DevNet & Programmability テクニカルセッション

第6回　Cisco Security 製品APIご紹介

Satoshi Katayama
セキュリティ事業 コンサルティングシステムズエンジニア
2018/03/20

SBG supports API as of March 2018

Product	API	CRUD	Use Case
AMP4E	✓	✓	エンドポイントの一括グループ移動やイベントの取得など
Threat Grid	✓	✓	複数の検体を一括解析など
Cloud lock	–	–	N/A
Umbrella	✓	✓	複数ドメインリストの一括削除など
ESA	✓	✓	メール関連レポートを取得
CES	–	–	N/A
Firepower	✓	✓	ルールの設定やイベントログの抽出など
Meraki MX	✓	✓	ルールの設定など
ASA	✓	✓	ルールの設定など
ISE	✓	✓	人事システムと連携したID管理など
SWATCH	✓	–	Flow情報の長期保管、必要な情報のみの抽出、独自検索UIなど
WSA	–	–	N/A
CTA	✓	–	外部SIEMへTAXIIでの情報提供
PSIRT	✓	–	保有製品及びバージョンでCVE確認、OVAL取得など

AMP4E

Item	
Documents	https://api-docs.amp.cisco.com/api_versions?api_host=api.amp.cisco.com
Self Study Contents	n/a

Cisco AMP for Endpoints APIの使い方について – Cisco Support Community
https://supportforums.cisco.com/t5/%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3-%E3%83%89%E3%82%AD%E3%83%A5%E3%83%A1%E3%83%B3%E3%83%88/cisco-amp-for-endpoints-api%E3%81%AE%E4%BD%BF%E3%81%84%E6%96%B9%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6/ta-p/3220035

Threat Grid

Item	
Documents	https://panacea.threatgrid.com/doc/main/api-getting-started.html
Self Study Contents	DEVNET Learning Labs(**Cisco Threat Grid – Introduction to the Threat Grid API**) https://learninglabs.cisco.com/labs/tags/Security,Threat+Grid+API

Cloudlock

Item	
Documents	n/a
Self Study Contents	n/a

Umbrella

Item	
Documents	https://docs.umbrella.com/developer
Self Study Contents	DEVNET Learning Labs

ESA

Item	
Documents	https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-programming-reference-guides-list.html
Self Study Contents	n/a

https://www.cisco.com/c/en/us/td/docs/security/esa/esa_all/esa_api/b_ESA_API_Getting_Started_Guide/b_ESA_API_Getting_Started_Guide_chapter_00.html#con_1092467
情報の取得は可能だが、アップデート等に関しては基本的にサポートしておらず

CES (API not provided for customer)

Item	
Documents	https://www.cisco.com/c/ja_jp/support/docs/security/cloud-email-security/209696-CES-How-can-I-use-AsyncOS-API.html
Self Study Contents	n/a

Firepower

Item	
Documents	https://www.cisco.com/c/en/us/support/security/defense-center/products-programming-reference-guides-list.html
Self Study Contents	DEVNET Learning Labs

Meraki MX

Item	
Documents	https://dashboard.meraki.com/api_docs#mx-l3-firewall
Self Study Contents	n/a

ASA

Item	
Documents	https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html#id_44480
Self Study Contents	n/a

ISE

Item	
Documents	https://communities.cisco.com/docs/DOC-66297
Self Study Contents	https://<ise ip address>:9060/ers/sdk

下記にはほとんど情報なく、筐体のsdk参照。
https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/api_ref_guide/api_ref_book.html

SWATCH

Item	
Documents	https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-programming-reference-guides-list.html
Self Study Contents	https://developer.cisco.com/docs/stealthwatch/

Flow Collectorにたまっていくフローログそのものをパースしてライブストリームで取得可能。
https://github.com/CiscoDevNet/stealthwatch-data-exporter

WSA

Item	
Documents	–
Self Study Contents	–

Anti-Malware and Reputationの設定のみで、WSA本体に対するAPIは無い。
https://www.cisco.com/c/ja_jp/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01110.html#task_2260707

CTA

Item	
Documents	https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_0100011.html
Self Study Contents	n/a

