

WSA와 CTR 통합

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[어플라이언스 등록](#)

[다음을 확인합니다.](#)

소개

이 문서에서는 WSA(Web Security Appliance)를 CTR(Cisco Threat Response) 포털과 통합하는 단계에 대해 설명합니다.

기고자: Shikha Grover, Yeraldin Sanchez Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WSA 액세스
- CTR 포털 액세스
- Cisco 보안 계정

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 비동기 운영 체제 버전 12.x 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

주의: 아시아 태평양, 일본 및 중국 URL(<https://visibility.apjc.amp.cisco.com/>)을 사용하여 CTR에 액세스하는 경우 어플라이언스와의 통합이 현재 지원되지 않습니다.

1단계. CLI의 REPORTINGCONFIG 아래에서 TROBSERVABLE을 활성화하고 이미지에 표시된 대

로 변경 사항을 커밋합니다.

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

Choose 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

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

Choose 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.
```

2단계. SSE(Security Service Exchange) 클라우드 포털을 구성하고 **Network(네트워크) > Cloud Services Settings(클라우드 서비스 설정) > Edit settings(설정 수정)**로 이동하고 이미지에 표시된 대로 **Enable and Submit(활성화 및 제출)**을 클릭합니다.

Cloud Services Settings

Settings	
Threat Response:	Enabled
Edit Settings	

이미지에 표시된 대로 위치에 따라 클라우드를 선택합니다.

Cloud Services Settings

Success — Your changes have been committed.

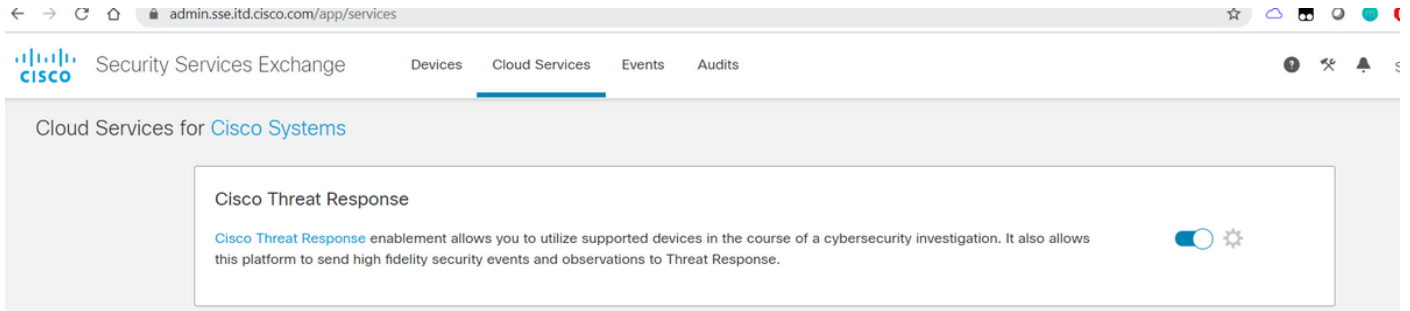
Settings	
Threat Response:	Enabled
Edit Settings	

Registration	
Cloud Services Status:	Not Registered
Threat Response Server:	AMERICAS (api-sse.cisco.com) ▼
Registration Token: ?	<input type="text"/> Register

3단계. Cisco Security 계정이 없는 경우 Cisco Threat Response 포털에서 관리자 액세스 권한을 가진 사용자 계정을 생성할 수 있습니다.

새 사용자 계정을 생성하려면 Cisco Threat Response 포털 [로그인 페이지](#)로 이동합니다.

4단계. 이미지에 표시된 대로 SSE 포털의 클라우드 서비스 아래에서 Cisco Threat Response를 활성화합니다.



5단계. WSA가 포트 443에서 SSE 포털에 연결할 수 있는지 확인합니다.

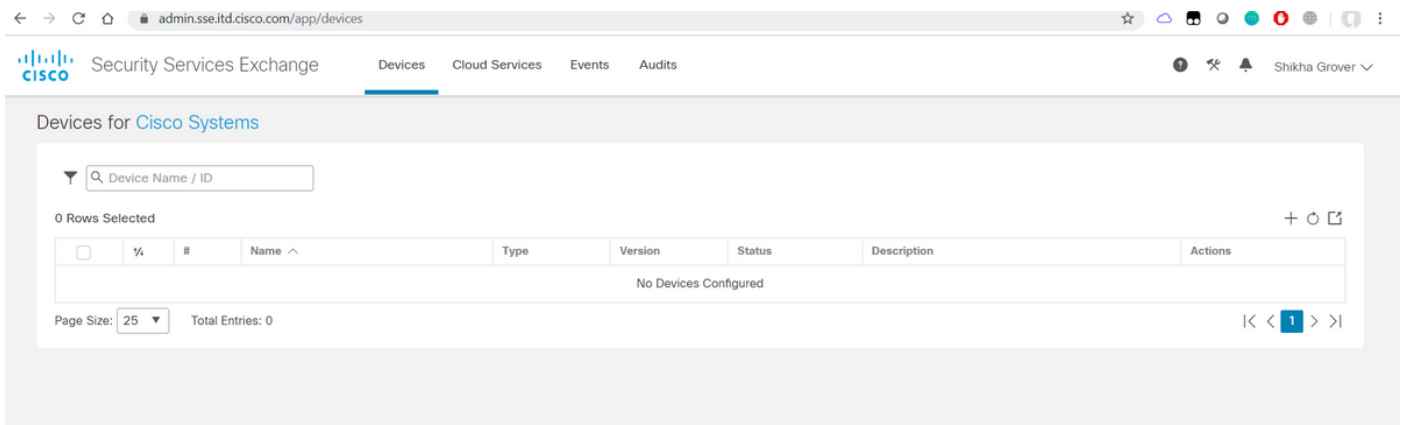
- api.eu.sse.itd.cisco.com(유럽)
- api-sse.cisco.com(미국)

어플라이언스 등록

1단계. SSE(Security Services Exchange) 포털에서 등록 토큰을 가져와 Security Services Exchange 포털에 어플라이언스를 등록합니다.

SSE 포털 링크는 <https://admin.sse.itd.cisco.com/app/devices>입니다.

참고:CTR 계정 자격 증명을 사용하여 SSE 포털에 로그인합니다.



Add Devices and Generate Tokens ?
✕

Number of devices

Up to 100

Token expiration time

Cancel
Continue

Add Devices and Generate Tokens ?
✕

The following tokens have been generated and will be valid for 1 hour(s):

