Integrazione di WSA con CTR

Sommario

Introduzione

In questo documento viene descritta la procedura per integrare Web Security Appliance (WSA) con il portale Cisco Threat Response (CTR).

Contributo di Shikha Grover e modificato da Yeraldin Sanchez Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- accesso WSA
- Accesso portale CTR
- Account di sicurezza Cisco

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Async Operating System versione 12.x o successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

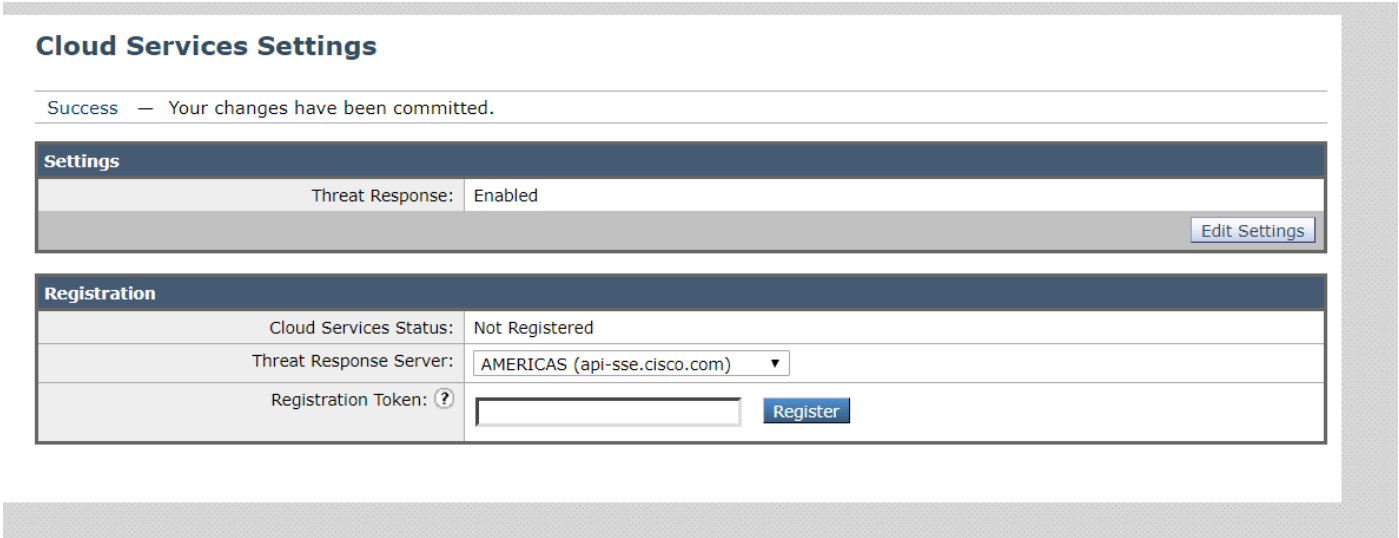
> **Attenzione:** Se si accede a CTR con un URL regionale per Asia Pacifico, Giappone e Cina (https://visibility.apjc.amp.cisco.com/), l'integrazione con l'accessorio non è attualmente supportata.

Passaggio 1. Abilitare **CTROBSERVABLE** in REPORTINGCONFIG nella CLI ed eseguire il commit delle modifiche, come mostrato nell'immagine.

```
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.
```

Passaggio 2. Configurare il portale cloud di Security Service Exchange (SSE), passare a **Rete > Impostazioni servizi cloud > Modifica impostazioni**, fare clic su **Abilita** e **invia**, come mostrato nell'immagine.