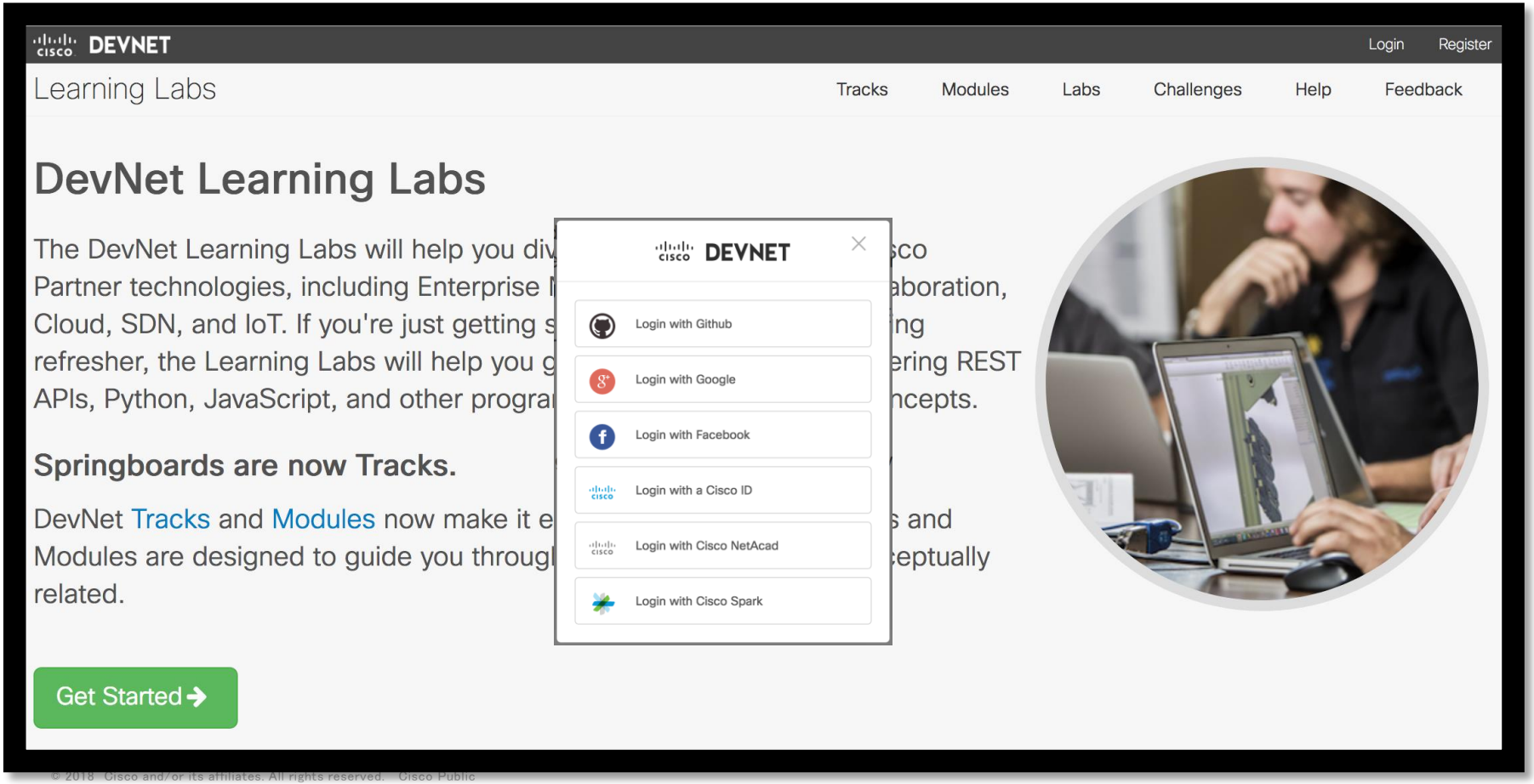
Splunk等のSIEMに脅威情報をTAXIIで連携する仕組み
https://github.com/CiscoCTA/taxii-log-adapter/wiki/Integration-with-Splunk

