

CISCO
SECURE

SecureX

workflow how to guide

シスコシステムズ合同会社

SecureX workflow project team

2023/06

本資料について

- 本ガイドを進めるにあたり、以下のアカウントが必要になりますので、予めご準備ください。
 - SecureX
 - Umbrella
 - Webex
- 本ガイドは、SecureXの初学者向けで、Workflowを動かしたことがない人でもスライド通りに操作していけば動かせるように作成されています。(ハンズオンのパートは1~2時間程度のボリュームとなります)
- 2023年6月時点でSecureXはまだUmbrellaのnew APIは非サポートとなっておりますが、今後サポートされる前提で作成されています。
 - Umbrella New APIについて(<https://community.cisco.com/t5/-/-/ta-p/4684042#toc-hId-1386194768>)
- 本ガイドに記載されている仕様および製品に関する情報は、2023年6月時点のものとなり、予告なしに変更されることがあります。
- シスコは、本ガイドに関してその正確性または完全性について一切の責任を負わないこととします。

Umbrella アカウントを持っていない場合 (Devnet Sandboxの利用)

- Devnet Sandboxとは？

- Cisco製品が手元になくてもAPIなどを使った開発や実験を行える無料のクラウド型サンドボックス

- <https://developer.cisco.com/site/sandbox/>

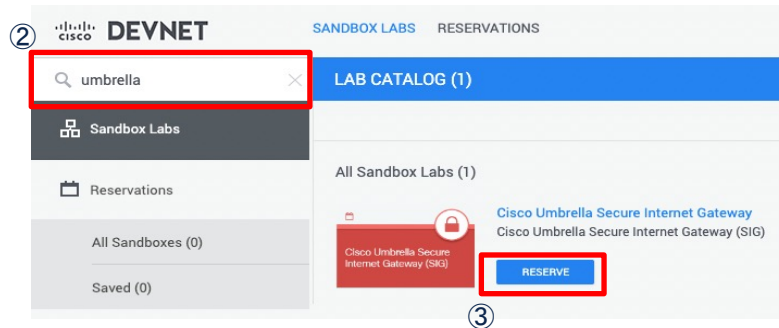
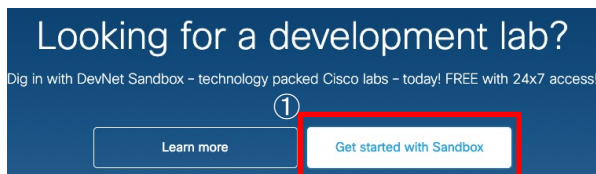
- Devnet Sandbox日本語解説

- <https://community.cisco.com/t5/-/-/ta-p/4043967>

②左上の検索ボックスで“umbrella”と入力し検索

③表示された“Cisco Umbrella Secure Internet Gateway”の“RESERVE”をクリック
あとは日本語解説の通り進める
(しばらくすると送られてくるメールにログイン情報など詳しい記載がございます)

①“Get started with Sandbox”をクリック



Agenda



1. 構成要素(画面の項目と意味)
2. モデルケースについて
3. ワークフロー事前準備&設定
4. Trigger
5. No Code開発
6. Logic

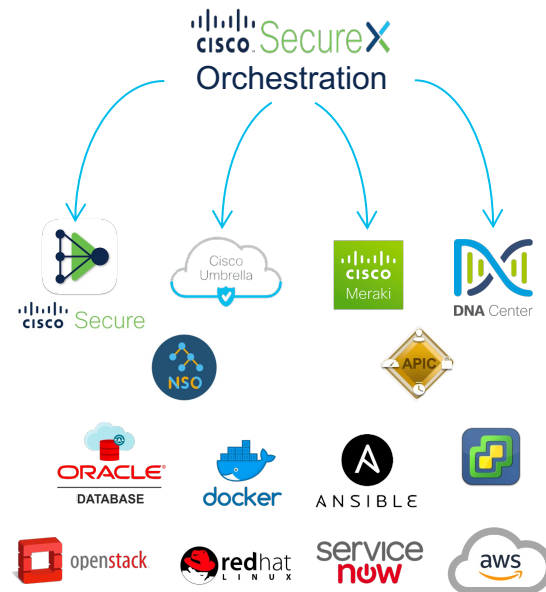


1. 構成要素 (画面の項目と意味)

SecureX Orchestrationとは

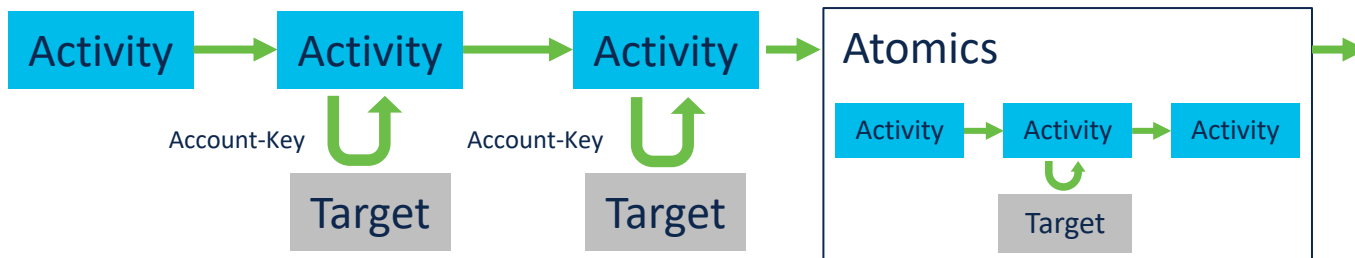
SecureX Orchestrationは、モダン、Next-Generation、Cross-Domain、Technology-Agnosticなオーケストレーション&オートメーションプラットフォーム、no-to-low-code GUI アプローチによりハイパフォーマンス、スケーラブルなプロセスオートメーションを実現：**エキスパートオートメーションをシンプルに**

 調査	 自動化	 統合	 スケール
マシンスピードで実行するワークフローによりリサーチとレスポンスにかかる時間を短縮	反復的タスクを自動化し、MTTR (平均修復時間) を削減することで、生産性を大幅に向上させ、ミッションクリティカルなプロジェクトに集中できる	Out of Band アダプタを利用して外部システムと迅速に統合、Toolbox を拡張できる独自の統合モデル	無限に拡張、休む間もなく、24時間同じSLAを提供できるオートメーション



WorkFlowとは？

WorkFlow = SecureX Orchestrationにより、自動化された一連の作業



主な構成要素：

- Activities: 基本的な処理(例. Umbrellaにアクセス, 変数定義, 条件分岐...)
- Targets: Activityの実行対象となる相手 (例. Umbrella, Webex, など)
- Account-Keys: Targetにアクセスする時の認証情報
- Atomics(or Atomic Actions): WorkFlowから実行できる、小さなWorkFlow (プログラミング経験のある人ならば、関数だと思えばOK)

Orchestration画面 構成要素

SecureX Dashboard Integration Modules **Orchestration** In

SecureX Orchestration Beta

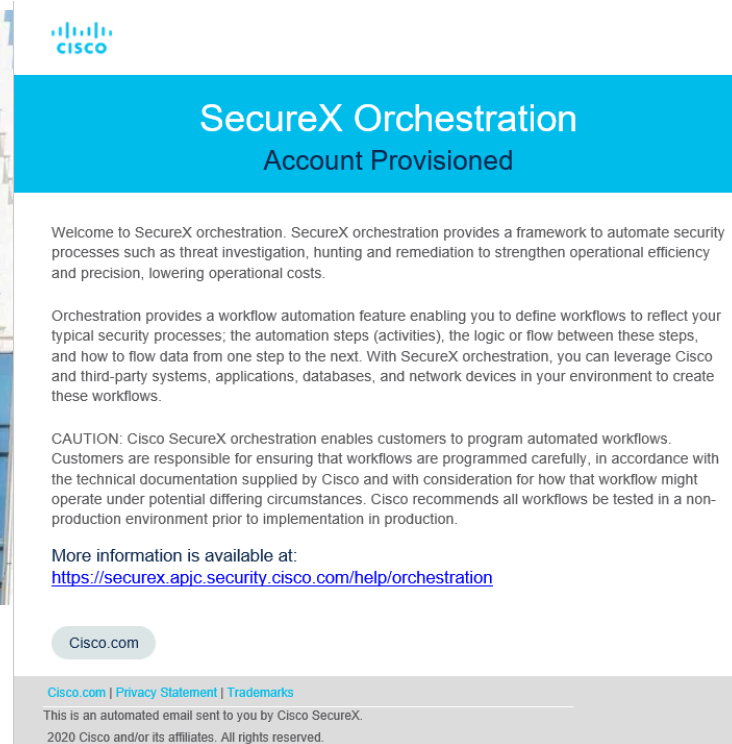
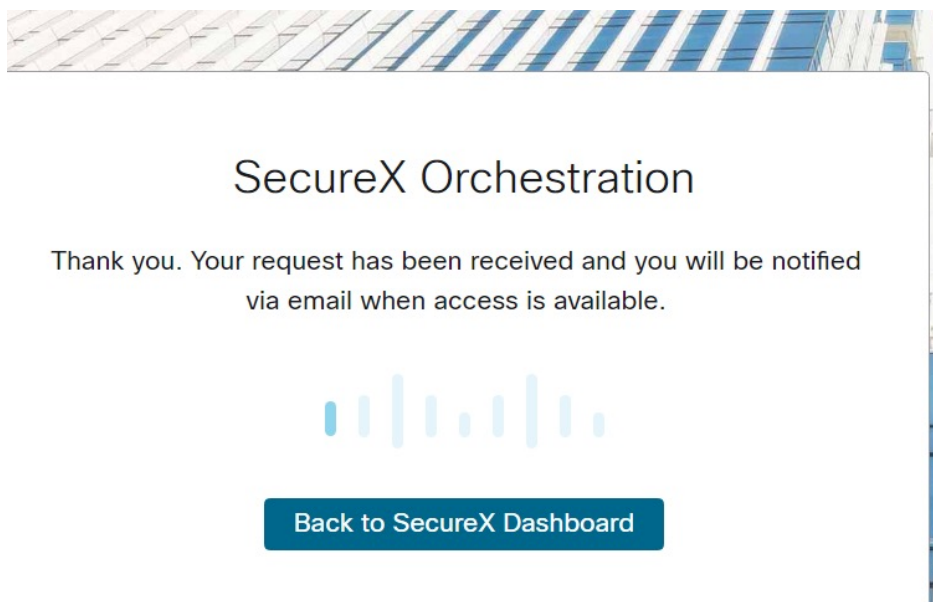
マウスオーバーするとページ左側のメニューが展開します。

Workflows	Workflows	MyWorkflows/Runs&SystemMonitor/My Exchangeが含まれる。
Runs	Runs	Workflowを実行したステータス表示や変更、削除を行うことが可能。
Targets	Targets	Workflowsと通信可能とするシステムやリソースを作成が可能。
Account Keys	Account Keys	Targetsの種類に応じて様々なタイプがあり作成が可能。
Variables	Variables	グローバル変数の設定や変数の定義を作成が可能。
Calendars	Calendars	Schedulesと組み合わせて使用し、毎日や毎週等の日付を作成が可能。
Schedules	Schedules	Workflowsを実行する時間を作成が可能。
Tasks	Tasks	Workflow実行に上司の承認を必要とするなど別途タスクを追加可能。
Events & Webhooks	Events & Webhooks	Workflow実行時トリガーとなる内部・外部イベントを表示・作成が可能。
Admin	Admin	さまざまな管理を行うことが可能。

① 初めに「Orchestration」をクリックして移動
※初回のみ「アクセス権申請要」の申請画面が表示されるため申請後に**②**を実施

② 新規にWorkflow作成する場合は「New Workflow」をクリック

(参考) Orchestration申請後の通知画面



Workflows メニュー

The screenshot displays the Cisco SecureX Orchestration interface. At the top, there are navigation tabs for Dashboard, Integration Modules, Orchestration (selected), Insights, and Administration. The user is identified as APJC | Admin. The main heading is "SecureX Orchestration" with a "Beta" badge. Below this, there are sections for "My Workflows" and "Runs". A blue callout bubble points to the "Runs" section with the text "すべてのワークフローリスト確認". Under "Runs", there are filters for "All Workflows (4)", "Atomics (176)", "Recents", and "Favorites (0)". The "Atomics" filter is highlighted with a red box, and a blue callout bubble points to it with the text "使用可能なAtomicsリスト確認". Below the filters, there are several workflow cards, including "Move Computer to Triage Group", "Take Forensic Snapshot and Isolate", "Take Orbital Forensic Snapshot", and "Host Isolation with Tier 2 Approval". At the bottom of the screenshot, the text "Atomics: ワークフローで実行可能な小さなワークフロー" is displayed.

Runsメニュー

SecureX Dashboard | Integration Modules | **Orchestration** | Insights | Administration

SecureX Orchestration Beta

My Workflows | **Runs & System Monitor** | My Exchange

System Monitor

For all workflows

Last 7 Days

Running	0	Failed	0
Paused	0	Cancelled	0

Workflow Runs over time

Daily run volume at workflows

Last 7 Days

Date	Run Volume
Jan 27, 2023	0
Jan 28, 2023	0
Jan 29, 2023	0
Jan 30, 2023	0
Jan 31, 2023	0
Feb 01, 2023	0
Feb 02, 2023	0
Feb 03, 2023	0

Type to search workflows by name

Showing runs from: Last 24 Hours

Workflow Runs

Workflow Name

Type to search workflows

Last Run Status

All

Runs List

Enter a full or partial workflow name in the **Type to Search Workflows** text box and check the workflow name. See the **Runs** Help topic for more information.

Actions are cleaned up after 30 days. Run summary data is available for 90 days.