Tokens	
ef1324a199c106371542ee4d2d1bf1e7	P

Close
Copy to Clipboard
Save To File

2단계. WSA의 Security Services Exchange 포털에서 가져온 등록 토큰을 입력하고 이미지에 표시된 대로 **Register**(등록)를 클릭합니다.

Cloud Services Settings

Success — Your changes have been committed.

Settings

Threat Response: Enabled

[Edit Settings](#)

Registration

Cloud Services Status: Not Registered

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

Registration Token: ?

ef1324a199c106371542ee4d2d

[Register](#)

3단계. 몇 초 후에 등록이 성공적으로 완료되었음을 확인할 수 있습니다.

주의: 생성된 토큰이 만료되기 전에 사용되는지 확인합니다.

Cloud Services Settings

Success — Your appliance is successfully registered with the Cisco Threat Response portal.

Settings

Threat Response: Enabled

Edit Settings

Registration

Cloud Services Status: Registered

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

Deregister Appliance: [Deregister](#)

4단계. SSE 포털에서 디바이스 상태를 볼 수 있습니다.

The screenshot shows the Cisco Security Services Exchange (SSE) portal. The browser address bar displays `admin.sse.itd.cisco.com/app/devices`. The page title is "Security Services Exchange" and the user is logged in as "Shikha Grover". The main heading is "Devices for Cisco Systems". Below this is a search bar for "Device Name / ID". A table lists the registered devices:

	%	#	Name ^	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	vWSA-12-0-1-173.COM	WSA	12.0.1-173	Registered	S300V	/ 🗑️ 🔍

Page Size: 25 Total Entries: 1

5단계. CTR 포털에 등록된 디바이스가 나타납니다.

The screenshot shows the Cisco Threat Response (CTR) portal. The browser address bar displays `visibility.amp.cisco.com/settings/devices`. The page title is "Threat Response" and the user is logged in as "Shikha Grover". The main heading is "Devices". Below this are "Manage Devices" and "Reload Devices" buttons. A table lists the registered devices:

Name	Type	Version	Description	ID	IP Address
vWSA-12-0-1-173.COM	WSA	12.0.1-173	S300V	3af01d56-a93e-4edc-926e-de1a4588409d	10.150.215.123

25 per page 1-1 of 1

이 장치를 모듈에 연결하고 이미지에 표시된 대로 **Modules > Add New Module > Web Security Appliance**로 이동할 수 있습니다.



Settings

Your Account

Devices

API Clients

▼ Modules

Available Modules

Users

Add New Web Security Appliance Module

Module Name*

Registered Device*

▼

Request Timeframe (days)