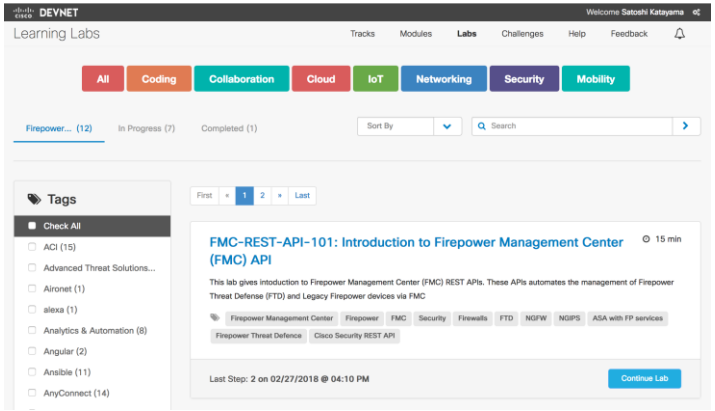
PSIRT

Item	
Documents	https://developer.cisco.com/site/PSIRT/discover/overview/
Self Study Contents	https://developer.cisco.com/site/PSIRT/get-started/getting-started.html

DEVNET Learning Labs
Firepowerラボを触ってみましょう

https://learninglabs.cisco.com/



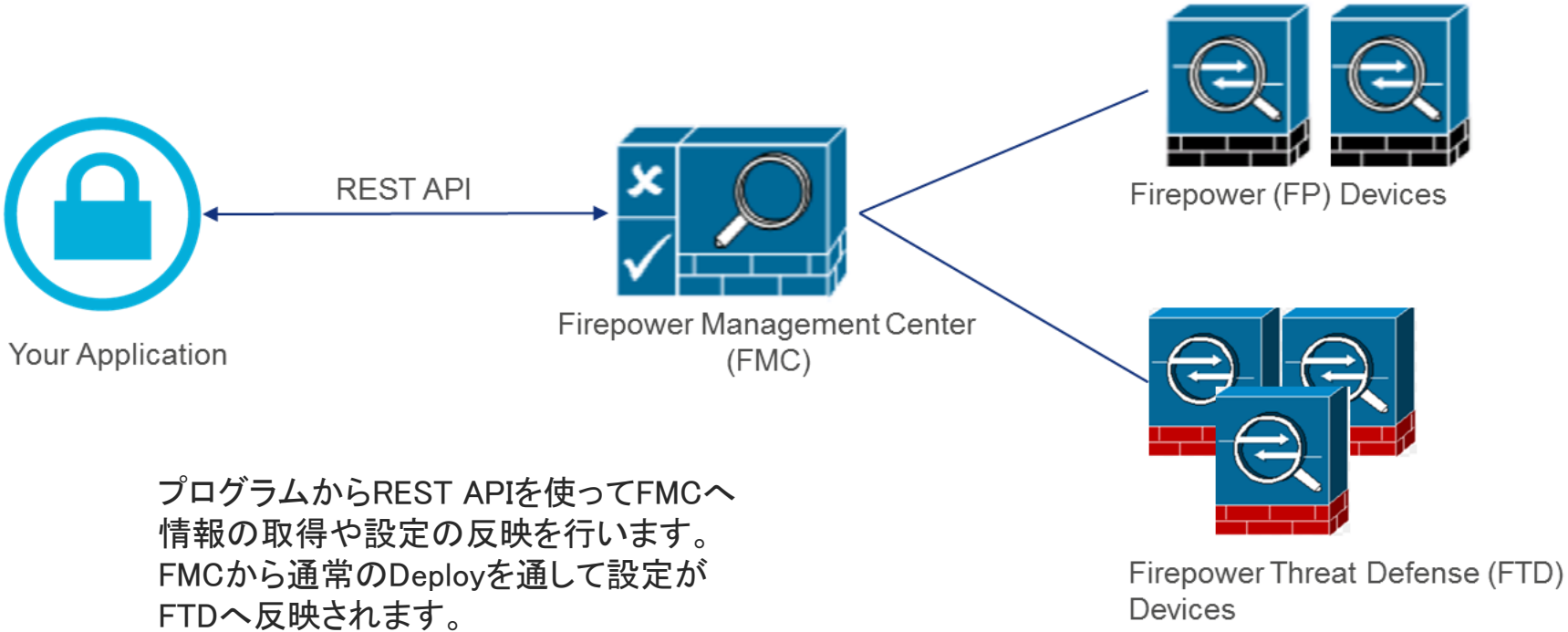


TagsからFirepowerをチェックしてフィルタします

FMC-REST-APIラボも充実しています

- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**
- **FMC-REST-API-102: FMC REST api authentication and access**
- **FMC-REST-API-103: Add/register a device to Firepower Management Center (FMC)**
- **FMC-REST-API-104: FMC REST api REQUEST AND RESPONSE structures and error codes**
- **FMC-REST-API-105: Debugging the FMC REST API errors**