ワークフロー実行履歴を確認(検索 or フィルタ可能)

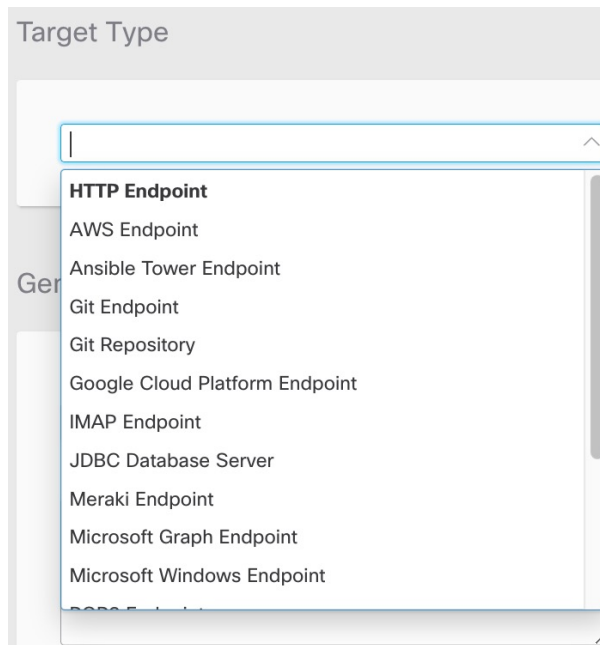
Targetsメニュー

ターゲットとターゲットグループを確認および作成

Display name +	Created on	Status	Owner	Actions
AMP_Target HTTP Endpoint	2022/1/13 23:53:38	Valid	younna@cisco.com	
CTIA_Target HTTP Endpoint	2022/1/13 23:53:41	Valid	younna@cisco.com	
CTR_API HTTP Endpoint	2022/1/13 23:53:40	Valid	younna@cisco.com	
CTR_For_Access-Token HTTP Endpoint	2022/1/13 23:53:40	Valid	younna@cisco.com	
Email Endpoint SMTP Endpoint	2022/1/13 23:53:41	Valid - See Notes ⓘ	younna@cisco.com	
Orbital_For_Access-Token HTTP Endpoint	2022/1/13 23:53:38	Valid	younna@cisco.com	

Targetタイプ一覧

Target タイプ	目的 / 対象
AWS Endpoint	Amazon Web Services APIs
Git Endpoint	Git repositories
Google Cloud Platform Endpoint	Google Cloud Platform
HTTP Endpoint	HTTP ベース API (例 : REST API)
JDBC Database Server	MySQL, Microsoft SQL, Oracle, and SAP HANA database servers
Meraki Endpoint	Meraki デバイス API
Microsoft Windows Endpoint	Window ベースホスト
SMTP Endpoint	SMTP / MTA からのメール送信
SNMP Endpoint	SNMP ベースデバイス管理
Terminal Endpoint	SSH ベースコマンド実行 (例 : ルータ、スイッチ)
Terraform Endpoint	Terraform API
Unix/Linux Endpoint	Unix/Linux ベースコマンド実行 (例 : Unix/Linux)



Account Keys ✕ ニュー

SecureX Dashboard Integration Modules **Orchestration** Insights Administration APJC | Admin

Account Keys

Search

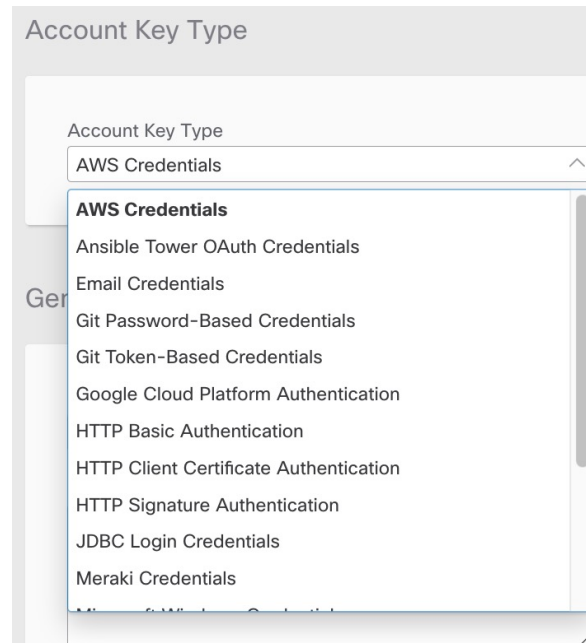
New Account Key

Display name	Status	Owner	Last modified +	Actions
CTR_Credentials HTTP Basic Authentication	Created	younna@cisco.com	2022/1/13 23:53:35	
Orbital_Credentials HTTP Basic Authentication	Created	younna@cisco.com	2022/1/13 23:53:35	
AMP_Credentials HTTP Basic Authentication	Created	younna@cisco.com	2022/1/13 23:53:35	
Git_Credentials Git Password-Based Credentials	Created	younna@cisco.com	2022/1/13 23:53:07	

アカウントキーを確認および作成

Account Keyタイプ一覧

Key タイプ	Target タイプ
AWS Credentials	AWS Endpoint
Email Credentials	POP3 Endpoint, SMTP Endpoint
Git Password-Based Credentials	Git Endpoint
Git Token-Based Credentials	Git Endpoint
Google Cloud Platform Authentication	Google Cloud Platform Endpoint
HTTP Basic Authentication	HTTP Endpoint
HTTP Client Certificate Authentication	HTTP Endpoint
HTTP Signature Authentication	HTTP Endpoint
JDBC Login Credentials	JDBC Database Server
Meraki Credentials	Meraki Endpoint
Microsoft Windows Credentials	Microsoft Windows Endpoint
SecureX Token	HTTP Endpoint
SNMP Credentials	SNMP Endpoint
Terminal Key-Based Credentials	Terminal Endpoint, Terraform Endpoint, Unix/Linux Endpoint
Terminal Password-Based Credentials	Terminal Endpoint, Terraform Endpoint, Unix/Linux Endpoint



Variablesメニュー

- **Global Variables**
 - SecureX Orchestration のテナント内に保存し利用
 - ワークフローインポート時に新規 Global Variables がインポートされる場合あり
- **Local Variables**
 - オークストレーションワークフロー単位全体に定義、保存し利用
 - オークストレーションワークフローを構成するAtomic単位で指定される Variables

The screenshot shows the 'Variables' page in the SecureX interface. The 'Global Variables' tab is selected. A table lists two variables: 'SECUREX_ENVIRONMENT' (String) and 'AO_LOOP_LIMIT' (Integer). A 'New Variable' button is visible in the top right corner. A blue callout box points to the table with the text: '数値や文字を入れられる変数(Variables)を確認および作成'.

Display name	Scope	Value	Owner	Last modified +	Actions
SECUREX_ENVIRONMENT String	env	prod-apjc	system	2020/6/16 9:40:46	
AO_LOOP_LIMIT Integer	env	500	system	2020/6/16 9:40:46	

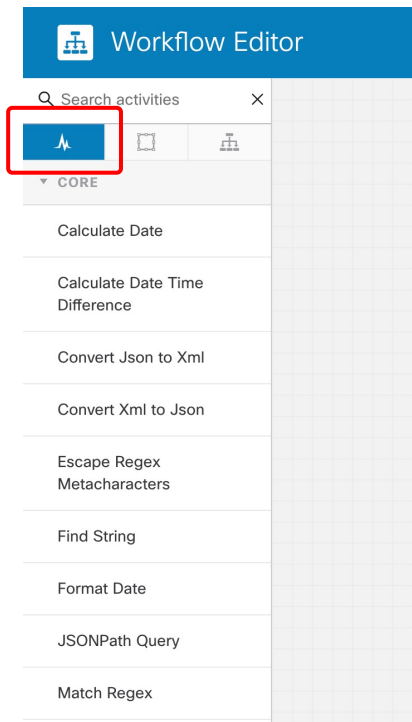
Workflow画面 構成要素

The screenshot displays the Workflow Editor interface. At the top, the title bar reads "Workflow Editor" and includes a "Modified: 2023年1月24日 at 13:10:13" timestamp, along with buttons for "Validate", "Commit", "View Runs", and "Run".

The interface is divided into three main sections:

- Activity Palette (Left):** A sidebar titled "Search activities" containing a list of activities under the "CORE" category. A red dashed box highlights the "CORE", "LOGIC", and "WORKFLOWS" icons. A tooltip is shown over these icons with the following descriptions:
 - CORE:** 組み込み、またはアトミックアクションの追加
 - LOGIC:** グループやループ、条件などの追加
 - WORKFLOWS:** 別ワークフローの追加
- Canvas (Center):** A grid-based workspace labeled "キャンパスエリア" (Canvas Area) with the instruction "Urag activity here".
- Properties Panel (Right):** A panel titled "PROPERTIES" with a "1 WARNING" indicator. It contains a "General" section with a "Display Name" input field (labeled "プロパティエリア"), an "Owner" field with the value "gokato@cisco.com", and a "Description" text area. A checkbox at the bottom is labeled "Clean up after successful execution".

Core Activity



Core Activityは、アクションを実行するために使用できる、ビルトインおよびサードパーティ製の関数

Workflowで利用可能なCore Activities (1)

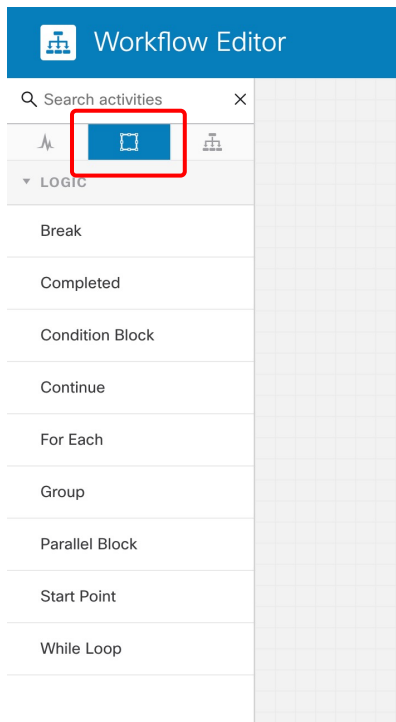
名称	概要	備考
Calculate Date	時刻情報 (日時) の加算減算	
Calculate Date Time Difference	2つの時刻情報 (日時) の差分計算	
Convert JSON to XML	JSONをXMLに変換	
Convert XML to JSON	XMLをJSONに変換	
Escape Regex Metacharacters	正規表現におけるメタ文字のエスケープ	Match Regexで使用する正規表現の事前処理として利用
Find String	文字列の検索	
Format Date	時刻情報 (日時) のフォーマット変換	
JSONPath Query	JSON形式の文字列から要素のデータ抽出	
Match Regex	正規表現による文字列検索	
Parse Date	文字列から時刻情報 (日時) 変数への変換	
Replace Staring	文字列の置換	

Workflowで利用可能なCore Activities (2)

名称	概要	備考
Set Variables	変数の値変更	
Sleep	Workflowの一時停止	
Split String	文字列を区切り文字で分割	
Substring	文字列を文字の位置指定 (開始/終了) で部分参照	
To Lower	アルファベットを小文字に変換	
To Upper	アルファベットを大文字に変換	
Trim String	文字列の切り取り	
Xpath Query	XML形式の文字列から要素のデータ抽出	
XSL Transform	Extensible Stylesheet Language Transformations (XSLT)に基づくXMLの形式変換	

<https://docs.securex.security.cisco.com/Orchestration-Help/Content/activities-core.html>

Logic Activity

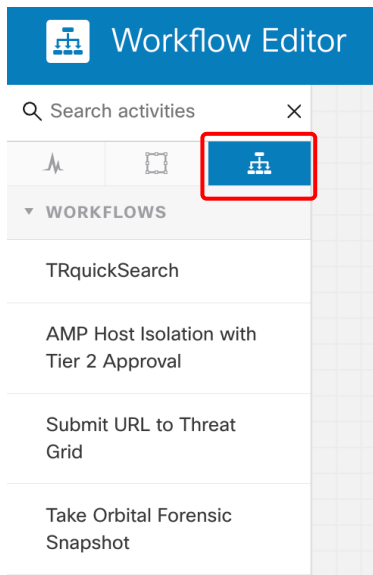


グループ、条件、ループなどの要素を追加することで、柔軟なワークフローを作成可能

Workflowで利用可能なLogic Activities

名称	概要	備考
[Logic Block]		
Condition Block	条件に一致した場合処理を実行	
Parallel Block	複数の処理を並列で実行	
For Each	配列の要素を順番に処理	
While Loop	条件が真である間処理を継続	
[実行制御]		
Break	For Each/While Loopの処理途中でLoopの強制終了	For Each/While Loop内のみ利用可能
Continue	For Each/While Loopの処理途中で後続の処理をスキップし、次のLoop処理を実行	For Each/While Loop内のみ利用可能
Complete	完了状態を指定し、Workflowを終了(停止)	
[その他]		
Group	Workflowの可視性向上のため、Activityのグループ化	処理上の動作影響は無し
Start Point	デフォルトの開始点とは異なる地点を開始点として選択可能	手動実行の場合のみ

Workflow activity



ワークフローの中に、**既存のワークフロー**を子オブジェクトとして追加が可能。そうすることで複雑にはなるが、目的を達成するために必要な、より小さなワークフローが作成可能



2. モデルケースについて

モデルケースの概要

【初心者向けガイドとして、以下のモデルケースを参考にその手順を解説】

• Umbrella Report APIを使ったドメイン情報取得ならびにWebex APIによる情報投稿

<https://qiita.com/dmatsumu/items/40b07c64bb2d688a923c>

【概要】

- UmbrellaのAPI keyならびにWebexのToken取得
- Webex Bot作成、アクセストークン取得、Space作成、Space ID取得
- SecureXへUmbrellaを統合
- SecureXのWorkflowを使ってUmbrellaから情報取得、ならびにWebexへの投稿
- SecureXで日次で上記処理が走るようにTrigger設定

3.ワークフロー事前 準備&設定



事前準備 Umbrella編

- APIキーとシークレットの取得

APIキーとシークレットの取得

Admin -> API Keys -> Add からReports用のAPI Keyを作成

Cisco Umbrella

Overview

Deployments >

Policies >

Reporting >

Investigate >

Admin ▾

- Accounts
- User Roles
- Log Management
- Authentication
- Bypass Users
- Bypass Codes
- API Keys**

API Keys

Umbrella's API keys are used to authenticate your Umbrella API requests. You can create multiple keys and manage each key's access controls to meet specific use cases. For more information, see Umbrella's [Help](#).

③ "Add" をクリック

② "API Keys" をクリック

API Keys 0

KeyAdmin Keys 0

Static Keys 3

Legacy Keys 4

Search by API Name, Key or Creator

① "Admin" から "API Keys" をクリック

APIキーとシークレットの取得

④任意の名前を設定

Add New API Key

To add this unique API key to Umbrella, select its scope—what it can do—and set an expiry date. The key and secret created here are unique. Deleting, refreshing or modifying this API key may break or interrupt integrations that use this key. For more information, see Umbrella's [Help](#).

API Key Name

REPORT-API

⑤“Reports”を選択

Key Scope

Select the appropriate access scopes to define what this API key can do.

- Admin 3 >
- Auth 1 >
- Deployments 11 >
- Policies 3 >
- Reports 5 >

Expiry Date

Never expire

Expire on: Jun 26 2023

CANCEL

1 selected

REMOVE ALL

Scope

Reports

Read-Only

⑥“Read-Only”を選択

Key Scope:
生成したAPI Keyでどのような情報を取り扱うことができるか指定

Scope:
生成したAPI Keyの権限を選択

Expiry Date:
API Keyの有効期限を指定



CREATE KEY


⑦“CREATE KEY”をクリック

APIキーとシークレットの取得

API Key/Secretをメモ帳などに保存

Copy the API key and secret and use them to authenticate API requests. This secret is only displayed once. Click Refresh to generate a new key and secret. For more information, see Umbrella's [Help](#).

API Key abd5317440 [REDACTED] 	Key Secret 68bf575c2a [REDACTED] 
---	--

 **Copy the Key Secret.** For security reasons, it is only displayed once. If lost, it cannot be retrieved. **ACCEPT AND CLOSE**

⑧“API Key” “Key Secret” の値をメモ帳などに保存

シークレットは一度しか表示されない点に注意
もし閉じてしまった場合は”REFRESH”で再度作成すればOK

事前準備 Webex編

- Botの作成
- Bot access token取得
- Spaceの作成
- SpaceIDの取得

Botの作成

Webex for Developersページ(下記URL)から、以下の内容でBotを追加

<https://developer.webex.com/my-apps/new/bot>

【重要】

“Bot username”は必ず一意である必要があり、右記のユーザ名は入力不可です。また似たような名前によるSpace作成やID取得のミスも出てくるためご注意ください

Bot name:

Webex上で見えるBotの名前(日本語可)

Bot username:

Botのユーザ名(後から変更不可、**重複不可**)

Icon:

Botのアイコン。画像サイズが厳密に512x512px である必要あり

App Hub Description:

BotをApp Hubで公開する場合の説明文

webex for Developers Documentation Blog Support Resources

New Bot

Bot name*
Name of your bot as it will appear in Webex.

Bot username*
The username users will use to add your bot to a space. Cannot be changed later.

Icon*
Upload your own or select from our defaults. Must be exactly 512x512px in JPEG or PNG format.

App Hub Description*
What does your app do, how does it benefit users, how do users get started? Does your app require a non-Webex account? If your app is not free or has additional features for paid users, please note that and link to pricing information. 1024 character limit.