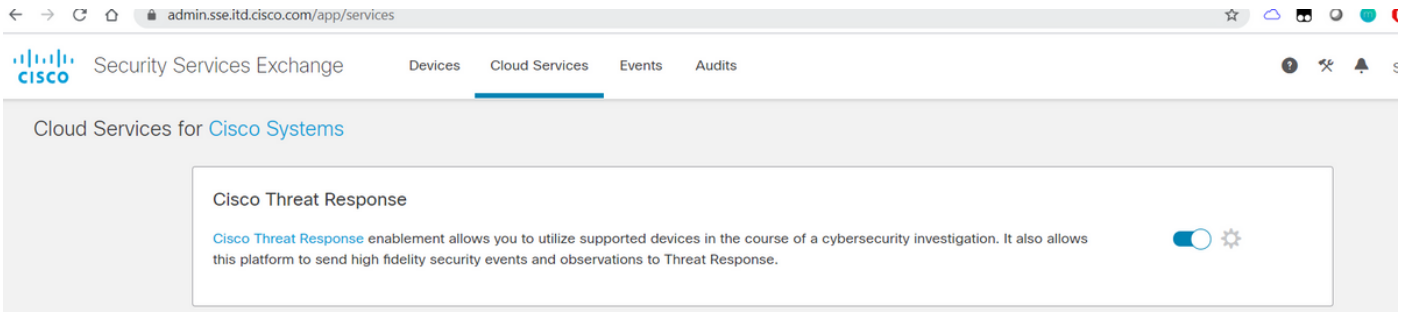
Scegliere il cloud in base alla posizione, come mostrato nell'immagine.



Passaggio 3. Se non si dispone di un account Cisco Security, è possibile creare un account utente nel portale Cisco Threat Response con diritti di accesso di amministratore.

Per creare un nuovo account utente, accedere alla pagina di accesso del portale Cisco Threat Response.

Passaggio 4. Abilitare Cisco Threat Response in Cloud Services sul portale SSE, come mostrato nell'immagine.



Passaggio 5. Verificare che WSA sia raggiungibile sulla porta 443 al portale SSE:

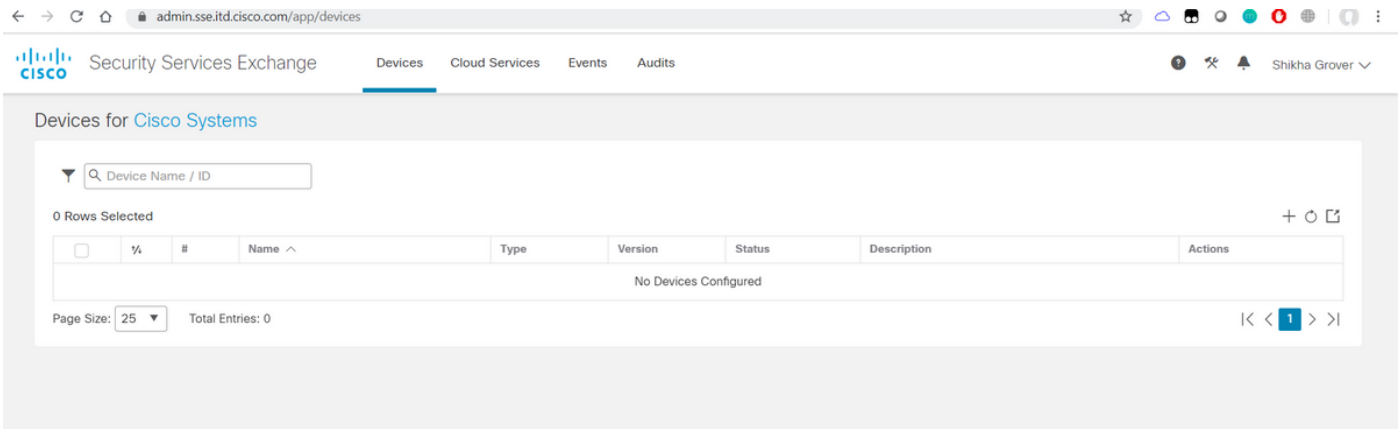
- api.eu.sse.itd.cisco.com (Europa)
- api-sse.cisco.com (America)