- **FMC-REST-API-106: FMC object(s) and CRUD operations using REST API**
- **FMC-REST-API-107: Firewall Policy fundamentals and Policy CRUD**
- **FMC-REST-API-109: Creating a Threat Centric AC Policy using the FMC REST API**
- **FMC-REST-API-110: Using evenstreamer API to identify a potentially compromised host**
- **FMC-REST-API-111: Cisco Threat Intelligence Director (TID) APIs and their usage via API Explorer and Postman**
- **FMC-REST-API-112: Introduction to Firepower Management Center (FMC) API CRUD operations**
- **Firepower eStreamer and Splunk: Learn to create custom Splunk App that visualize threat data using Firepower Management Center (FMC) eStreamer API**

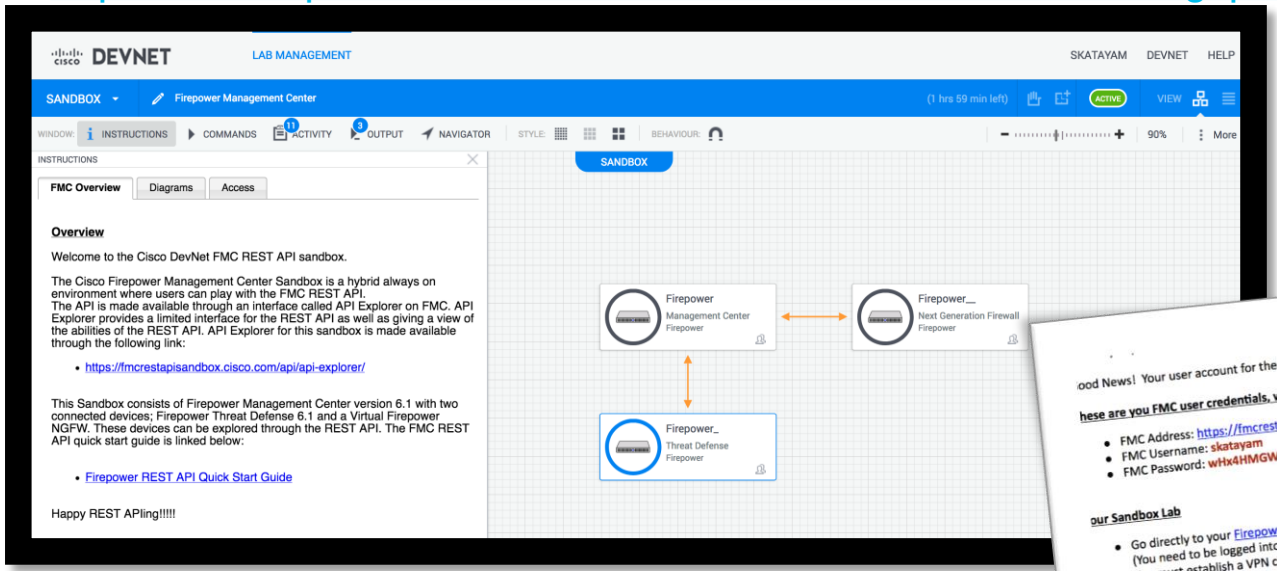
- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**