Supported markdown 1475 characters remaining

Cancel Add Bot

※必ず任意の名前を付けましょう
(こちらのみ日本語可)

① Bot nameを任意の名前に設定

② Bot usernameを指定

※必ず任意の名前を付けましょう

③ Icon、App Hub Description を記入

④ “Add Bot”をクリック

Bot access token取得

Congratulations! 🎉

SecureX_Umbrella_Demo is one step closer to becoming a reality.

SecureX_Umbrella_Demo

👉 **Next Step:** Use your Bot Access Token to set up your webhook and finish building your bot.

Bot access token

Non-expiring (good for 100 years) access token for your bot. Save this token to set up your webhook.

`ZDVkNzFmNzUtZDEzZS00MWMYLTg5ODQtMWU5ZDRmNzg1OG'` [Copy Token](#)

💡 **Tip:** Save this token!
It won't be shown again (but you can regenerate a new one if needed).

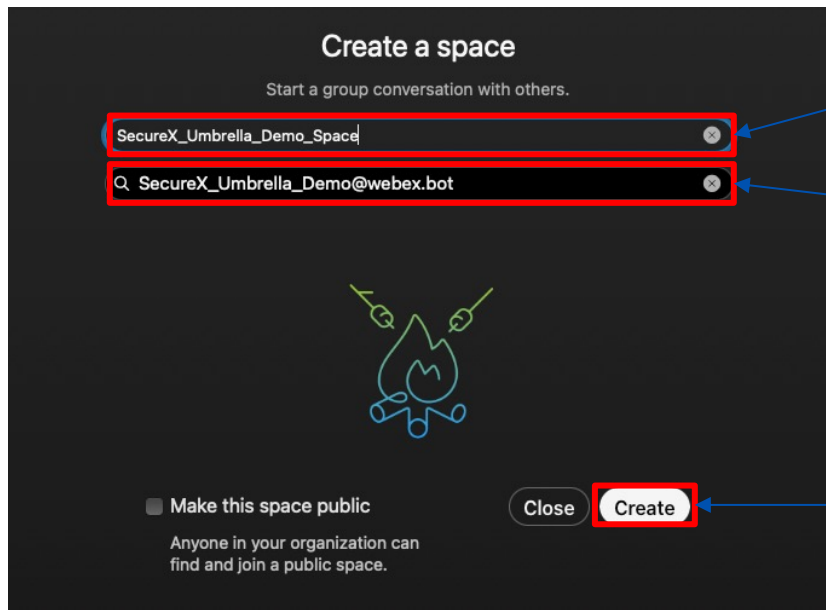
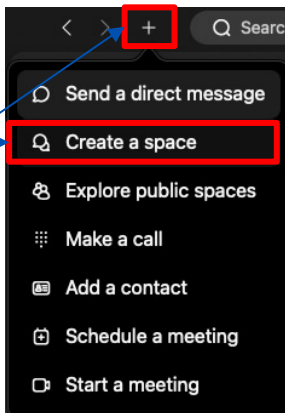
⑤ 出力されたBot access tokenをメモ帳に保存 (STEP6で利用)

Bot access tokenは一度しか表示されない点に注意
もし閉じてしまった場合は”Regenerate Access Token”から再度作成すればOK

Spaceの作成

Webex デスクトップクライアントからSpaceを作成

① “+” から
“Create a space”
をクリック



② 任意のSpace名(日本語可)

③ P32の「②Bot username」を
記入
(他に追加したいユーザがいれば
随時追加)

④ “Create”をクリック

Make this space public:
同じ組織内のユーザがこのスペースを検索できる
ようにする場合にチェックする

SpaceIDの取得

下記URLからBotを追加したスペースのIdを取得してメモ帳などに保管

<https://developer.webex.com/docs/api/v1/rooms/list-rooms>

The screenshot displays the Webex API documentation for the 'List Rooms' endpoint. On the left, a sidebar lists various API endpoints, with 'Rooms' highlighted in red. The main content area shows the 'List Rooms' endpoint details, including a 'GET /v1/rooms' request and a 'Run' button at the bottom right, which is also highlighted in red. The 'Header' section shows a 'Bearer' token field, and the 'Query Parameters' section shows 'sortBy' set to 'lastactivity'.

このURLについて:

開発者がWebex APIを検証用途で手軽に利用できるツール。
ただしこのページで実施した内容は実環境にも影響しますのでリソースの削除などに注意。

ここではSpaceのIDを取得したいため”Rooms”の”List Rooms”というリソースから情報を取得。(WebexにおいてSpaceとRoomは同義です)

Header:

このツール内で使える検証用途の開発者トークン。
実環境で全権限を持つトークンなので取り扱いに注意。

Query Parameters:

詳細な検索条件などが指定可能。
”created”もしくは”lastactivity”を指定することで先程作成したスペースが上位に表示される(オプション)

① “Run” をクリック

SpaceIDの取得

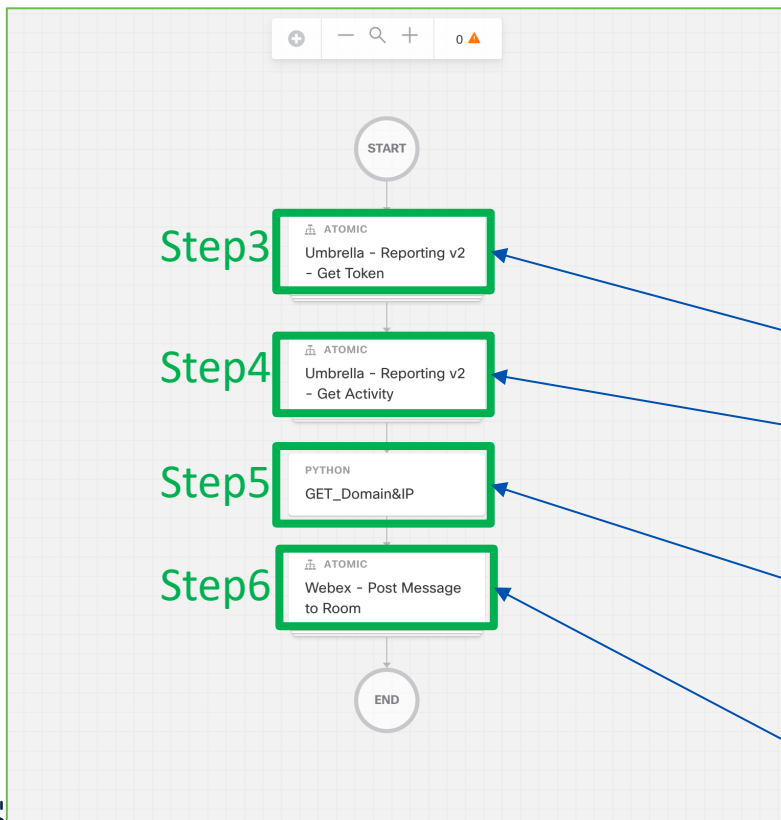
このid(SpaceID)をメモ帳などに保存
(STEP6で利用)

前ページの実行結果の中から、
"title"が先程作ったBotのSpace
名を探し、その上部のidをメモ
※状況によっては一番上に表示され
ない可能性もあります。

```
Request  Response
{
  "items": [
    {
      "id": "Y21zY29zcGFyazovL3VzL1JPT00vYTgyZTVjZTAtY2Q0ZC0xMWVkbWE5ZTYtYTU3MzM4ZDRmZGUz",
      "title": "SecureX_Umbrella_Demo_Space",
      "type": "group",
      "isLocked": false,
      "lastActivity": "2023-03-28T09:48:13.614Z",
      "creatorId": "Y21zY29zcGFyazovL3VzL1BFT1BMRS9jMGJjNDY3OS0wNjkyLTQ5NmMtODhiOC1iMzgzNTIxNTNhODY",
      "created": "2023-03-28T09:48:13.614Z",
      "ownerId": "Y21zY29zcGFyazovL3VzL09SR0FOSVpBVElPTi8xZWl2NWZkZi05NjQzLTQxN2YtOTk3NC1hZDcyY2F1MGUxMGY",
      "isPublic": false,
      "isReadOnly": false
    }
  ]
}
```

SecureX ワークフロー設定編

ワークフロー全体図



Step1:

Account Keyの登録

UmbrellaのAPIクレデンシャルをAccount KeyとしてSecure X上に登録

Step2:

Targetの登録

ワークフローで使用する下記のTargetを登録

1. Umbrella のAPIのAccess Token作成用
2. Umbrella のReport API用
3. Webex Teamsへのメッセージポスト用

Step3:

Umbrella Reporting APIから情報を取得するためのAccess Token取得

Step4:

Step3で取得したAccess Token を使用してUmbrella Reporting APIからマルウェアを提供しているサーバーやマルウェアに感染している疑いのある Web サイトへアクセスしたイベント情報を取得

Step5:

Step4で取得した情報からマルウェアを提供しているサーバーやマルウェアに感染している Web サイトである疑いのあるドメイン名とそのドメインにアクセスしたIPアドレスをPython Scriptを使用して抽出

Step6:

Step5で抽出した情報をWebex teamsのスペースにポスト

Step1 Keyの登録

- 事前準備 で取得したUmbrellaのAPIクレデンシャルをAccount KeyとしてSecure X上に登録する

UmbrellaのAPIクレデンシャルをAccount Keyとして登録

”New Account Key”からUmbrella用のAPI Credentialを登録

② “New Account Key”をクリック

Display name	Status	Owner	Last modified	Actions
Umbrella_cred HTTP Basic Authentication	Valid	dmatsumu+jpamp@cisco.com	2022/9/2 14:36:38	
AMP_Credentials HTTP Basic Authentication	Created	dmatsumu+jpamp@cisco.com	2022/3/10 15:10:05	
CTR_Credentials	Created	dmatsumu+jpamp@cisco.com	2022/3/10 15:10:05	

① “Account Keys”をクリック

③下記の情報を入力

Account Key Type: HTTP Basic Authentication

Display Name: 任意の名前 ex. “Umbrella_Key”

Username: APIキー

Password: APIシークレット

Authentication Option: Basic

④ “Submit”をクリック

Step2

Targetの登録

- ワークフローで使用する下記のTargetを登録する
- Umbrella のAPIのAccess Token作成用
- Umbrella のReport API用
- Webex Teamsへのメッセージポスト用

Target登録1 Umbrella のAPI Access Token発行用

TargetsからAccess Token発行用のURLをTargetとして登録。

① “Target”をクリック

② “New Target”をクリック

Display name	Create...	Status	Owner	Actions
AMP_Target HTTP Endpoint	2022/3/10 15:10:08	Valid	dmatsumu+jpamp@ciscom	
CTIA_Target HTTP Endpoint	2022/3/10 15:10:11	Valid	dmatsumu+jpamp@ciscom	

③下記の情報を入力

Target Type
“HTTP Endpoint”を選択

Display Name:
任意の名前 ex. “Umbrella_Token”

No Account Keys:
False

Default Account Keys:
Step1で作成したAccount Keyを選択
“Umbrella_Key”

Protocol:
HTTPS

HOST/IP Address:
api.umbrella.com

Port:
443

“Disable server certificate validation”
にチェック

“Ignore Proxy”を有効化

④ “Submit”をクリック

(参考) Umbrella APIのアクセストークンについて

- Umbrella API は、標準の REST インターフェイスを提供し、OAuth 2.0 クライアント クレデンシャル フローをサポート
- APIを利用するためには、Umbrella ダッシュボードから取得したUmbrella API 資格情報を使用して API アクセストークンを生成する必要がある
- SHELLスクリプトからのアクセストークンRequest

```
curl --user '<key>:<secret>' --request POST --url 'https://api.umbrella.com/auth/v2/token' \  
-H 'Content-Type: application/x-www-form-urlencoded' \  
-d 'grant_type=client_credentials'
```

- <https://developer.cisco.com/docs/cloud-security/#!authentication>

Target登録2 Umbrella Reporting API用

TargetsからUmbrella Reporting API用のURLをTargetとして登録。



<https://developer.cisco.com/docs/cloud-security/#!reporting-v2-getting-started/base-uri>

The Umbrella Reporting v2 API begins with the following base URI:
https://reports.api.umbrella.com/v2

③下記の情報を入力

Target Type
“HTTP Endpoint”を選択

Display Name:
任意の名前 ex. Umbrella_Report

No Account Keys:
True

Protocol:
HTTPS

HOST/Address:
reports.api.umbrella.com

Port:
443

※HOST/AddressのターゲットURI
にv2の記載は不要

“Disable server certificate validation”
にチェック

“Ignore Proxy”を有効化

④ “Submit”をクリック

(参考) Umbrella のReporting APIについて

- Umbrella Reporting API を使用すると、Umbrellaのログとレポートにプログラムでアクセスすることが可能
- APIの詳細はこちら
 - <https://developer.cisco.com/docs/cloud-security/#!api-reference-reports-reporting-overview>
- SHELL Scriptで過去 7 日間のActivityレポートを取得する例

```
curl --location --location-trusted \  
--request GET --url 'https://api.umbrella.com/reports/v2/activity?from=-7days&to=now&limit=10' \  
-H 'Authorization: Bearer %YourAccessToken%' \  
-H 'Content-Type: application/json'
```

Copy

(参考) Webex Message APIについて

- <https://developer.webex.com/docs/api/v1/messages>

The screenshot displays the 'Create a Message' endpoint documentation. On the left is a navigation menu with categories like Bots, Integrations and Authorization, Webhooks, Buttons and Cards, Reference, Attachment Actions, Events, Memberships, Messages, and Messages with Edit. The 'Messages' section is expanded, showing various actions such as 'List Messages', 'List Direct Messages', 'Create a Message', 'Edit a Message', 'Get Message Details', and 'Delete a Message'. The main content area is titled 'Create a Message' and includes a description: 'Post a plain text or rich text message, and optionally, a file attachment attachment, to a room. The files parameter is an array, which accepts multiple values to allow for future expansion, but currently only one file may be included with the message. File previews are only rendered for attachments of 1MB or less.' Below this is the endpoint 'POST /v1/messages' and a 'Body Parameters' section with the following fields: 'roomId' (string, 'The room ID of the message.'), 'parentId' (string, 'The parent message to reply to.'), 'toPersonId' (string, 'The person ID of the recipient when sending a private 1:1 message.'), and 'toPersonEmail' (string, 'The email address of the recipient when sending a private 1:1 message.'). To the right is a dark-themed 'Try it' interface with 'Try it' and 'Example' buttons. It shows the 'POST /v1/messages' endpoint, 'Content-Type' as 'application/json', and an 'Authorization' section with a 'Use personal access token' toggle and a 'Bearer' token field. The 'Body' section contains input fields for 'roomId', 'parentId', 'toPersonId', and 'toPersonEmail' with example values.