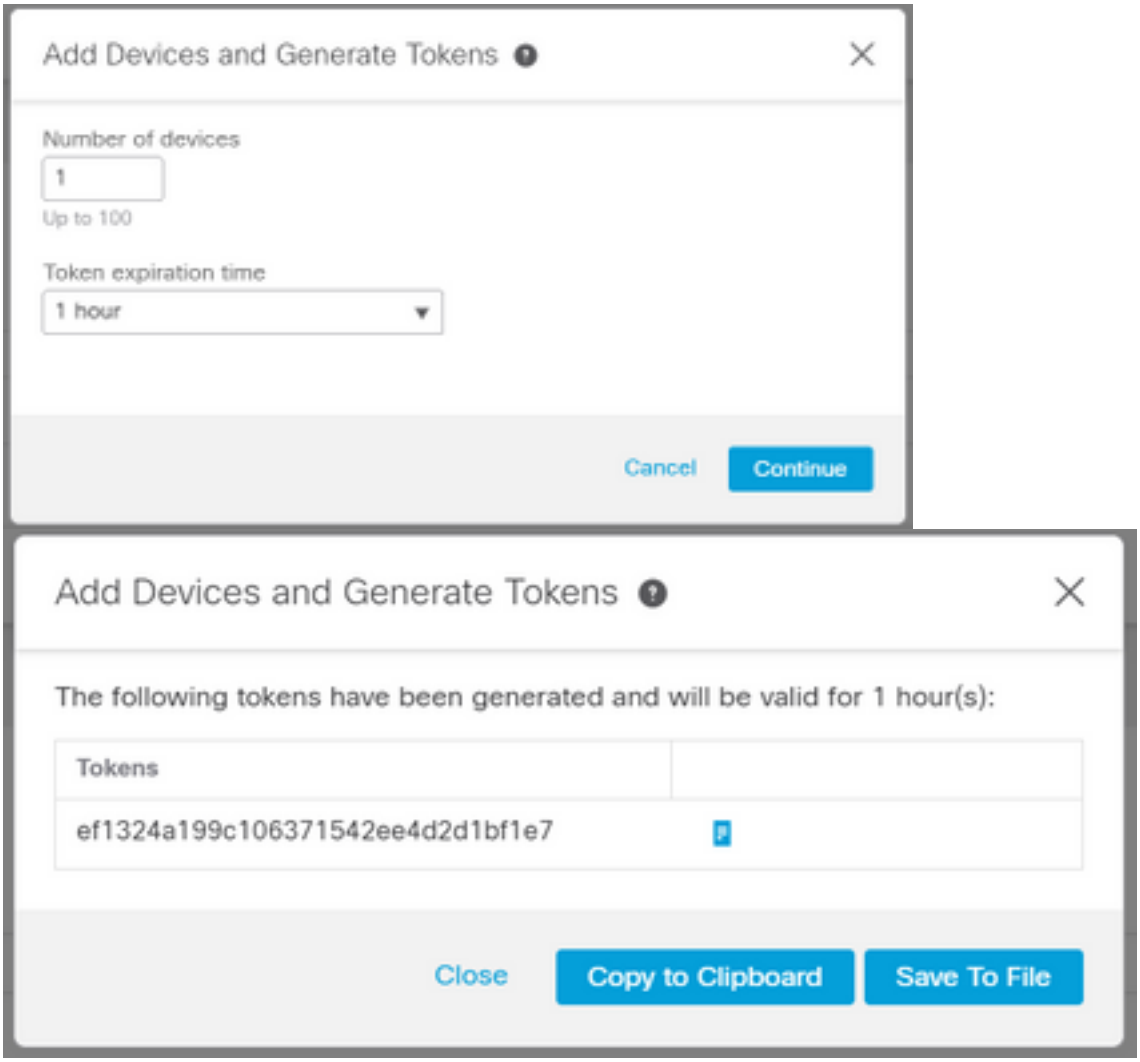
Registrazione dell'accessorio

Passaggio 1. Ottenere un token di registrazione dal portale SSE (Security Services Exchange) per registrare l'appliance nel portale Exchange dei servizi di sicurezza.