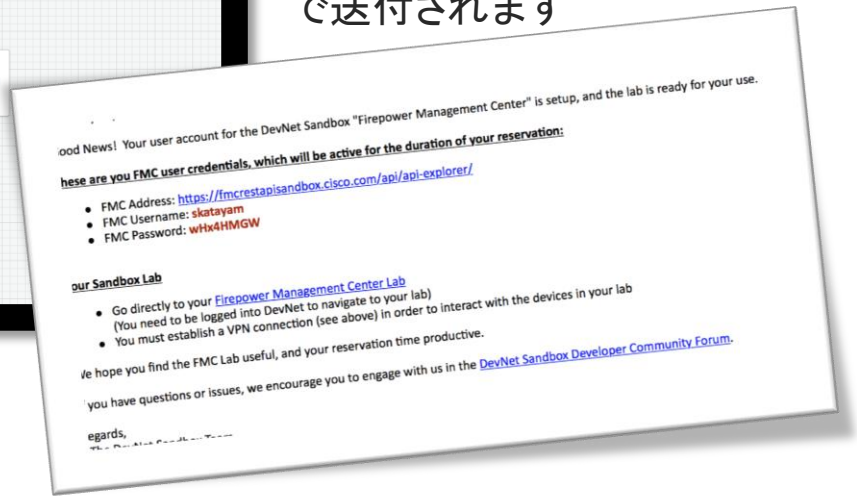
プログラムからREST APIを使ってFMCへ
情報の取得や設定の反映を行います。
FMCから通常のDeployを通して設定が
FTDへ反映されます。

- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**

FMCサンドボックスが用意されていますのでそちらを使うこともできます。
サンドボックスを利用するには予め予約が必要です。
https://developer.cisco.com/site/devnet/sandbox/docs/index.gsp#security/overview



サンドボックス予約が完了するとID/PWがメールで送付されます


ood News! Your user account for the DevNet Sandbox "Firepower Management Center" is setup, and the lab is ready for your use.

hese are you FMC user credentials, which will be active for the duration of your reservation:

- FMC Address: https://fmcrestapisandbox.cisco.com/api/api-explorer/
- FMC Username: skatayam
- FMC Password: wHx4HMGW

our Sandbox Lab

- Go directly to your Firepower Management Center Lab
  (You need to be logged into DevNet to navigate to your lab)
- You must establish a VPN connection (see above) in order to interact with the devices in your lab

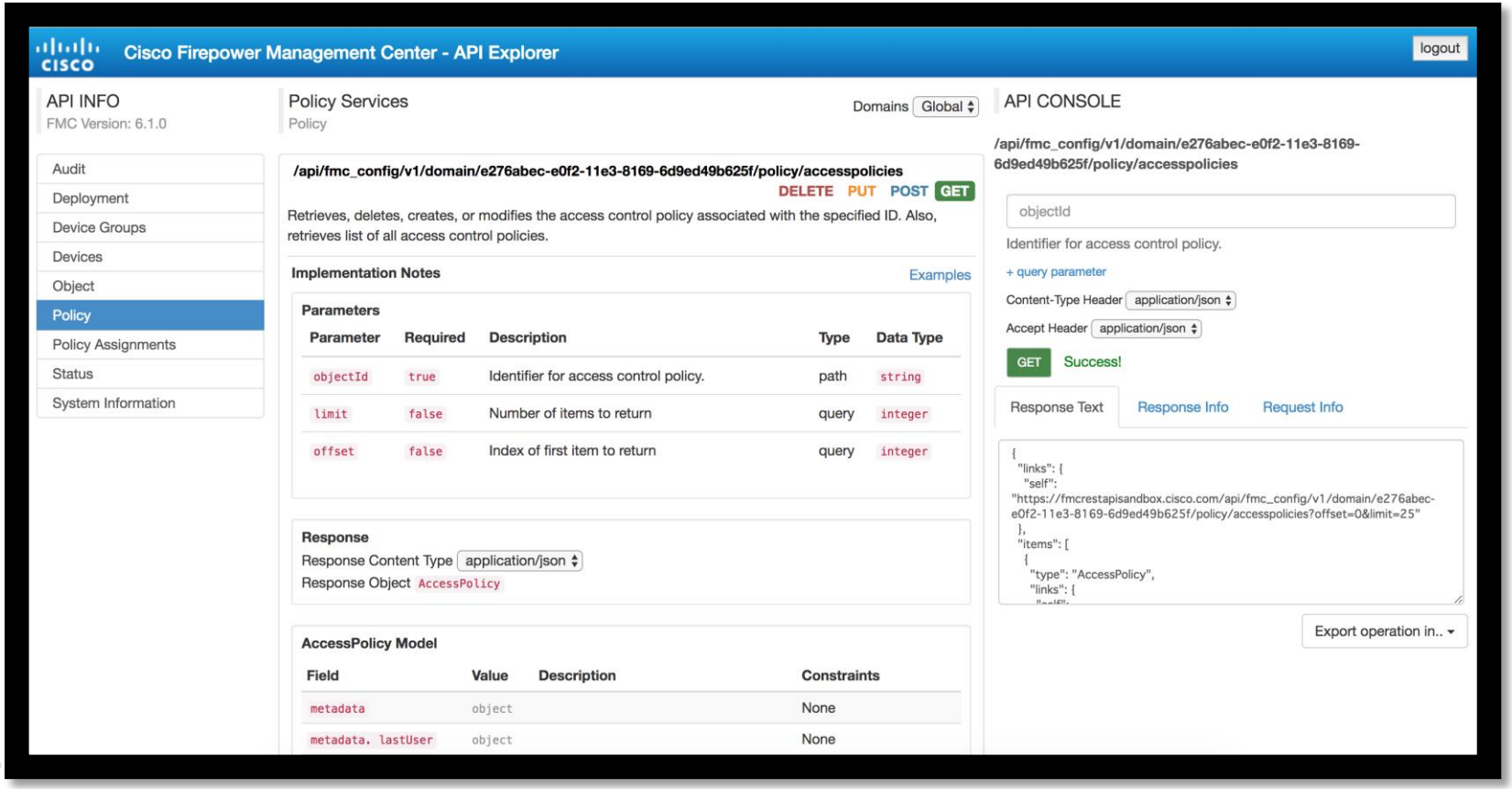
Ve hope you find the FMC Lab useful, and your reservation time productive.