Step3～Step6 ワークフローの作成

Step3:

Umbrella Reporting APIから情報を取得するための
Access Token取得

Step4:

Step3で取得したAccess Token を使用してUmbrella
Reporting APIからマルウェアを提供しているサーバーやマル
ウェアに感染している疑いのある Web サイトへアクセス
したイベント情報を取得

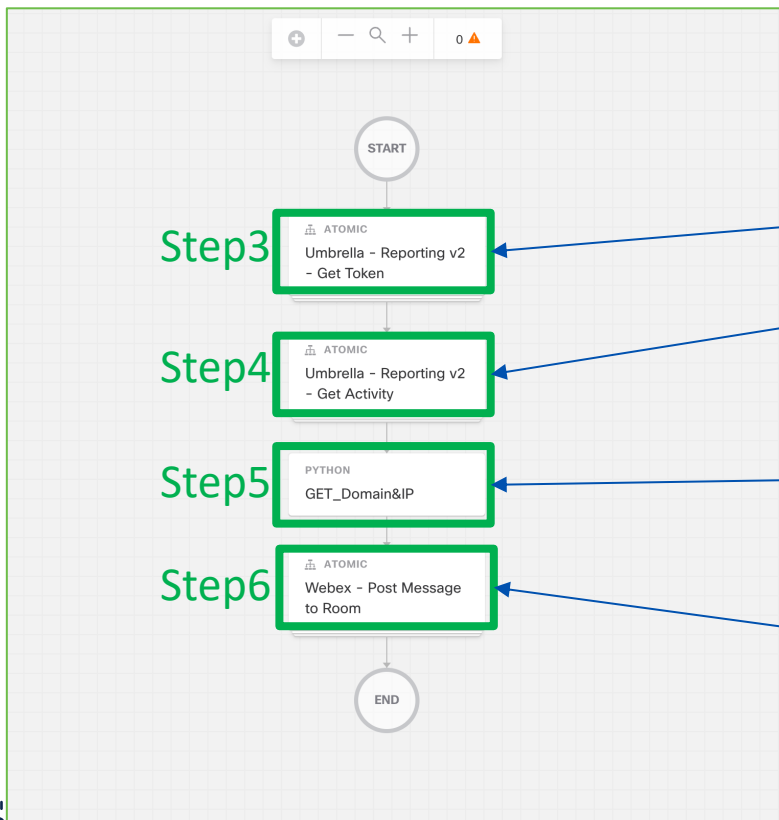
Step5:

Step4で取得した情報からマルウェアを提供しているサー
バーやマルウェアに感染している Web サイトである疑いの
あるドメイン名とそのドメインにアクセスしたIPアドレスを
Python Scriptを使用して抽出

Step6:

Step5で抽出した情報をWebex teamsのスペースにポスト

ワークフロー全体図



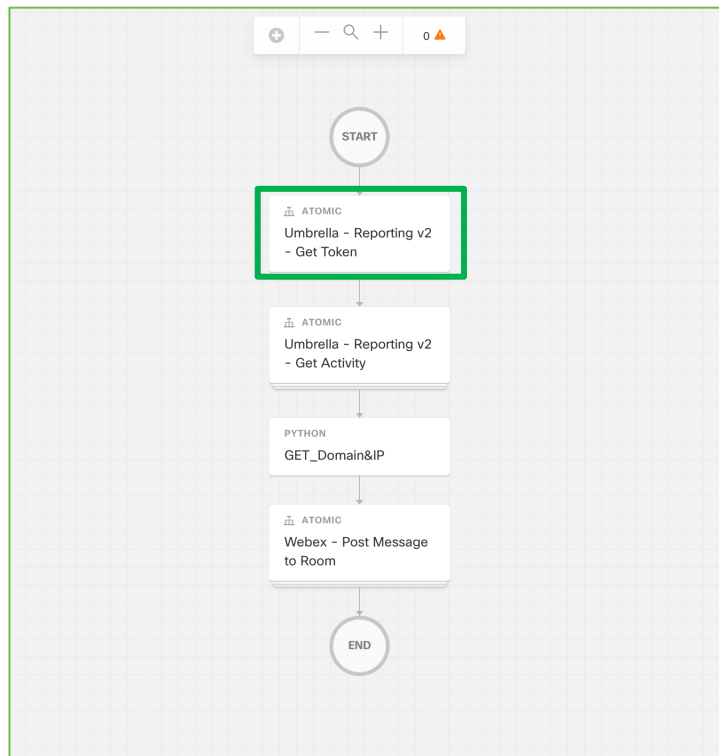
Step3:
Umbrella Reporting APIから情報を取得するためのAccess Token取得

Step4:
Step3で取得したAccess Token を使用してUmbrella Reporting APIからマルウェアを提供しているサーバーやマルウェアに感染している疑いのある Web サイトへアクセスしたイベント情報を取得

Step5:
Step4で取得した情報からマルウェアを提供しているサーバーやマルウェアに感染している Web サイトである疑いのあるドメイン名とそのドメインにアクセスしたIPアドレスをPython Scriptを使用して抽出

Step6:
Step5で抽出した情報をWebex teamsのスペースにポスト

Step3 Access Token取得



ワークフロー作成の開始

① “Workflow”をクリック

The screenshot displays the Cisco SecureX Orchestration dashboard. At the top, the navigation bar includes 'SecureX', 'Dashboard', 'Integration Modules', 'Orchestration', 'Insights', and 'Administration'. The 'Orchestration' tab is active. On the left sidebar, the 'Workflow' icon (a grid of four squares) is highlighted with a red box. An arrow points from the text '① “Workflow”をクリック' to this icon. Below the sidebar, the main content area shows 'SecureX Orchestration Beta' and tabs for 'My Workflows', 'Runs & System Monitor', and 'My Exchange'. The 'My Workflows' tab is selected. Below the tabs, there are filters for 'All Workflows (6)', 'Atomics (176)', 'Recents', and 'Favorites (0)'. A search bar with the placeholder text 'Type to search workflows by name' is present. On the right side of the main content area, the 'Import Workflow' button and the 'New Workflow' button are visible. The 'New Workflow' button is highlighted with a red box, and an arrow points from the text '② “New Workflow”をクリック' to it. Below the buttons, three workflow cards are displayed: 'Umbrella_GET_REPORT' (UPDATED), 'Take Forensic Snapshot and Isolate' (IMPORT COMPLETED), and 'Move Computer to Triage Group' (IMPORT COMPLETED). Each card includes the author's name (naogawa@cisco.com) and the last modified date.

Activitiesから”Umbrella – Reporting v2 – Get Token”を選択

SecureX-TEST

Modified: 2023年3月24日 at 6:44:39

Validate Commit View Runs Run

Search activities

Umbrella - Reporting - Get Security Activity Report

Umbrella - Reporting v2 - Get Activity

Umbrella - Reporting v2 - Get Categories

Umbrella - Reporting v2 - Get Token

Umbrella - Reporting v2 - Get Top Internal IPs

Umbrella - Reporting v2 - Get Top Threats

CISCO WEBEX

DATABASE

EMAIL

FILE OPERATIONS

GOOGLE CLOUD PLATFORM

KENNA

MERAKI

MICROSOFT WINDOWS

Drag activity here

PROPERTIES

SecureX-TEST

Version

Git Repository

Git Version

General

①任意のワークフロー名を定義

Display Name

SecureX-TEST

Owner

naogawa@cisco.com

Description

Clean up after successful execution

Is atomic workflow

Group Name

51

ActivityにTarget情報を入力

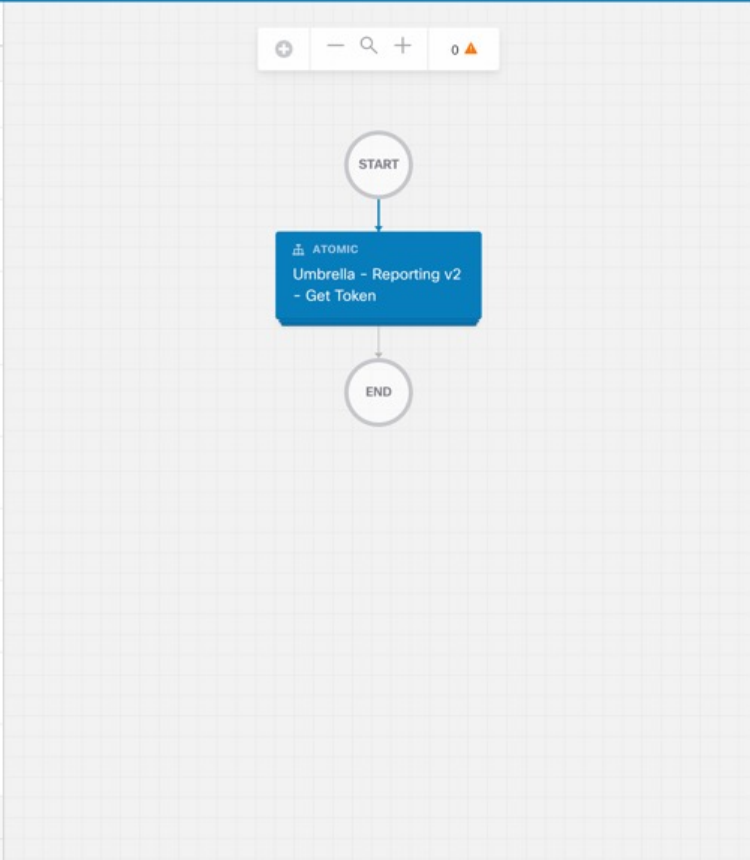
②Validateをクリック

③実行確認

SecureX-TEST Modified: 2023年3月24日 at 6:44:39 Validate Commit View Runs Run ⚙️ ✕

Search activities

- Umbrella - management - Get Destination List Entries
- Umbrella - Management - Get Destination Lists
- Umbrella - Management - Get Organizations
- Umbrella - Management - Remove Record from Destination List
- Umbrella - Reporting - Get Security Activity Report
- Umbrella - Reporting v2 - Get Activity
- Umbrella - Reporting v2 - Get Categories
- Umbrella - Reporting v2 - Get Token
- Umbrella - Reporting v2 - Get Top Internal IPs
- Umbrella - Reporting v2 - Get Top Threats
- CISCO WEBEX
- DATABASE



PROPERTIES: UMBRELLA - REPORTING V2 - GET TOKEN
Umbrella - Reporting V2 - Get Token

HTTP Endpoint

- No target
- Execute on this target
- Use workflow target
- Override workflow target
 - * Target
 - Umbrella_Token
- Execute on this target group
 - Target Group
 - Select
- Use workflow target group
- Override workflow target group criteria

Credentials

Account Key Type

Select

- Use target's default account keys
- Override account keys
 - Account Key Id
 - Select

①"Override workflow target"を選択し、Step2で作成したトークン作成用のTargetを選択する

STEP3 実行結果

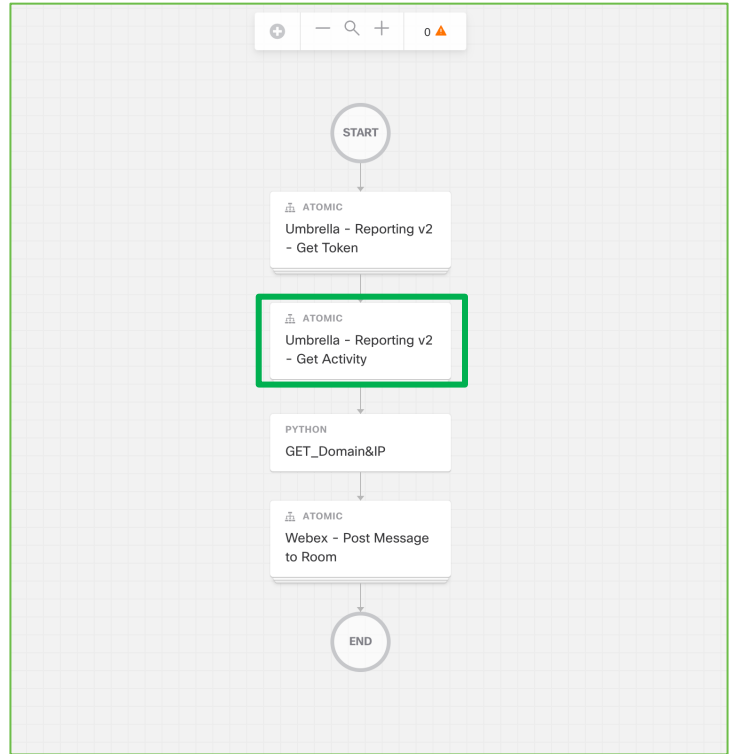
The screenshot displays the Cisco SecureX Orchestration interface. At the top, the navigation menu includes Dashboard, Integration Modules, Orchestration (selected), Insights, and Administration. The main header shows 'SecureX-TEST Run' with a 'SUCCESS' status and a 'RUN TIME' of 1.1 s. A sidebar on the left contains various tool icons.

The central workflow diagram shows a sequence: START -> ATOMIC 'Umbrella - Reporting v2 - Get Token' -> END. A red arrow points from this step to the 'Properties' panel on the right, which is titled 'Umbrella - Reporting v2 - Get Token'. The 'Properties' panel shows 'Target' set to '200' and 'Error Message' as 'SUCCESS'. Below this, the 'JSON Output' section displays the following data:

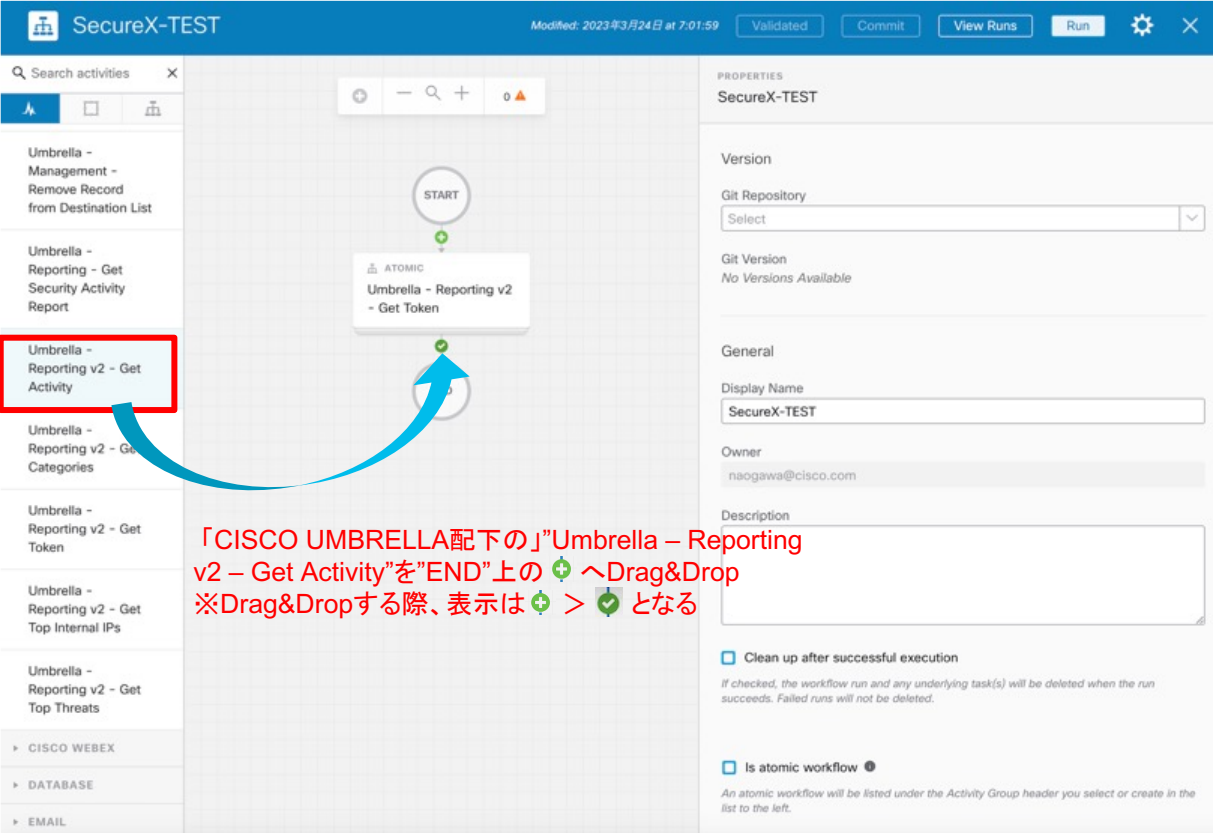
```
1 {
2   "output": {
3     "error": {
4       "code": "200",
5       "message": "success"
6     },
7     "response": {
8       [REDACTED]: 3600,
9       "*****",
10      "elapsed_time": 1.196411749,
11      "end_time": "2023-03-24T02:51:42.136Z",
12      "instance_id": [REDACTED],
13      "start_time": "2023-03-24T02:51:40.94Z",
14      "started_by": "[REDACTED]",
15      "succeeded": true
16    }
17  }
18 }
```

Two red text boxes provide instructions: '実行がエラーなく成功すると緑色になる。' (Execution becomes green when successful without error) and 'クリックするとJSON Outputを確認できる。' (Clicking allows you to check the JSON Output).