이제 디바이스가 통합되었습니다. WSA에서 트래픽을 전달하고 CTR 포털에서 위협을 조사할 수 있습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

CTR 포털에서 쿼리를 실행하기 위해 WSA 모듈에 사용 가능한 WSA 로그 쿼리 및 지원되는 형식:

- 도메인 - 도메인: "[com](#)"
- URL - url: "<http://www.neverssl.com>"
- SHA256 -
sha256: "8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872377999"
- IP - ip: "172.217.26.164"
- 파일 이름 - file_name: "test.txt"

그 예로,

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

New Investigation Assign to Incident Snapshots ... Automatic Layout

1 Target 1 Observable 0 Indicators 0 Domains 0 File Hashes 0 IP Addresses 1 URL 2 Modules

Investigation 1 of 1 enrichments complete

url: http://amazon.com/

Investigate Clear Reset What can I search for?

Relations Graph Showing 3 nodes

Clean URL http://amazon.com/

Hosted By Connected To

IP 176.32.98.166 URL http://amazon.com/ Target endpoint TARGET ENDPOINT ASSOCIATED OBSERVABLES IP: 10.10.51.99 USER: 10.10.51.99

Sights Timeline

My Environment Global

1 Sighting in My Environment

First: Aug 28, 2019 Last: Aug 28, 2019

Observables

http://amazon.com/ Clean URL

My Environment Global

1 Sighting in My Environment

First: Aug 28, 2019 Last: Aug 28, 2019

Judgement (1) Verdict (1) Sighting (1)

Module	Observed	Description	Confidence	Severity	Details	Resolution	Sensor
Web Security Appliance	4 hours ago	Transaction processed by Web Proxy Services	High	Low	Allowed	network proxy	

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

New Investigation Assign to Incident Snapshots ... Automatic Layout

0 Targets 1 Observable 0 Indicators 1 Domain 0 File Hashes 0 IP Addresses 0 URLs 1 Module

Investigation 1 of 1 enrichments complete with 5 Alerts

www.cisco.com

Investigate Clear Reset What can I search for?

Relations Graph Showing 1 node Expand

Domain www.cisco.com

Sights Timeline

My Environment Global

0 Sightings in My Environment

Observables

www.cisco.com Domain

My Environment Global

0 Sightings in My Environment

Judgements (1) Verdicts (1)

Module	Observable	Disposition	Reason
Talos Intelligence	DOMAIN: www.cisco.com	Unknown	Neutral Talos Intelligence reputation

포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오. 포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오. 포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오. 포함해야 할 항목이 누락되었는지 언제든지 알려 주십시오.