you have questions or issues, we encourage you to engage with us in the DevNet Sandbox Developer Community Forum.

egards,

- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**

予約することで送付されたメールに記載あるID/PWにてAPIエクスプローラーにログイン



- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**

APIコンソールからACPをGETした結果と実際のFMC上のAPC

API CONSOLE

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies

objectId

Identifier for access control policy.

+ query parameter

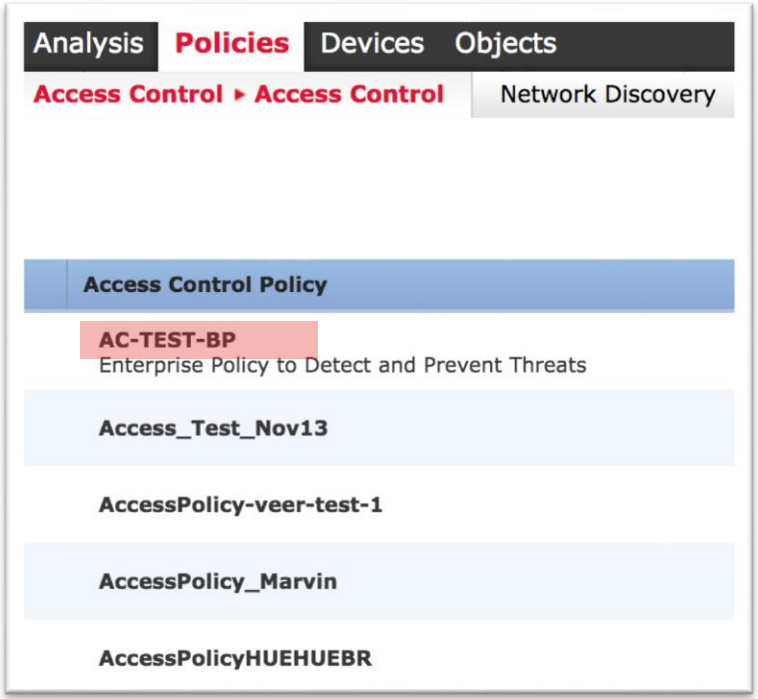
Content-Type Header application/json

Accept Header application/json

GET Success!

