

WSAとCTRの統合

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[アプライアンスの登録](#)

[確認](#)

概要

このドキュメントでは、Webセキュリティアプライアンス(WSA)とCisco Threat Response(CTR)ポータルを統合する手順について説明します。

著者 : Shikha Grover、編集 : Yeraldin Sanchez Cisco TACエンジニア

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WSAアクセス
- CTRポータルアクセス
- シスコセキュリティアカウント

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Async Operating Systemバージョン12.x以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

注意：アジア太平洋地域、日本、中国のURL(<https://visibility.apjc.amp.cisco.com/>)を持つCTRにアクセスする場合、アプライアンスとの統合は現在サポートされていません。

ステップ1: 図に示すように、CLIでREPORTINGCONFIGの下のCTROBSERVABLEを有効にし、変更を確定します。

```
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
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.
]> 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.
```

ステップ2: Security Service Exchange (SSE)クラウドポータルを設定し、Network > Cloud Services Settings > Edit settingsに移動し、Enable and Submitをクリックします。

Cloud Services Settings

Settings	
Threat Response:	Enabled
Edit Settings	

図に示すように、ロケーションに応じてクラウドを選択します。

Cloud Services Settings

Success — Your changes have been committed.

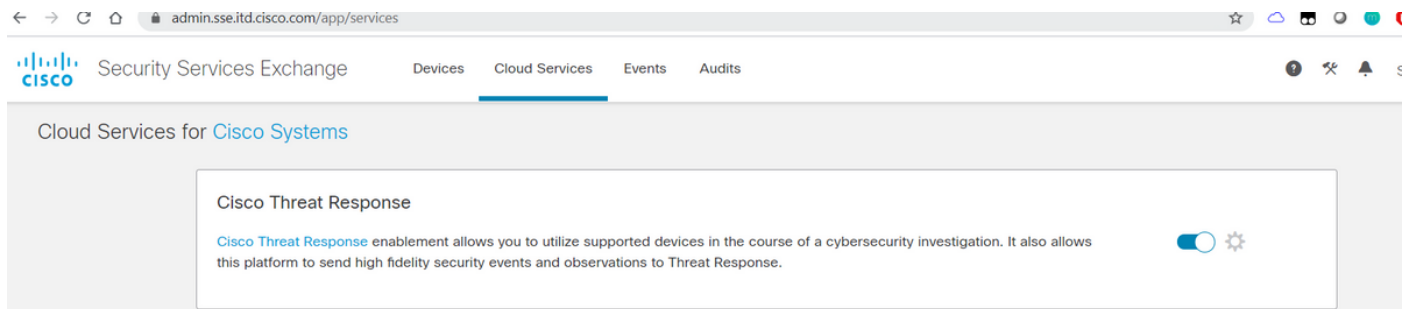
Settings	
Threat Response:	Enabled
Edit Settings	

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

ステップ3: Cisco Securityアカウントがない場合は、Cisco Threat Responseポータルで管理者アクセス権を持つユーザアカウントを作成できます。