Step4 イベント情報取得



Activitiesから“Umbrella – Reporting v2 – Get Activity”を選択



SecureX-TEST

Modified: 2023年3月24日 at 7:01:59 Validated Commit View Runs Run

Search activities

Umbrella - Management - Remove Record from Destination List

Umbrella - Reporting - Get Security Activity Report

Umbrella - Reporting v2 - Get Activity

Umbrella - Reporting v2 - Get Categories

Umbrella - Reporting v2 - Get Token

Umbrella - Reporting v2 - Get Top Internal IPs

Umbrella - Reporting v2 - Get Top Threats

CISCO WEBEX

DATABASE

EMAIL

START

ATOMIC

Umbrella - Reporting v2 - Get Token

PROPERTIES

SecureX-TEST

Version

Git Repository

Select

Git Version

No Versions Available

General

Display Name

SecureX-TEST

Owner

naogawa@cisco.com

Description

Clean up after successful execution

If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

Is atomic workflow

An atomic workflow will be listed under the Activity Group header you select or create in the list to the left.

「CISCO UMBRELLA配下の」"Umbrella – Reporting v2 – Get Activity"を”END”上の + へDrag&Drop
※Drag&Dropする際、表示は + > ✓ となる

Get Activityに各種パラメータを入力する

**Activity Typeを指定
"dns" (小文字で記入)**

**マルウェアを提供または感染の疑いある
WebサイトのCategory IDを指定
例)66, 67 = Malware
(*IDの確認方法はP61,62に記載)**

**レポート取得期間の設定
"今"から"過去1日間"の情報を取得**

**UmbrellaのOrganization IDを入力
(*IDの確認方法はP60に記載)**

取得するUmbrella Activityの件数のリミットを指定

**TargetにStep2で作成した
レポート用のTargetを選択**

**クリックして、Umbrella Get TokenのAccess
Tokenを選択**

SecureX-TEST
Modified: 2023年3月24日 at 11:09:26
Validate Commit View Runs Run

Search activities
CORE
Calculate Date
Calculate Date Time Difference
Convert Json to Xml
Convert Xml to Json
Escape Regex Metacharacters
Find String
Match Regex
Replace String

START
END

ATOMIC
Umbrella - Reporting v2 - Get Activity

PROPERTIES: UMBRELLA - REPORTING V2 - GET ACTIVITY
Umbrella - Reporting V2 - Get Activity 1 WARNING

Workflow
Umbrella - Reporting v2 - Get Activity

* INPUT
Activity Type
dns

Additional Parameters
categories=66,67

* To Time
now

* Limit
5

* Offset
0

* Organization ID
XXXXXX

* Access Token
[Sactivity.Umbrella - Reporting v2 - Get Token.output.Access Token]

* From Time
-1days

PROPERTIES: UMBRELLA - REPORTING V2 - GET ACTIVITY
Umbrella - Reporting V2 - Get Activity

Target

* Target
* Target Type
HTTP Endpoint

No target
 Execute on this target
 Use workflow target

Override workflow target
* Target
Umbrella_Report

Execute on this target group
Target Group

Browse Variables

Search variable

Activities > Umbrella - Reporting v2 - Get Token > Elapsed time (seconds) DECIMAL
Env > End time DATE
Global > Start time DATE
Workflow > Succeeded BOOLEAN
Expires in INTEGER

Access Token SECURE STRING

実行確認

①Validateをクリック

②実行確認

The screenshot displays the SecureX-TEST interface. At the top, a blue header bar contains the title "SecureX-TEST", a modification timestamp "Modified: 2023年3月24日 at 11:09:26", and several buttons: "Validated" (highlighted with a red box), "Commit", "View Runs", "Run" (highlighted with a red box), a settings gear icon, and a close "X" icon. On the left, a sidebar lists various activities under the "CORE" category, including "Calculate Date", "Calculate Date Time Difference", "Convert Json to Xml", "Convert Xml to Json", "Escape Regex Metacharacters", "Find String", "Format Date", "JSONPath Query", "Match Regex", "Parse Date", "Replace String", "Set Variables", "Sleep", "Split String", and "Substring". The main workspace shows a workflow diagram starting with a "START" node, followed by an "ATOMIC" activity "Umbrella - Reporting v2 - Get Token", then another "ATOMIC" activity "Umbrella - Reporting v2 - Get Activity" (highlighted in blue), and ending at an "END" node. On the right, the "PROPERTIES: UMBRELLA - REPORTING V2 - GET ACTIVITY" panel is visible, showing configuration options for "Target" (with "Override workflow target" selected and "Umbrella_Report" chosen) and "Credentials" (with "Use target's default account keys" selected).

(参考)

UmbrellaのActivity APIについて

- <https://developer.cisco.com/docs/cloud-security/#!activity-all>

Documentation > Cloud Security API

Reporting API Reference

Overview

API

Activity

- GET Activity (all)
- GET Activity DNS
- GET Activity Proxy
- GET Activity Firewall
- GET Activity Intrusion
- GET Activity IP
- GET Activity AMP Retrospective

- Top Identities
- Identity Distribution
- Top Destinations
- Top Categories
- Top Event Types
- Top DNS query types
- Organization Requests by Hour
- Organization Requests by Timerange
- Organization Requests by Hour and Category
- Organization Requests by Timerange and Category
- Deployment Status
- MSP Deployment Status
- MSP Requests by Hour
- MSP Requests by Timerange

Activity

Activity (all)

Operation ID: getActivity

Description: List all activity entries (dns/proxy/firewall/intrusion) within the timeframe.
Note: The IP activity report is not available.

GET /organizations/{organizationid}/activity

Request Parameters

Path

organizationid ^{required} | number

The organization ID

Query

from ^{required} | string

A timestamp or relative time string (for example: '-1days').
Filter for data that appears after this time.

to ^{required} | string

A timestamp or relative time string (for example: 'now').
Filter for data that appears before this time.

Documentation > Cloud Security API

offset | number

A number that represents an index into the collection.

limit ^{required} | number

The maximum number of records to return from the collection.

domains | string

A domain name or comma-delimited list of domain name.

uris | string

A URL or comma-delimited list of URL.

categories | string

A category ID or comma-delimited list of category ID.

polycategories | string

A category ID or comma-delimited list of category ID.
Filter request by the categories that trigger a policy.

ip | string

An IP address

ports | string

A port number or comma-delimited list of port number.

Documentation > Cloud Security API

identityids | string

An identity ID or comma-delimited list of identity ID.

identitytypes | string

An identity type or comma-delimited list of identity type.

applicationid | string

An application ID.

verdict | string

A verdict string or comma-delimited list of verdict string.

ruleid | number

A firewall policy rule ID.

filename | string

A string that identifies a filename. Filter request by the filename.
Supports globbing or use of the wildcard character (*). The asterisk (*) matches zero or more occurrences of any character.

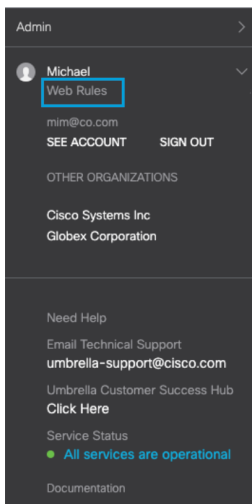
securityoverridden | boolean

Specify whether to filter on requests that override security.

(参考)Umbrellaのorganization IDの確認方法について

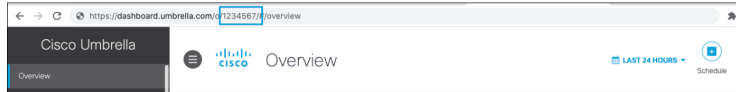
Procedure

1. Cisco Umbrellaにログインします(<https://dashboard.umbrella.com>)。
2. ナビゲーションメニューからアカウント名を展開し、正しいCisco Umbrellaダッシュボードにログインしていることを確認します。組織名はアカウント名の下に表示されます。
アクセスできる他の組織は以下にリストされています。 **その他の組織**.



- <https://docs.umbrella.com/deployment-umbrella/docs/find-your-organization-id>

3. 正しいダッシュボードにログインしたら、アドレスバーのURLを確認します。
`https://dashboard.umbrella.com/<*>OrgID>/#/<*>page*> . <OrgID> represents your unique Umbrella Org ID.`



(参考)

UmbrellaのCategory IDについて

- セキュリティカテゴリについて
 - Umbrella にはマルウェアなど 8 種類のセキュリティ カテゴリが用意されており、個々のカテゴリをブロックするか否かをポリシーの中で設定できます。
 - <https://community.cisco.com/t5/tkb-セキュリティ-ドキュメント/umbrella-各セキュリティ-カテゴリの説明/ta-p/3222902#toc-hld-378582300>
 - <https://docs.umbrella.com/deployment-umbrella/docs/dns-security-categories>
- Category ID はAPIで取得可能
 - <https://developer.cisco.com/docs/cloud-security/#!get-categories>

(参考)

UmbrellaのCategory ID取得方法（詳細）

1. こちらの記事 or P43 を参考に”Access Token”を取得

- <https://community.cisco.com/t5/-/-/ta-p/4684042>

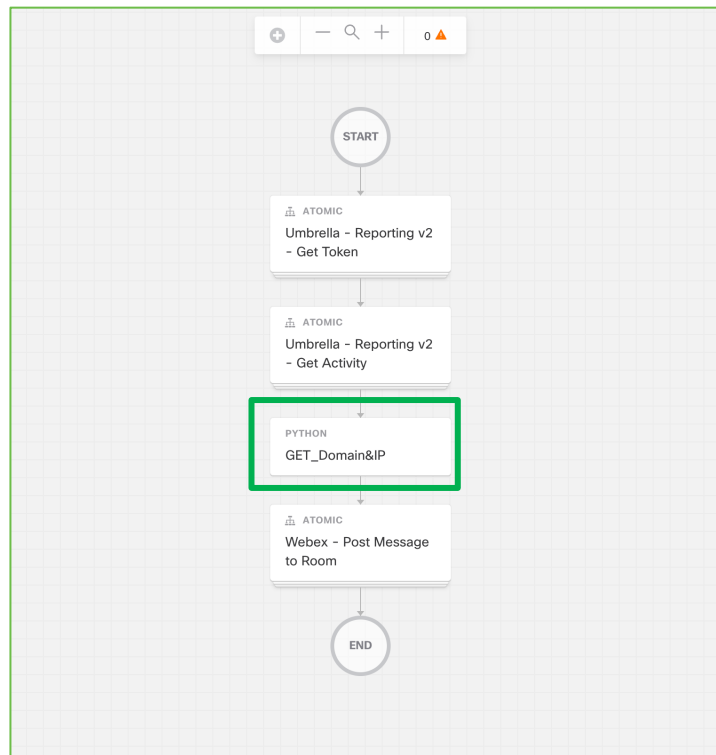
2. curlであれば以下のフォーマットで取得可能

```
curl --location --location-trusted ¥  
--request GET --url 'https://reports.api.umbrella.com/v2/organizations/⟨⟨org id⟩⟩/categories' ¥  
-H 'Authorization: Bearer <<access token>>' ¥  
-H 'Content-Type: application/json'
```

3. postmanであれば



Step5 ドメイン/IPアドレスを抽出



Activitiesから”Execute Python Script”を選択

SecureX-TEST

Modified: 2023年3月24日 at 11:51:40

Validated Commit View Runs Run

Search activities

- Get Top Internal IPs
- Umbrella - Reporting v2
 - Get Top Threats
- CISCO WEBEX
- DATABASE
- EMAIL
- FILE OPERATIONS
- GOOGLE CLOUD PLATFORM
- KENNA
- MERAKI
- MICROSOFT WINDOWS
- Execute Python Script**
- SNMP
- TABLE
- TASK
- TERMINAL
- TERRAFORM
- UNIX/LINUX SYSTEM
- WEB SERVICE

START

ATOMIC Umbrella - Reporting v2 - Get Token

ATOMIC Umbrella - Reporting v2 - Get Token

END

PROPERTIES

SecureX-TEST

Version

Git Repository

Git Version

General

Display Name

Owner

Description

Clean up after successful execution

Is atomic workflow

Group Name

Execute Python Script’を”END”上の + へ Drag&Drop

Display Nameを入力

The screenshot displays a workflow editor interface. On the left, a vertical flowchart shows the workflow steps: a circular 'START' node, followed by two 'ATOMIC' steps labeled 'Umbrella - Reporting v2 - Get Token' and 'Umbrella - Reporting v2 - Get Activity', and finally a 'PYTHON' step labeled 'Get_Domain&IP'. The 'PYTHON' step is highlighted in orange. On the right, the configuration panel for the 'EXECUTE PYTHON SCRIPT' activity is shown. The 'Display Name' field is highlighted with a red border and contains the text 'Get_Domain&IP'. Other fields include 'Description' (empty), 'Activity timeout (seconds)' (set to 180), and two checkboxes: 'Continue Workflow Execution On Failure' and 'Skip activity execution'.