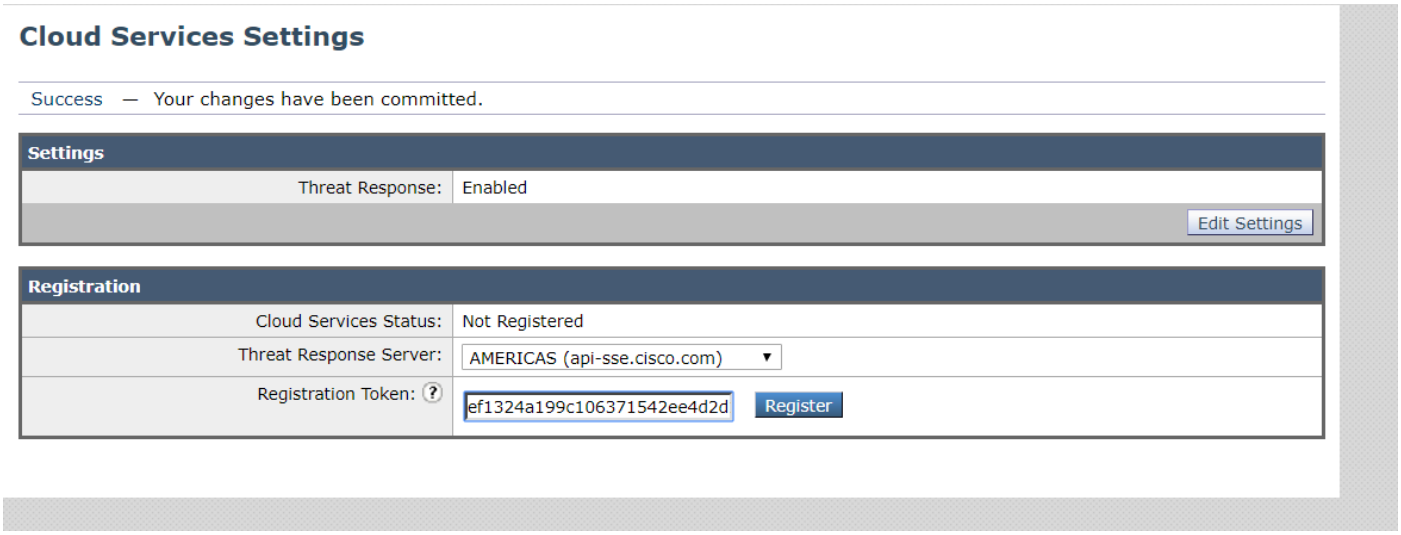
Il collegamento al portale SSE è https://admin.sse.itd.cisco.com/app/devices.

> **Nota:** Usa le credenziali dell'account CTR per accedere al portale SSE.