新しいユーザアカウントを作成するには、Cisco Threat Responseポータルログインページに移動します。

ステップ4：図に示すように、SSEポータルのクラウドサービスでCisco Threat Responseを有効にします。



ステップ5：WSAがポート443からSSEポータルに到達できることを確認します。

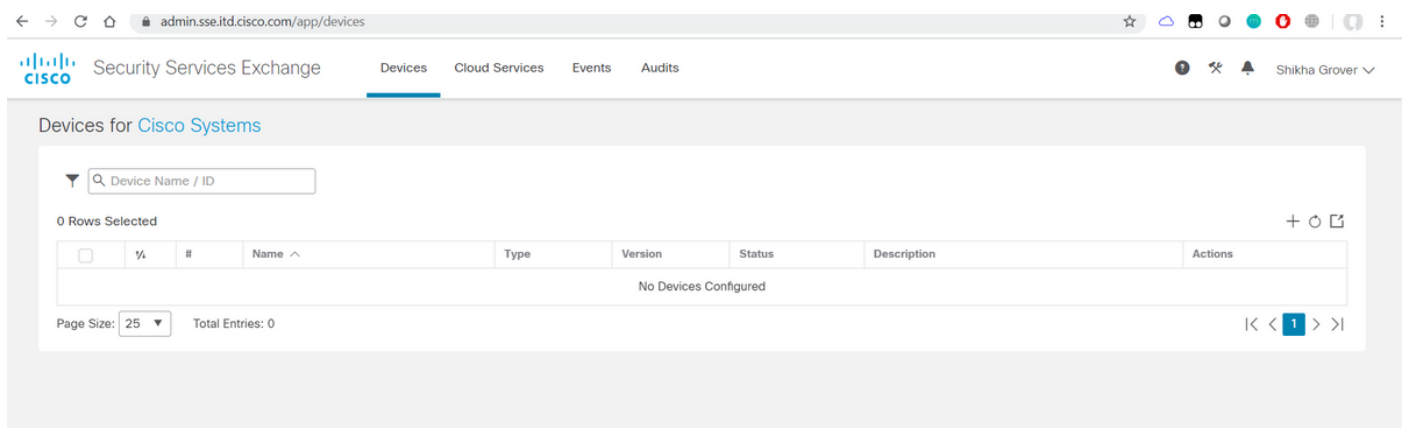
- api.eu.sse.itd.cisco.com (ヨーロッパ)
- api-sse.cisco.com (アメリカ)

アプライアンスの登録

ステップ1：セキュリティサービス交換(SSE)ポータルから登録トークンを取得し、セキュリティサービス交換ポータルにアプライアンスを登録します。

SSEポータルのリンクは<https://admin.sse.itd.cisco.com/app/devices>です。

注：CTRアカウントのクレデンシャルを使用してSSEポータルにログインします。



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](#)

ステップ2: WSAのSecurity Services Exchangeポータルから取得した登録トークンを入力し、図に示すように[Register]をクリックします。

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](#)

ステップ3: 数秒後、登録が成功したことが表示されます。

注意: 生成されたトークンが期限切れになる前に使用されていることを確認します。

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](#)

ステップ4:SSEポータルで、デバイスのステータスを確認できます。

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 "Devices for Cisco Systems". A search bar is present with the placeholder "Device Name / ID". Below the search bar, it indicates "0 Rows Selected". 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	/ 🗑️ 🔍

At the bottom, it shows "Page Size: 25" and "Total Entries: 1".

ステップ5:CTRポータルに登録されたデバイスが表示されます。

The screenshot shows the Cisco Threat Response portal. The browser address bar displays `visibility.amp.cisco.com/settings/devices`. The page title is "Threat Response". The left sidebar shows a navigation menu with "Settings" selected, and sub-items: "Your Account", "Devices", "API Clients", "Modules", and "Users". The main content area is titled "Devices" and contains two buttons: "Manage Devices" and "Reload Devices". Below the buttons is a table listing 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

At the bottom, it shows "25 per page" and "1-1 of 1".

このデバイスをモジュールに関連付け、図に示すように、[Modules] > [Add New Module] > [Web Security Appliance]に移動できます。



Settings
Your Account
Devices
API Clients
▼ Modules
Available Modules
Users

Add New Web Security Appliance Module

Module Name*

Registered Device*
 ▼

Request Timeframe (days)

デバイスが統合されました。WSAからのトラフィックをパススルーし、CTRポータルの特威を調査できます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

WSAモジュールで使用可能な富化 (WSAログの照会)、およびCTRポータルからクエリを実行するためのサポートされる形式 :

- ドメイン - ドメイン : "[com](#)"
- URL - url: "<http://www.neverssl.com>"
- SHA256 -
sha256: "8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - ip: "172.217.26.164"
- Filename - file_name: "test.txt"

例として使用される富化 :

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

Sightings 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

Domain

www.cisco.com

Sightings 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 s

含めるべき何かを見逃した場合は、ご連絡ください。含めるべき何かを見逃した場合は、ご連絡ください。含めるべき何かを見逃した場合は、ご連絡ください。含めるべき何かを見逃した場合は、ご連絡ください。