Display Nameを入力

下記のPythonスクリプトを入力

```
import json

umb_data =

response_report = json.loads(umb_data)

domainlist = []
iplist = []

if len(response_report["data"]) == 0:
    message_umb = "安心してください。最近悪意あるドメインにはアクセスしていません。" + "\n"
else:
    message_umb = "次のドメインは悪意あるドメインの可能性があります。ご注意ください。" + "\n"
    for i, domain in enumerate(response_report["data"]):
        domainlist.append(response_report["data"][i]["domain"])
        iplist.append(response_report["data"][i]["internalip"])
    domainlist = list(set(domainlist))
    domainlist_str = str("\n".join(domainlist))
    message_umb += domainlist_str
    message_umb += "\n" + "次のIPは悪意あるドメインに通信している可能性があります。ご注意ください。" + "\n"
    iplist = list(set(iplist))
    iplist_str = str("\n".join(iplist))
    message_umb += iplist_str

print(message_umb)
```

```
3 umb_data = '$Report'
4
5 re
6
7 do
8 ip
```

ACTIVITIES

Report Data

Activities > Umbrel ... ng v2 - Get Activity

umb_dataはVariablesからUmbrella Get ActivityのReport Dataを選択。
シングルクォテーション x 2(")を入力後、その間に「\$Report」を入力すると選択可能。
注意: 必ず「'」と「\$Report」の文字は手入力。コピペしてもポップアップは出てきません!

```
1 import json
2
3 umb_data = '[$activity.Umbrella - Reporting v2 - Get Activity.output.Report Data$]'
4
5 response_rep
6
7 domainlist =
8 iplist = []
9
10 if len(response_report["data"]) == 0:
11     message_umb = "安心してください。最近悪意あるドメインにはアクセスしていません。" + "\n"
12 else:
13     message_umb = "次のドメインは悪意あるドメインの可能性があります。ご注意ください。" + "\n"
```

正しく選択できるとこのような形で表示される

ここにコピペ

Python

SCRIPT OUTPUT VARIABLESを登録

SecureX-TEST Modified: 2023年3月27日 at 15:44:59

② "Validate"をクリック

③ "Run"をクリック

① SCRIPT OUTPUT VARIABLESに"message_umb"を登録

```
7
8 domainlist = []
9 iplist = []
10
11 if len(response_report["data"]) == 0:
12 message_umb = "安心してください。最近悪意あるドメインにはアクセスしていません。" + "\n"
13 else:
14 message_umb = "次のドメインは悪意あるドメインの可能性があります。ご注意ください。" + "\n"
15 for i, domain in enumerate(response_report["data"]):
16 domainlist.append(response_report["data"][i]["domain"])
17 iplist.append(response_report["data"][i]["internalip"])
18 domainlist = list(set(domainlist))
19 domainlist_str = str("\n".join(domainlist))
20 message_umb += domainlist_str
21 message_umb += "\n" + "次のIPは悪意あるドメインに通信している可能性があります。ご注意下
22 iplist = list(set(iplist))
23 iplist_str = str("\n".join(iplist))
24 message_umb += iplist_str
25
26 print(message_umb)
27
```

SCRIPT OUTPUT VARIABLES

* Script Variable

message_umb

Property Name

message_umb

* Property Type

String

+ ADD

Step5 実行結果

SecureX-TEST Run **SUCCESS**
Version 1.0.0

最後に必ず"Modify"をクリック

Properties: EXECUTE PYTHON SCRIPT
GET_Domain&IP

message_umb

Property Name
message_umb

* Property Type ●
String

+ ADD

Output

Start time
Mon Mar 27 2023 16:09:43 GMT+0900 (日本標準時)

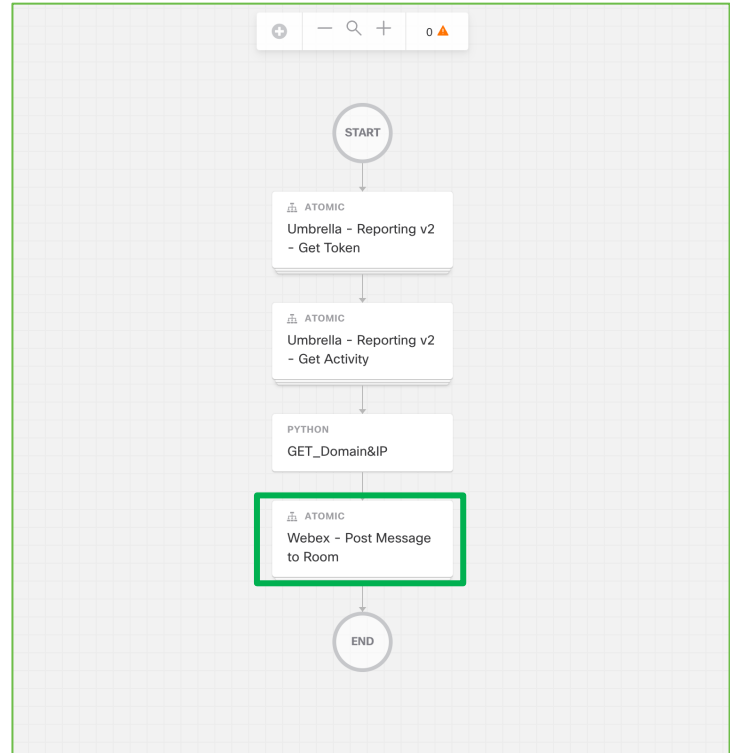
End time
Mon Mar 27 2023 16:09:43 GMT+0900 (日本標準時)

Elapsed time (seconds)
0.031114999

Response body
次のドメインは悪意あるドメインの可能性がります。ご注意ください。
examplemalwaredomain.com
www.examplemalwaredomain.com
次のIPは悪意あるドメインに通信している可能性があります。ご注意ください。
192.168.0.17

Succeeded

Step6 Webex スペースへポスト



Variablesを登録

The screenshot shows the SecureX-TEST interface. On the left is a sidebar with activity categories like 'CORE' and 'Calculate Date'. The main area displays a workflow diagram with steps: START, 'Umbrella - Reporting v2 - Get Token', 'Umbrella - Reporting v2 - Get Activity', 'PYTHON GET_Domain&IP', and END. On the right, the 'PROPERTIES' panel for 'SecureX-TEST' is visible. The 'Variables' section is highlighted with a red box and contains a table with columns: NAME, TYPE, SCOPE, VALUE, and REQUIRED. Below the table is a '+ ADD VARIABLE' button. A red arrow points from a text box containing the instruction 'ADD VARIABLE'をクリック to this button. Other sections in the properties panel include 'Group Name', 'Category', '+ ADD TRIGGER', 'Target', and 'Target Type'.

※前Stepで最後に右上の"Modify"をクリックしていないとこちらの画面に戻らないため注意

事前準備で取得したWebexのBot Access TokenとSpaceIDの2つをVariablesとして登録

① "ADD VARIABLE"をクリック

NAME	TYPE	SCOPE	VALUE	REQUIRED
Bot Access Token	Secure String	Static	*****	False
Webex Room ID	String	Static	L3VzL1JPT00vZDY 5MTA3ZDAY2NkNI 0AMVWVLMWESZTYt YTU3MzM4ZDRmZ	False

Variableは計2つ登録
1. "ADD VARIABLE"をクリック > Bot Access Tokenを登録
2. "ADD VARIABLE"をクリック > Space IDを登録
※画面上では"Webex Room ID"とありますが、本資料のSpaceIDと読み替えてください。

New Bot Access Token

Data Type **Secure String**を選択

General **Display Name**を入力

Scopeは固定変数のため"Static"を選択

"Value"の欄にP33で取得したBot Access Tokenを入力

New Webex Room ID

Data Type String

General **Display Name**を入力

Scopeは固定変数のため"Static"を選択

"Value"の欄にP37で取得したSpaceIDを入力

Activitiesから“Webex – Post Message to Room”を選択

SecureX-TEST Modified: 2023年3月27日 at 16:30:29 Validated Commit View Runs Run

Search activities

- Get Top Internal IPs
- Umbrella - Reporting v2 - Get Top Threats
- CISCO WEBEX
 - Webex - Add Member to Room
 - Webex - Create Room**
 - Webex - Post Message to Room**
 - Webex - Search for Room
 - Webex - Search for Team
 - Webex - Send Message to User
- DATABASE
- EMAIL
- FILE OPERATIONS
- GOOGLE CLOUD PLATFORM
- KENNA
- MERAKI
- MICROSOFT WINDOWS

START

ATOMIC Umbrella - Reporting v2 - Get Token

ATOMIC Umbrella - Reporting v2 - Get Activity

PYTHON GET_Domains

END

PROPERTIES SecureX-TEST

Version

Git Repository Select

Git Version No Versions Available

General

Display Name SecureX-TEST

Owner naogawa@cisco.com

Description

Clean up after successful execution
If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

Is atomic workflow ●
An atomic workflow will be listed under the Activity Group header you select or create in the list to the left.

Group Name ●
Select

“Webex – Post Messages to Room”を“END”上のへDrag&Drop

CISCO

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Webex Teams の Bot Access Token, Room ID、Postするメッセージを設定

SecureX-TEST Modified: June 22, 2023 at 11:04:29 AM Validate Commit View Runs Run

Workflow: Webex - Post Message to Room

- * INPUT
- Markdown Message
- * Access Token: [\${workflow.SecureX-TEST.static.Bot access token\$}]
- * Room ID: [\${workflow.SecureX-TEST.static.Webex Room ID\$}]
- Plain Text Message: [\${activity.Get_Domain&IP.output.Script Queries.message_umb\$}]
- Attachments
- Target
 - * Target
 - * Target Type
 - HTTP Endpoint
 - No target
 - Execute on this target
 - Use workflow target
 - Override workflow target
 - * Target: Webex Teams

- ① Access Tokenを選択
- ② Room IDを選択
- ③ Plain Textとして、Step5で登録した出力"message_umb"を選択

③ デフォルトで登録済みのWebex TeamsのTargetを選択

Browse Variables

Search variable

Activities > Static > Bot Access Token (SECURE STRING)

Env > Output > Webex Room ID (STRING)

Global >

Workflow >

Cancel Save

Browse Variables

Search variable

Activities > Static > Bot Access Token (SECURE STRING)

Env > Output > Webex Room ID (STRING)

Global >

Workflow >

Cancel Save

Browse Variables

Search variable

Activities > Umbrella - Reporting v2 - Get Token (ATOMIC WORKFLOW) > End time (DATE)

Env > Umbrella - Reporting v2 - Get Activity (ATOMIC WORKFLOW) > Response body (STRING)

Global > Get_Domain&IP (SCRIPT) > Start time (DATE)

Workflow > message_umb (STRING)

Script Queries >

Pro Tip: Type \$ in the form field to more quickly insert variable references.

Cancel Save

Step6 実行結果

The screenshot displays the SecureX workflow execution interface. At the top, it shows 'SecureX-TEST Run SUCCESS' with a 'Version 1.0.0' and a 'RUN TIME' of '3.2 s'. A 'Modify' button and a play button are also visible.

The workflow diagram shows a sequence of tasks:

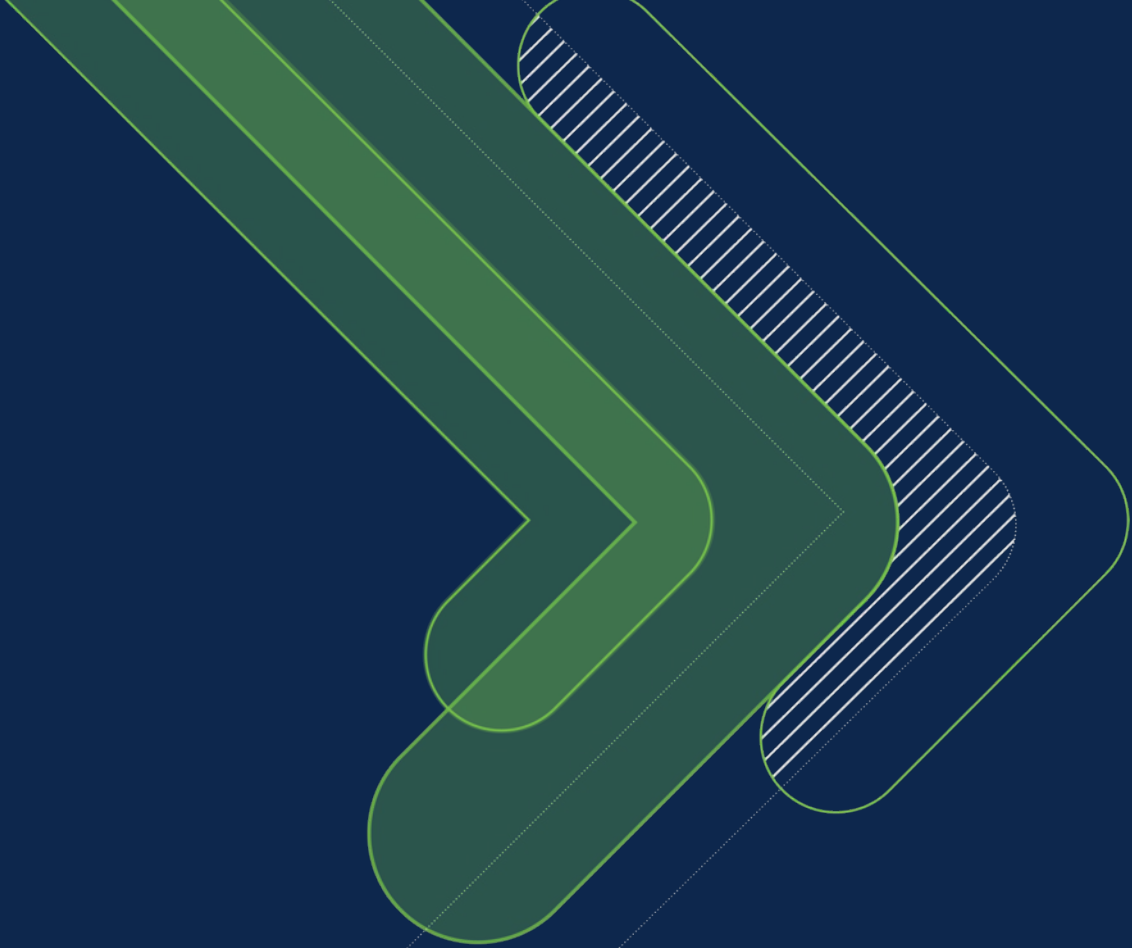
- START
- ATOMIC: Umbrella - Reporting v2 - Get Token
- ATOMIC: Umbrella - Reporting v2 - Get Activity
- PYTHON: GET_Domain&IP
- ATOMIC: Webex - Post Message to Room
- END

The 'PROPERTIES' panel for 'SecureX-TEST' includes:

- Version: No Versions Available
- Git Repository: Select
- Git Version: No Versions Available
- General: Display Name 'SecureX-TEST', Owner 'naogawa@cisco.com'
- Description: (Empty)
- Options: Clean up after successful execution

The message log on the right shows three messages from 'SecureX' at 11:18, 12:50, and 12:53. Each message contains a warning about a potential malicious domain and provides the IP address '192.168.0.10' and '192.168.0.10'.


4. Trigger




Triggerタイプ

- Triggerとは作成したWorkflowを自動的に発動させるキッカケとなる設定
- Triggerには”Event”と”Schedule”の2種類が存在

1. Event

- イベントは、何かが起こるのを待つ条件付きのアクティビティです。設定された条件が満たされると、そのイベントをトリガーとして使用するすべてのワークフローが実行されます。
- Orchestration > Events&Webhooks()から設定可能

2. Schedule ← 本資料ではこちらの設定のみ解説

- スケジュールは、ワークフローを実行する時間を定義します。開始時間、実行間隔、1日の実行回数を指定することができます。
- Orchestration > Schedule()から設定可能

新規Schedule作成

The screenshot shows the Cisco SecureX Orchestration interface. The navigation menu at the top includes Dashboard, Integration Modules, Orchestration (highlighted with a red box and circled 1), Insights, and Administration. The left sidebar contains several menu items: Workflows, Runs, Targets, Account Keys, Variables, Calendars, and Schedules (highlighted with a red box and circled 2). The main content area displays "No Schedules found." with a "New Schedule" button highlighted by a red box and circled 3.

Orchestration > Schedules > New Scheduleをクリック

新規Schedule設定

The screenshot shows a configuration window titled "New Umbrella_Report_Schedule" with a close button (X) in the top right corner. The window is divided into several sections:

- Select Type:** A dropdown menu with "Generic Schedule" selected. A green arrow points to this dropdown with the text "Generic Scheduleを選択".
- General:**
 - Display Name:** A text input field containing "Umbrella_Report_Schedule". A green arrow points to this field with the text "任意の名前 ex. Umbrella_Report_Schedule".
 - Description:** A text area containing "Daily umbrella report".
- Schedule:**
 - * Calendar:** A dropdown menu with "Daily" selected. A green arrow points to this dropdown with the text "日次、週次、毎週月曜など様々な形で実行時間を指定可能".
 - * Timezone:** A dropdown menu with "(UTC+09:00) Osaka, Sapporo, Tokyo" selected. A green arrow points to this dropdown with the text "タイムゾーン".
 - * Start Time:** A time input field showing "10:00 AM". A green arrow points to this field with the text "開始時間を定義(今回は日次となるため、毎日10:00AMに実行のイメージ)".
 - * Number of runs per day:** A dropdown menu with "1" selected. A green arrow points to this dropdown with the text "1日あたりの実行回数とインターバル。左図では日次で1回となっているが、日次で2回実施、その際のインターバルを12時間みたいな設定も可能".
 - Time Interval (Run Every):** Two input fields for "HRS" and "MIN", both set to "0". A green arrow points to these fields.