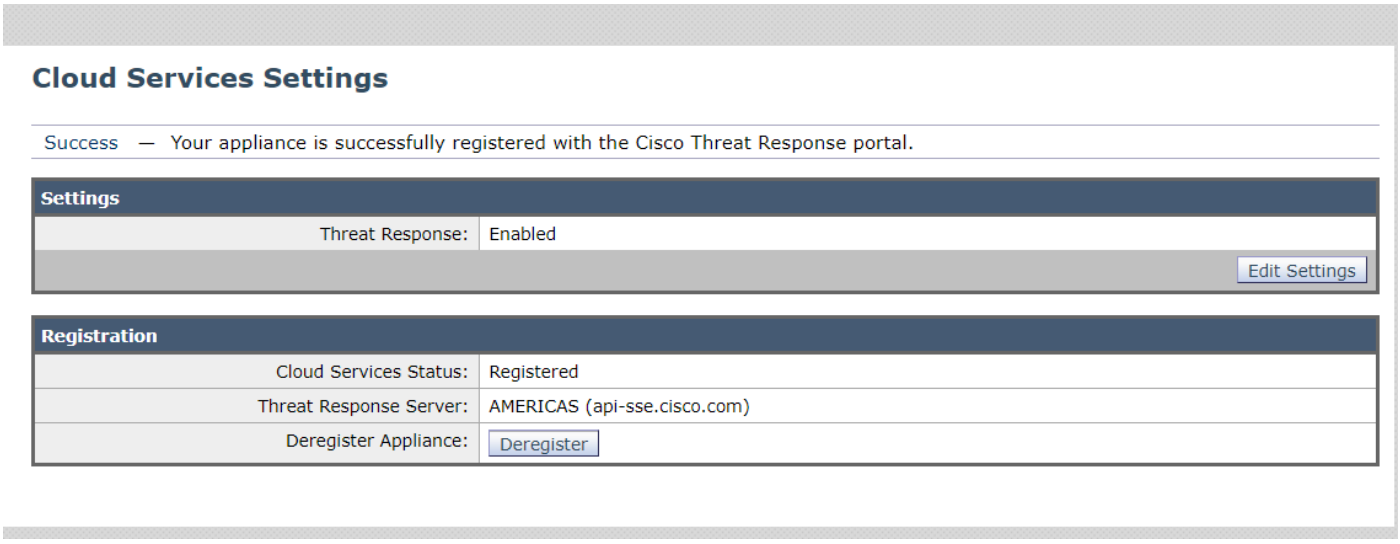


Passaggio 2. Immettere il token di registrazione ottenuto dal portale Security Services Exchange in WSA e fare clic su **Registra**, come mostrato nell'immagine.

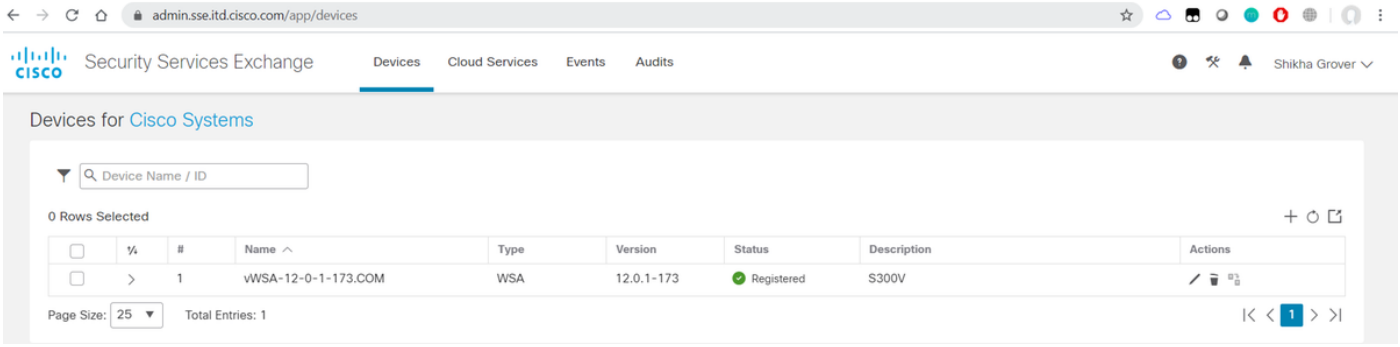


Passaggio 3. Dopo alcuni secondi, la registrazione è riuscita.

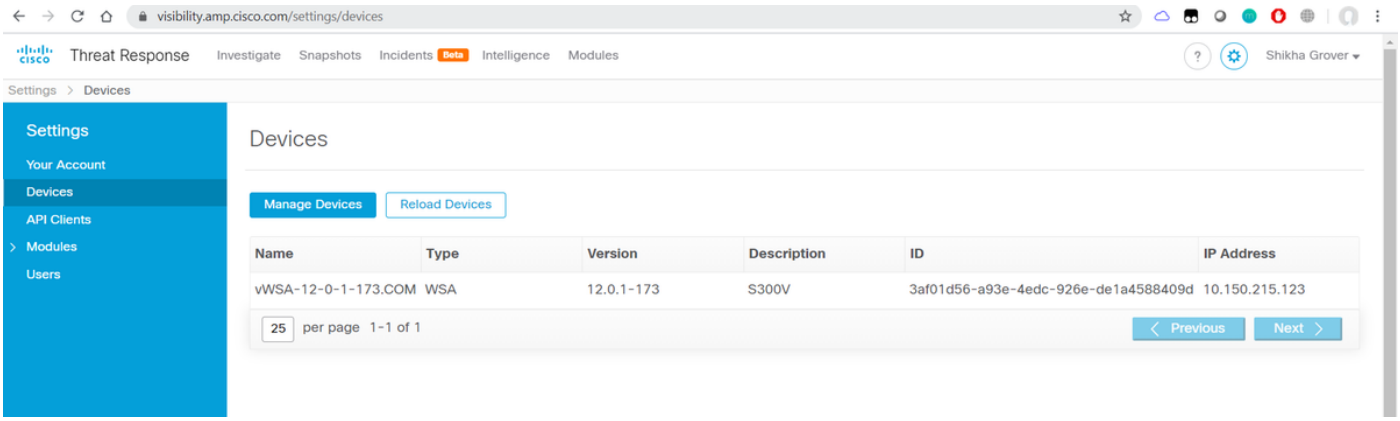
Attenzione: Assicurarsi che il token generato sia utilizzato prima della scadenza.



