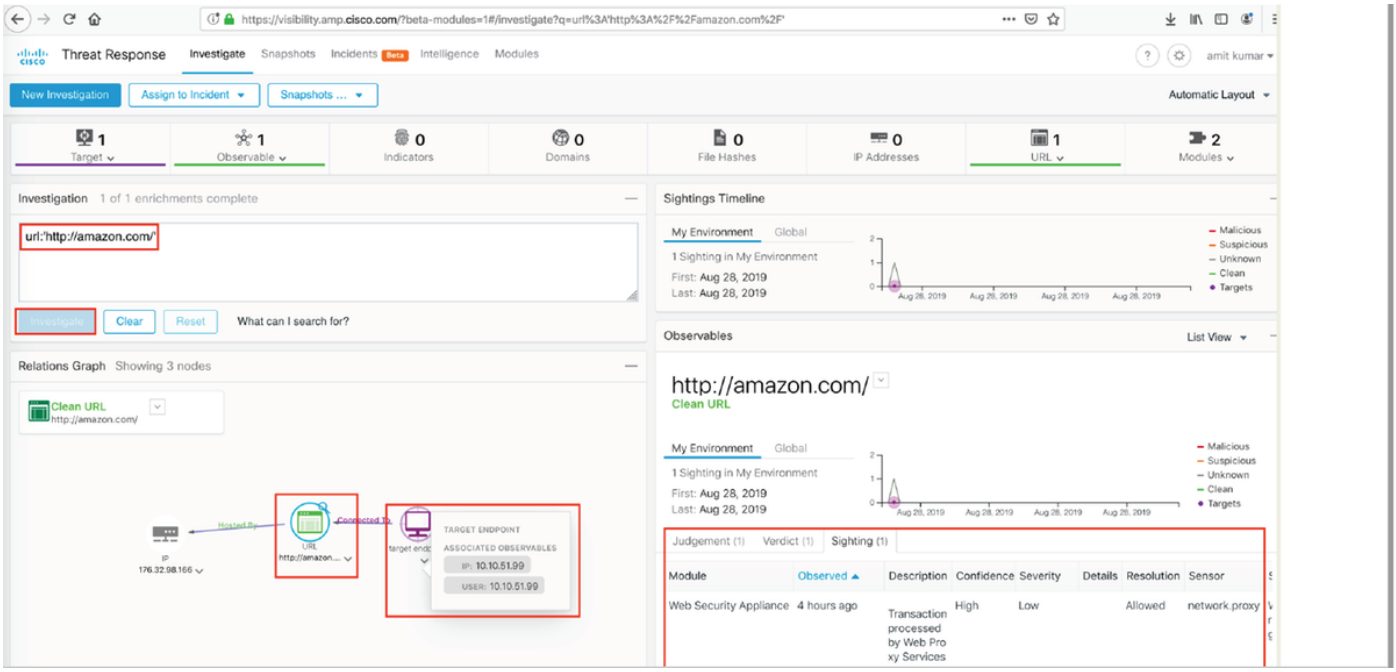
Überprüfen

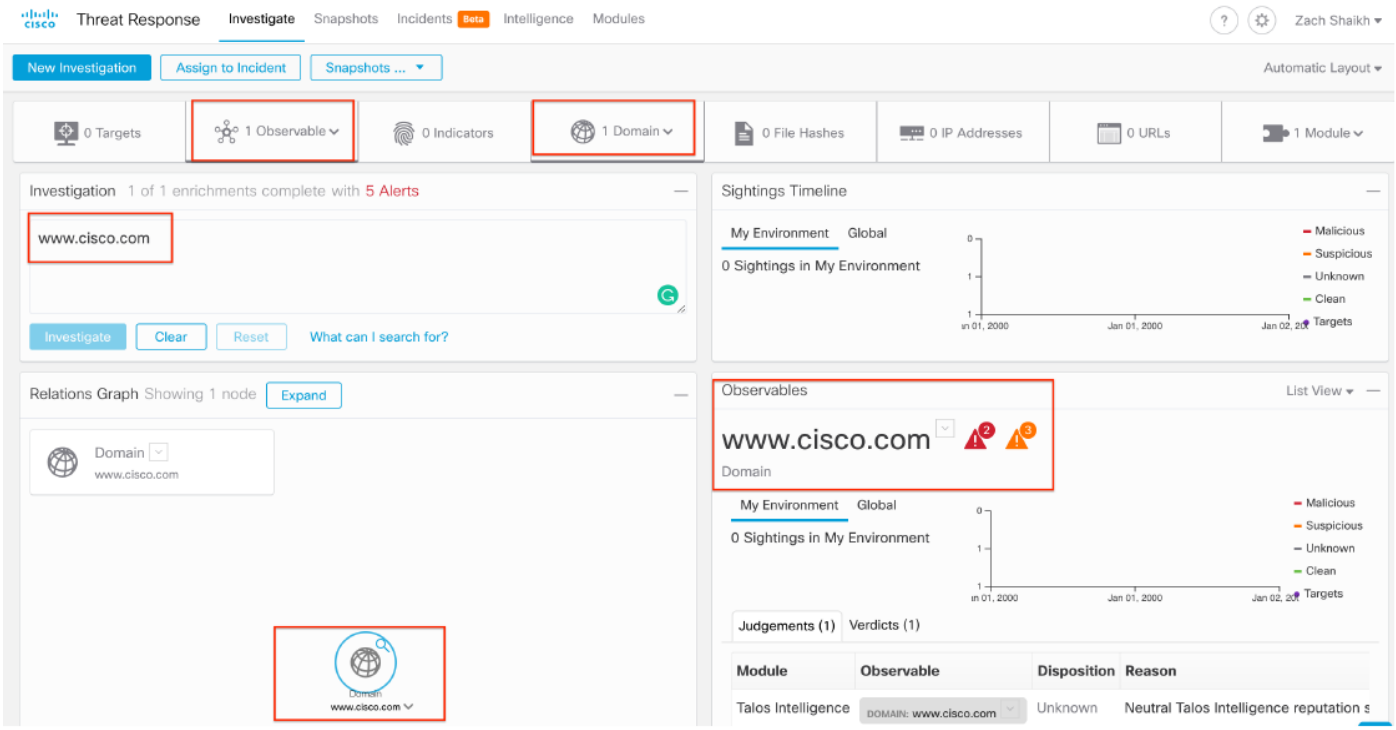
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Enrichments (Abfragen der WSA-Protokolle), verfügbar für das WSA-Modul und das unterstützte Format für die Ausführung der Abfrage vom CTR-Portal aus:

- Domäne - Domäne:"com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - IP:"172.217.26.164"
- Dateiname - Dateiname:"test.txt"

Als Beispiel werden Anreicherungen verwendet:





Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.
Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.
Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.
Bitte lassen Sie mich wissen, wenn ich etwas verpasst habe, das eingeschlossen werden sollte.