On the right side of the window, there is a scrollable list of schedule types: Christmas, Daily, Easter (US), Every Friday, Every Monday, Every Saturday, Every Sunday, Every Thursday, Every Tuesday, Every Wednesday, and a "+ ADD NEW" link. A vertical scrollbar is visible next to this list.

At the bottom of the window, there are "Cancel" and "Save" buttons. The word "Confidential" is printed in the bottom right corner of the window area.

参考) 新規Schedule作成

New Trigger

×

Trigger

Name

Description

* Type

* Schedule

+ ADD NEW

Disable trigger

Triggers are enabled by default. You may want to disable a trigger for testing.

Cancel

Save

New Triggerのページからも新規
Schedule作成可能

Scheduleのプルダウンをクリック
“+ADD NEW”が表示されるのでクリック

Schedule Triggerの設定

SecureX-TEST Modified: May 22, 2023 at 5:38:27 PM Validated

Q Search activities X

START

ATOMIC Umbrella - Reporting v2 - Get Token

ATOMIC Umbrella - Reporting v2 - Get Activity

PYTHON Execute Python Script

PROPERTIES SecureX-TEST

Variables

NAME	TYPE	SCOPE
Bot access token	Secure String	Static
Webex Room ID	String	Static

+ ADD VARIABLE

Triggers

NAME	TYPE
+ ADD TRIGGER	

ワークフロー編集画面右側
“PROPERTIES”配下の“Triggers”
+ADD TRIGGERをクリック

新規Trigger設定

New Trigger: **SecureX_Umbrella**



Trigger

Name

SecureX_Umbrella

← 任意の名前 ex. SecureX_Umbrella

Description

* Type

Schedule

← Scheduleを選択

* Schedule

Umbrella_Report_Schedule

← 前のページで作成したScheduleを選択

Disable trigger

Triggers are enabled by default. You may want to disable a trigger for testing.


Cancel

Save

Trigger設定確認

PROPERTIES
SecureX-TEST

Variables

NAME	TYPE	SCOPE	VALUE	REQUIRED
Bot access token	Secure String	Static	*****	False
Webex Room ID	String	Static		False

+ ADD VARIABLE

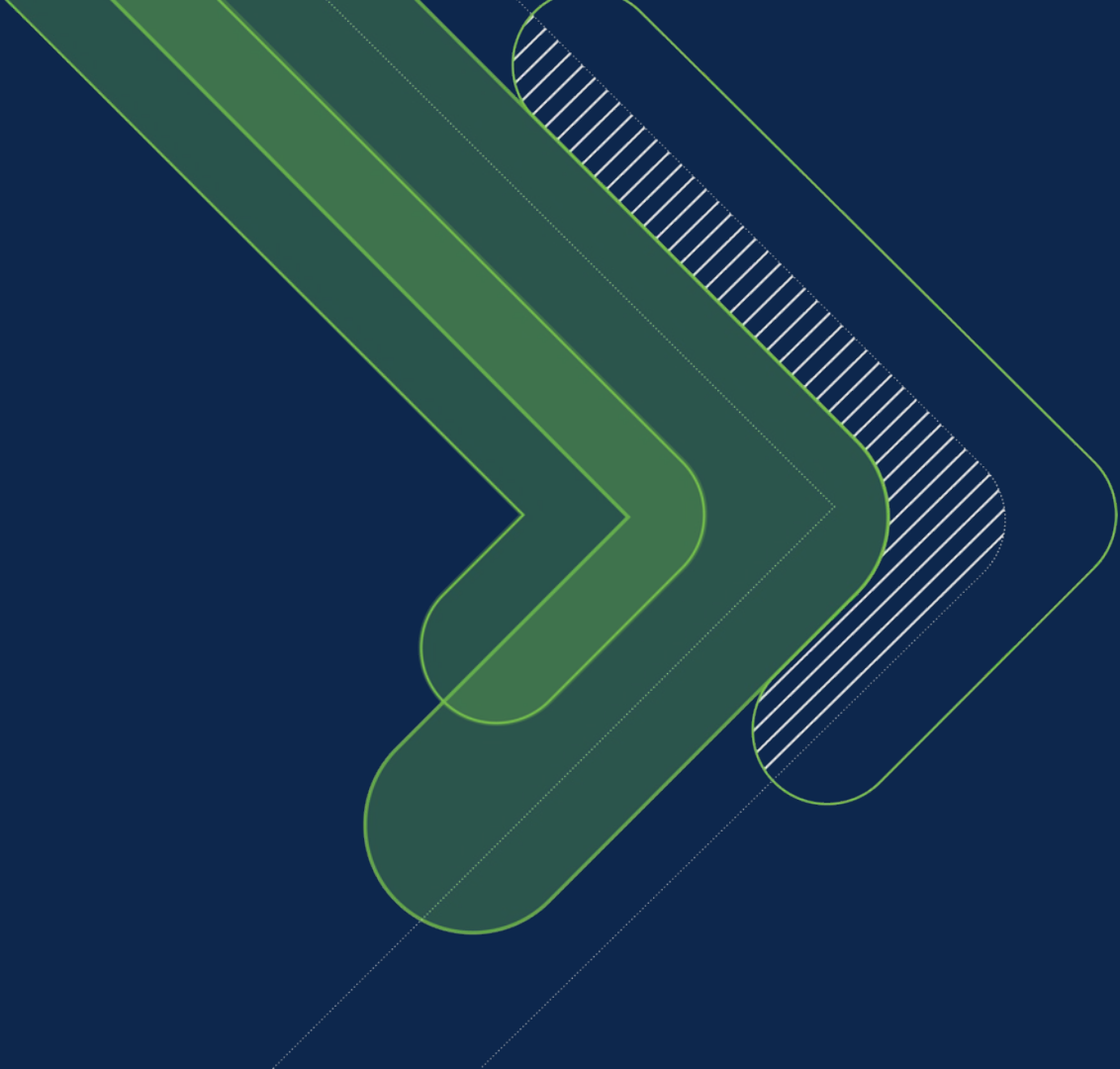
Triggers

NAME	TYPE	STATUS
SecureX_Umbrella	Schedule	Created

+ ADD TRIGGER

作成に成功するとSTATUS="Created"となり
PROPERTIES > Triggersに表示される

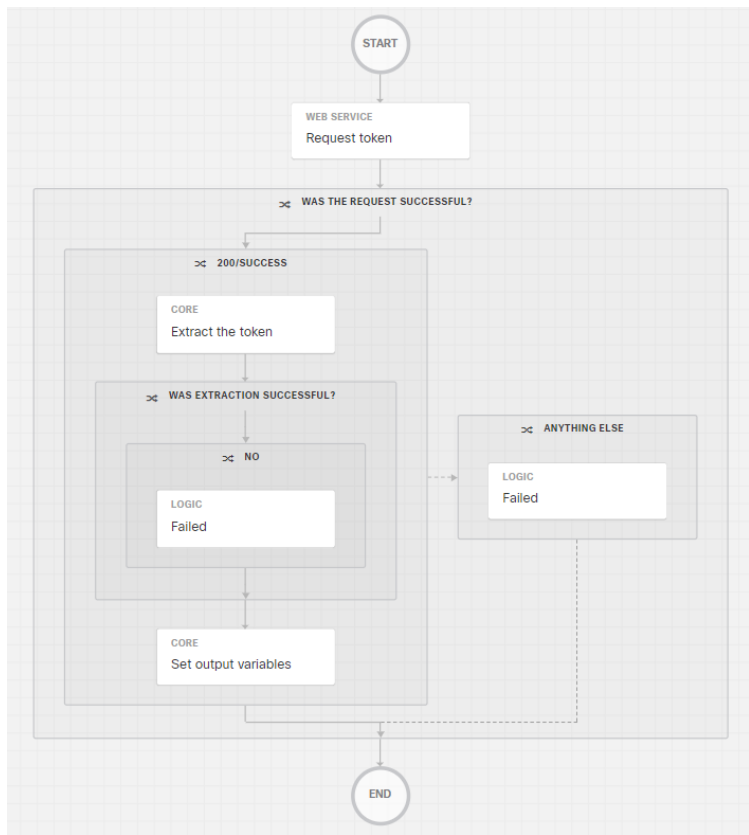
Activity



利用したActivityの説明

- Umbrella - Reporting v2 - Get Token
 - UmbrellaのTokenをGetするためのActivityです。
- Umbrella - Reporting v2 - Get Activity
 - 上記のTokenを使って、UmbrellaのReporting ActivityをGETするためのActivityです。
- Webex - Post Message to Room
 - Webex Teamsの特定のROOMにメッセージをPOSTするためのActivityです。

Umbrella - Reporting v2 - Get Tokenの中身



idential

- TokenをRequest
- HTTPレスポンスが200であれば、Tokenを抽出。
- Tokenの抽出に成功したら、Access Token変数にTokenをセット

Umbrella - Reporting v2 - Get Tokenの変数

PROPERTIES: Umbrella - Reporting V2 - Get Token 1 WARNING

General

Display Name
Umbrella - Reporting v2 - Get Token

Description

Continue Workflow Execution On Failure
Continue Workflow Execution On Failure

Skip activity execution
Skip activity execution

Workflow
Umbrella - Reporting v2 - Get Token

Target

* Target
* Target Type
HTTP Endpoint

No target

Execute on this target
Target
Select

Use workflow target
The Workflow is not configured to use target

Override workflow target

Execute on this target group
Target Group
Select

Use workflow target group

Override workflow target group criteria

Credentials

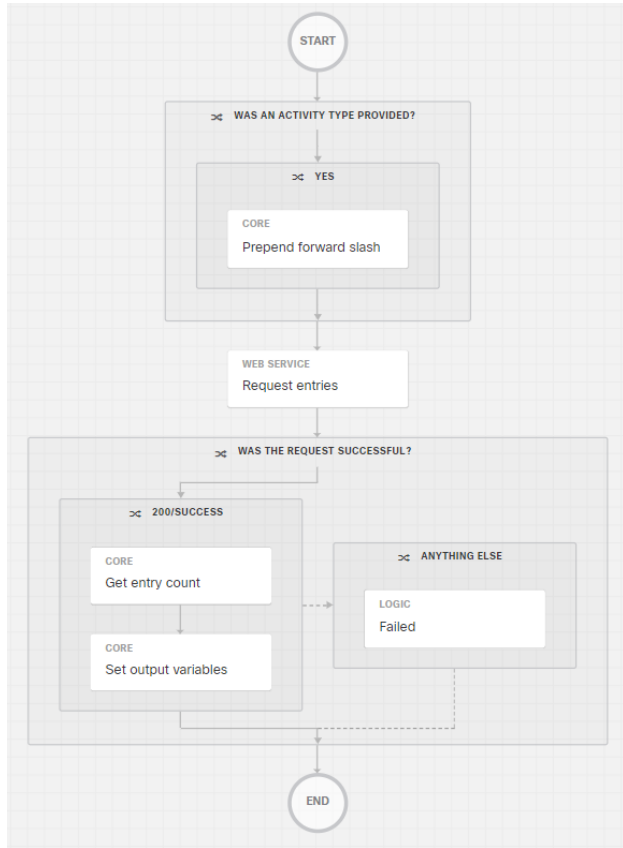
Account Key Type
Select

Use target's default account keys

Override account keys
Account Key Id
Select

- TargetとCredentialsに別途定義した適切な内容を入力

Umbrella - Reporting v2 - Get Activityの中身



- Activity Typeが提供されておれば、URL作成のため「/」を追加
- Reporting Endpointに対して、Get Tokenで取得したAccess Tokenをヘッダに挿入してRequest
- HTTPレスポンスが200であれば、エントリー数をGET
- さらにEntry Count変数とReport Data変数に値をセット

Umbrella - Reporting v2 - Get Activityの変数

PROPERTIES: Umbrella - Reporting V2 - Get Activity 5 WARNINGS

General

Display Name
Umbrella - Reporting v2 - Get Activity

Description

Continue Workflow Execution On Failure
Continue Workflow Execution On Failure

Skip activity execution
Skip activity execution

Workflow

* INPUT

Activity Type

Additional Parameters

* To Time

To Time is required

* Limit

* Offset

* Organization ID

Organization Id is required

* Access Token

Access Token is required

* From Time

From Time is required

Target

* Target
* Target Type
HTTP Endpoint

No target

Execute on this target
Target
Select

Use workflow target
The Workflow is not configured to use target

Override workflow target

Execute on this target group
Target Group
Select

Use workflow target group

Override workflow target group criteria

Credentials

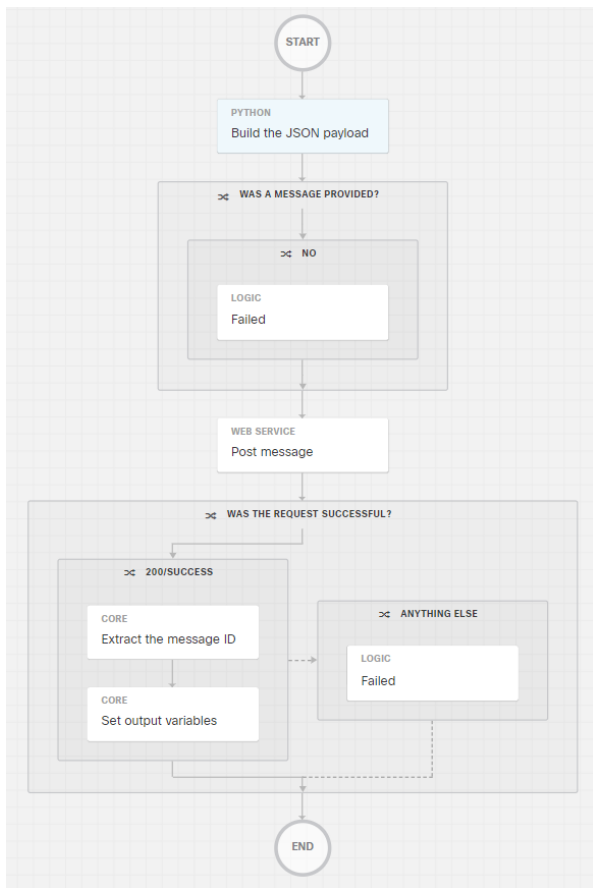
Account Key Type
Select

Use target's default account keys

Override account keys
Account Key Id
Select

- INPUT項目にはUmbrella Activity Reportから取得したいデータのパラメータ情報を入力(書式は下記URL参照)
- <https://developer.cisco.com/docs/cloud-security/#!reporting-v2-request-samples/request-samples>
- TargetとCredentialsに別途定義した適切な内容を入力

Webex - Post Message to Roomの中身



- Webex POSTに必要なRoomId、Text等の値をwebexObjectにセット
- メッセージが無い場合はFail
- WebexのAccess Tokenをヘッダに挿入してメッセージをPOST
- HTTPレスポンスが200であれば、Message IDを抽出
- さらにResponse Body変数とMessage ID変数に値をセット