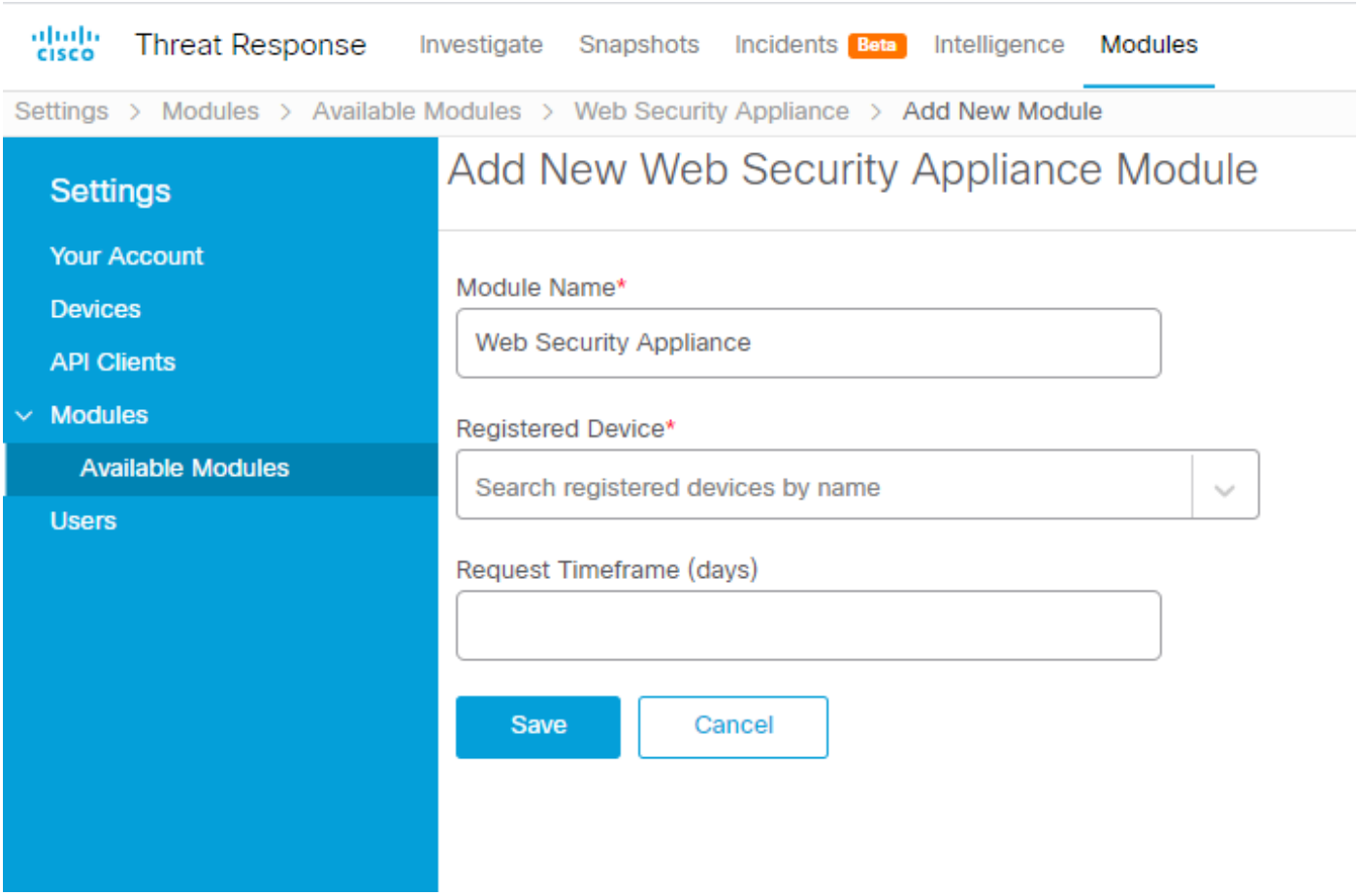
Passaggio 4. Sul portale SSE è possibile visualizzare lo stato del dispositivo.