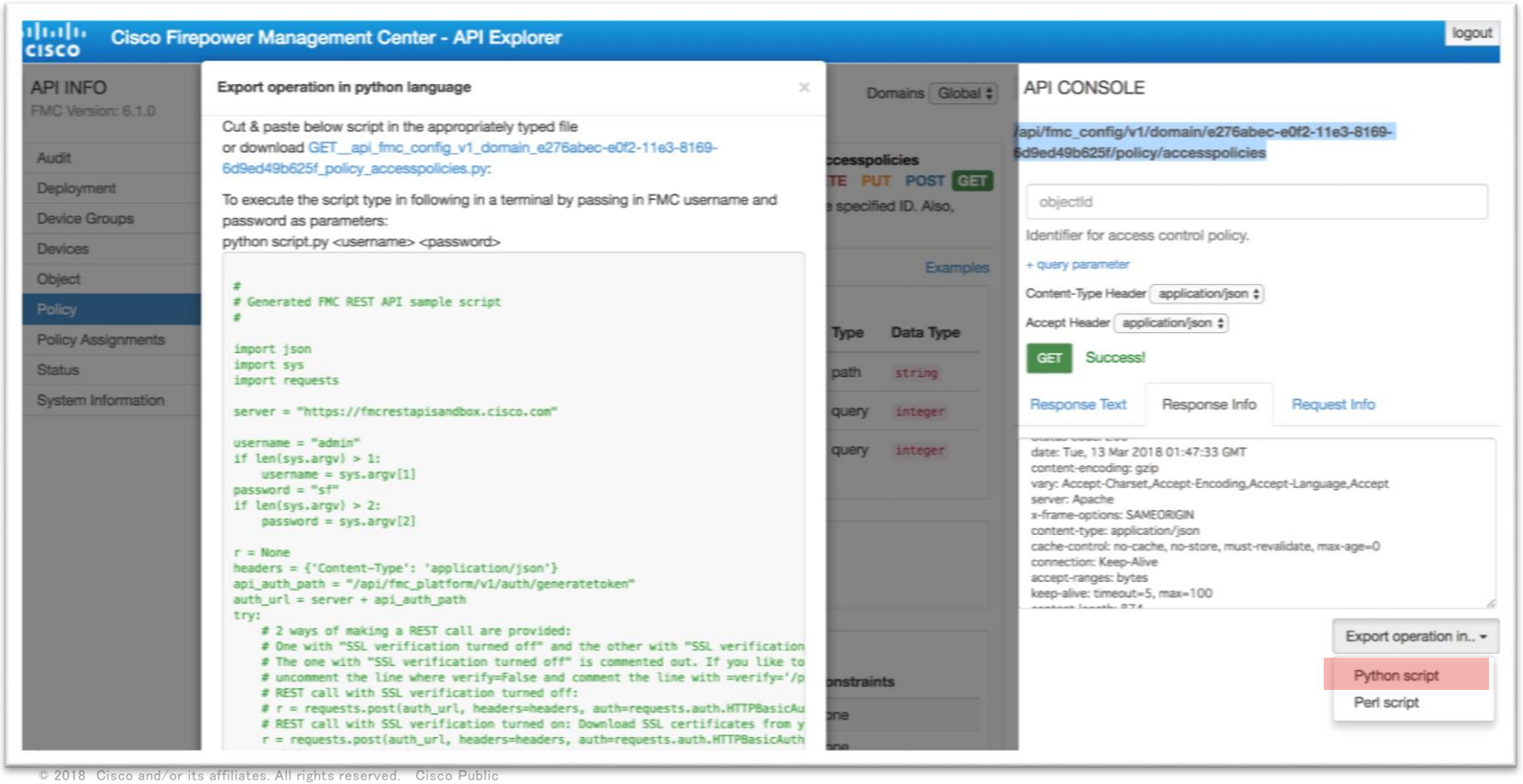
Response Text | Response Info | Request Info


```
{
  "type": "AccessPolicy",
  "links": {
    "self":
"https://fmcrestapisandbox.cisco.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/005056BB-0B24-0ed3-0000-266287972781"
  },
  "name": "AC-TEST-BP",
  "id": "005056BB-0B24-0ed3-0000-266287972781"
},
```

- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**

APIコンソールの実行サンプルスクリプトを入手も可能



まとめ

- 多くのシスコセキュリティ製品がAPIを公開しております。
- セルフスタディにはDEVNET Learning Labsがオススメです。
- サンプルスクリプトをカスタムして自分なりに使い勝手のいいものを作り上げることが近道です。
- 標準機能だけでは満たせない要件をAPI利用することで実現できた時のエンジニアとして達成感もあります（本来メーカーが対応すべきという意見はさておき。。。）
- APIを駆使して考えも見なかった新しい価値を創造できればエンジニアとしての価値はプライスレス。


CISCO