Passaggio 5. Sul portale CTR appare il dispositivo registrato.



Èpossibile associare il dispositivo a un modulo, selezionare **Moduli > Aggiungi nuovo modulo > Web Security Appliance**, come mostrato nell'immagine.



Il dispositivo è ora integrato. Puoi passare attraverso il traffico dalla WSA e indagare sulle minacce sul portale CTR.

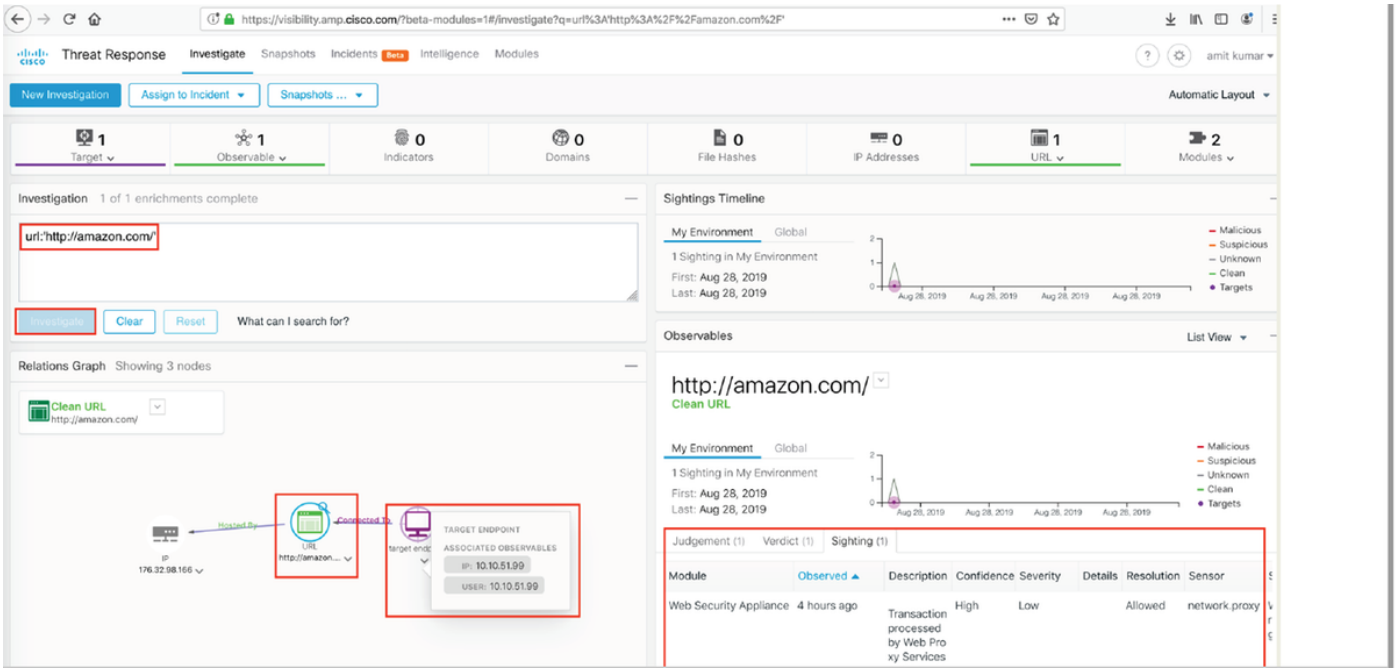
Verifica

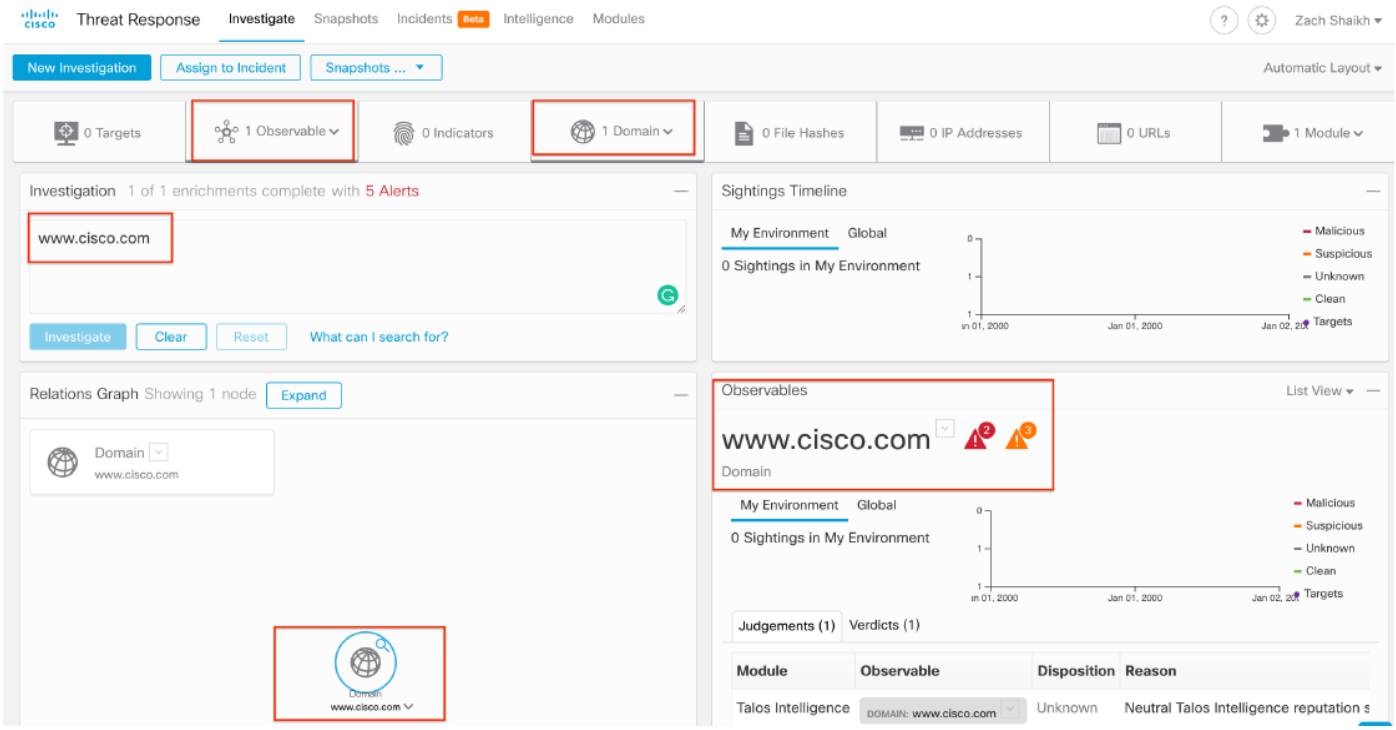
Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Enrichments(Query sui log WSA) disponibili per il modulo WSA e il formato supportato per l'esecuzione della query dal portale CTR:

- Dominio - dominio:"com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - ip:"172.217.26.164"
- Nome file - nome_file:"test.txt"

L'esempio dell'arricchimento utilizzato è il seguente:





Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso. Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso. Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso. Sentitevi liberi di farmi sapere se mi sono perso qualcosa che dovrebbe essere incluso.