Webex - Post Message to Roomの変数

PROPERTIES: WEBEX - POST MESSAGE TO ROOM
Webex - Post Message To Room 3 WARNING

General

Display Name
Webex - Post Message to Room

Description

Continue Workflow Execution On Failure
Continue Workflow Execution On Failure

Skip activity execution
Skip activity execution

Workflow

*** INPUT**

Markdown Message *

*** Access Token ***
Access Token is required

*** Room ID ***
Room Id is required

Plain Text Message *

Attachments *

Target

* Target
* Target Type
HTTP Endpoint

No target

Execute on this target
Target
Select

Use workflow target
The Workflow is not configured to use target

Override workflow target

Execute on this target group
Target Group
Select

Use workflow target group

Override workflow target group criteria

Credentials

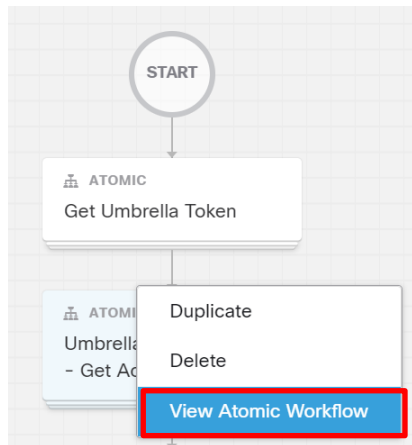
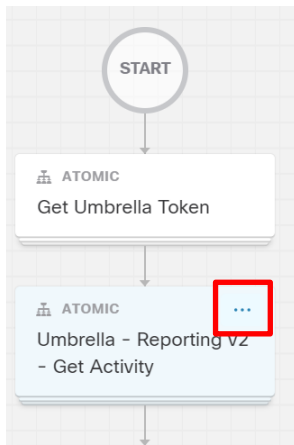
Account Key Type
Select

Use target's default account keys

Override account keys
Account Key Id
Select

- INPUT項目にはWebex TeamsにPOSTしたいRoomIdやメッセージ、Access Token等の情報を入力
- TargetとCredentialsに別途定義した適切な内容を入力

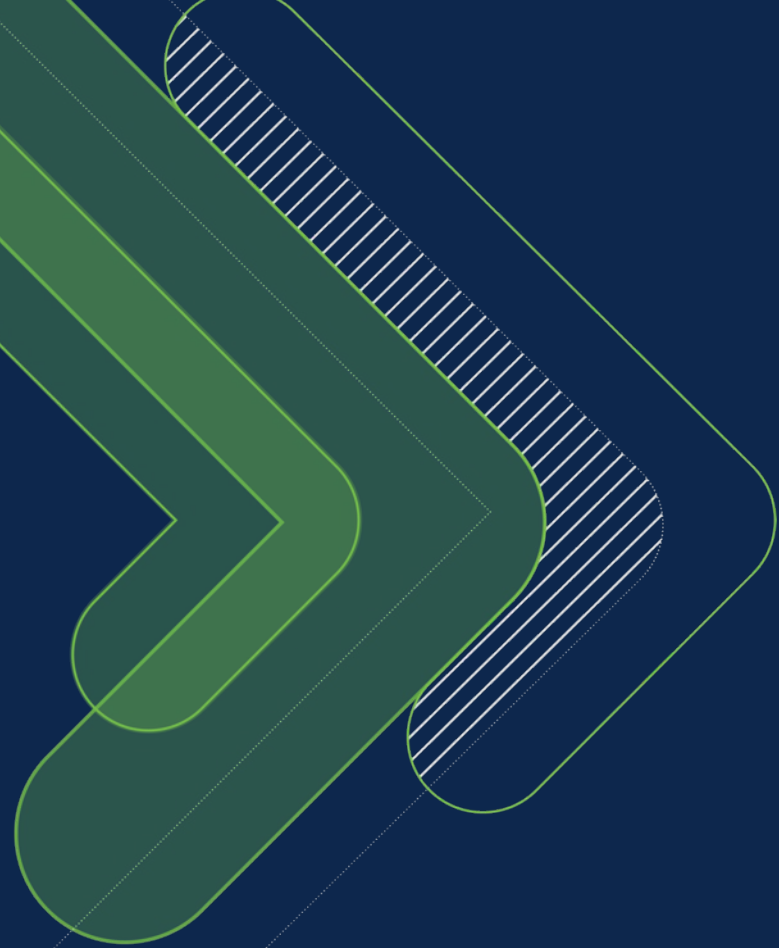
※本節に記載したAtomicsの中身の表示方法



Workflowの中の
Atomic Activityの箱の右上
にカーソルを持っていく

表示された...をクリックすると
プルダウンメニューが出てくるので、
View Atomic Workflowを選択

5. No Code開発

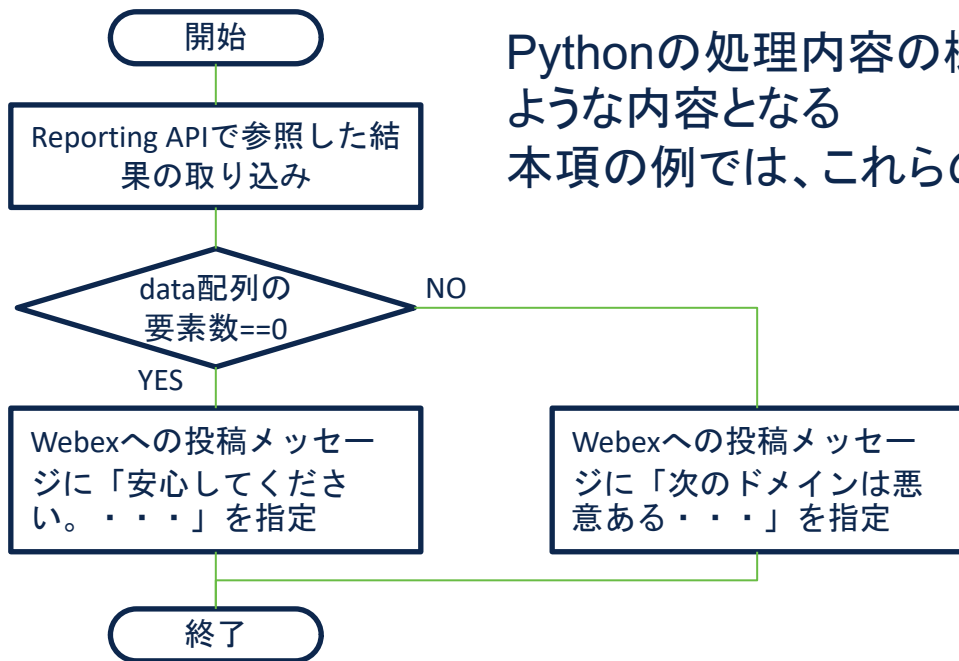


No CodeでWorkflowを構成する

SecureX Orchestrationでは、Pythonを使用せずとも、条件に応じた処理や、データの加工などを行うことが可能

本項では、前述の例でPythonで処理していた内容をNo Codeで実装する例を紹介

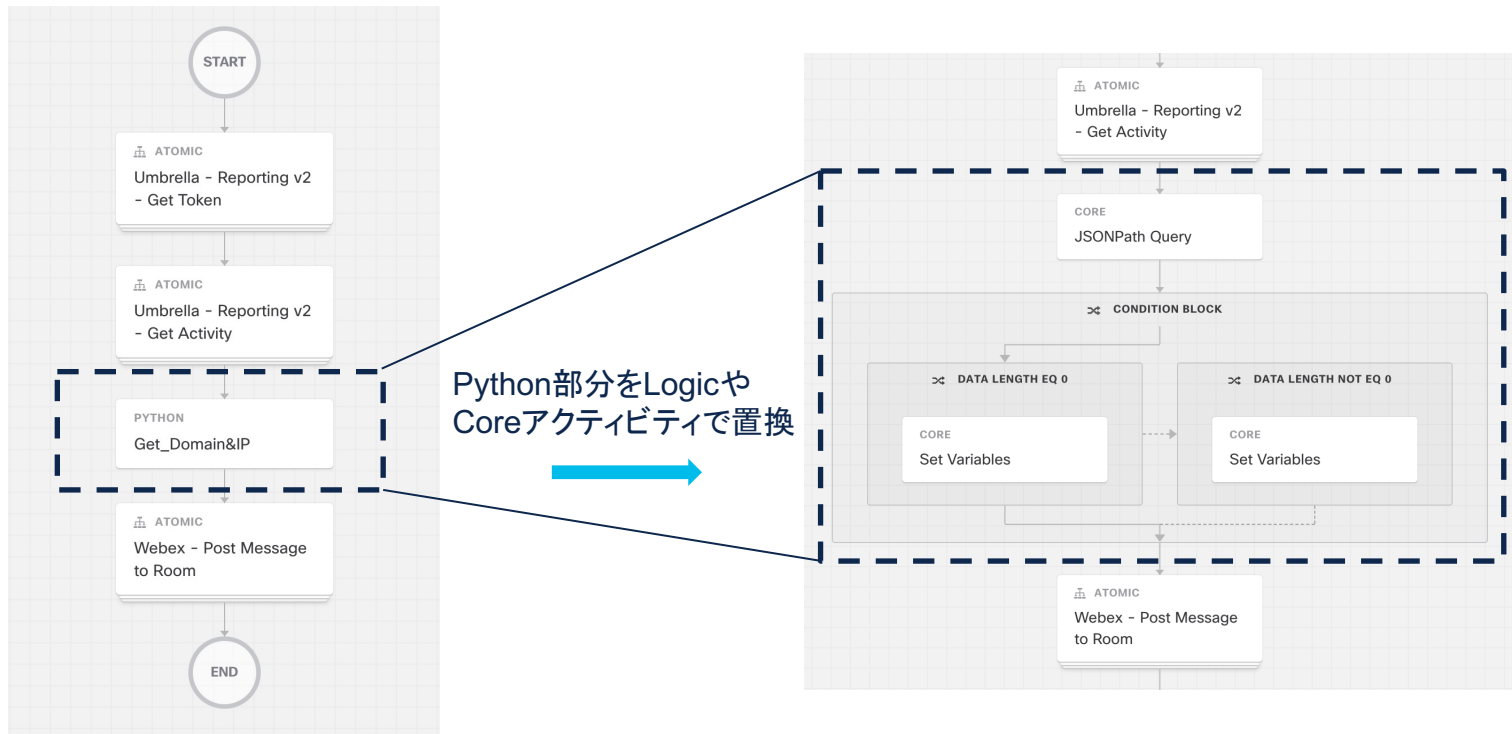
Pythonの処理内容



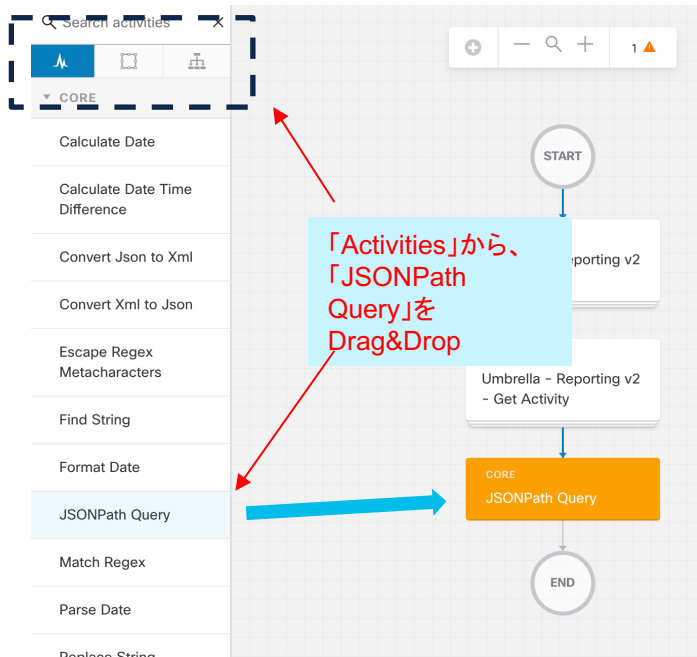
Pythonの処理内容の概要をフローチャートで表現すると左図のような内容となる

本項の例では、これらの処理をNo codeの形式に置換

PythonをNo codeに置き換え



data配列の要素数を取得



「Activities」から、「JSONPath Query」を Drag&Drop

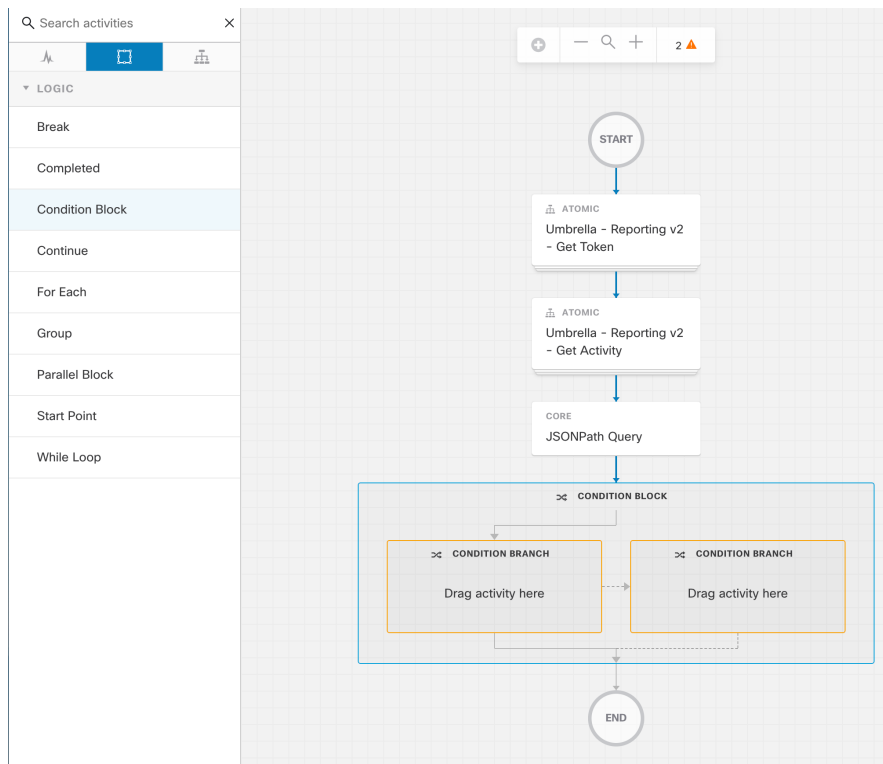
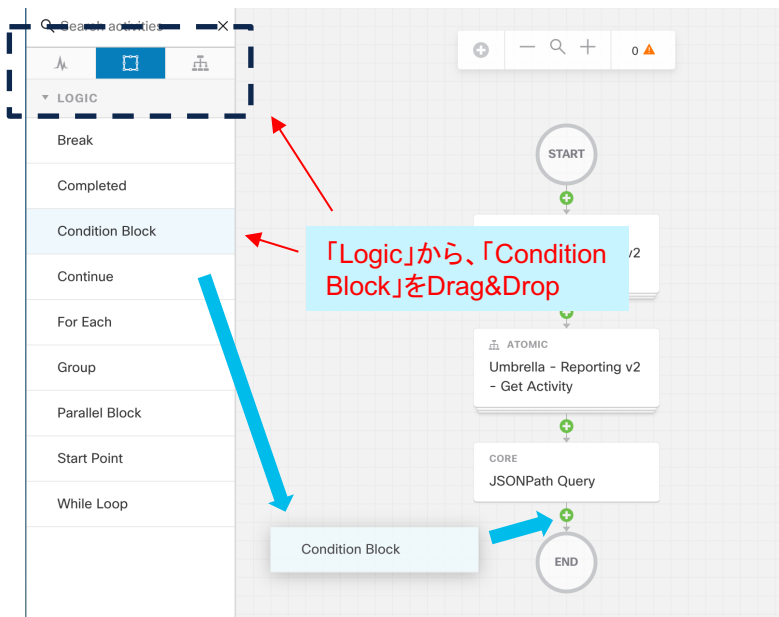
フローチャート中の条件分岐で使用するdata配列の要素数を取得。JSONPath Queryでは、JSONの文字列をそのまま処理可能なので、データの取り込み/加工処理は不要。

クリックして、Activities > Umbrella – Reporting v2 – Get Activity > Report Dataを選択

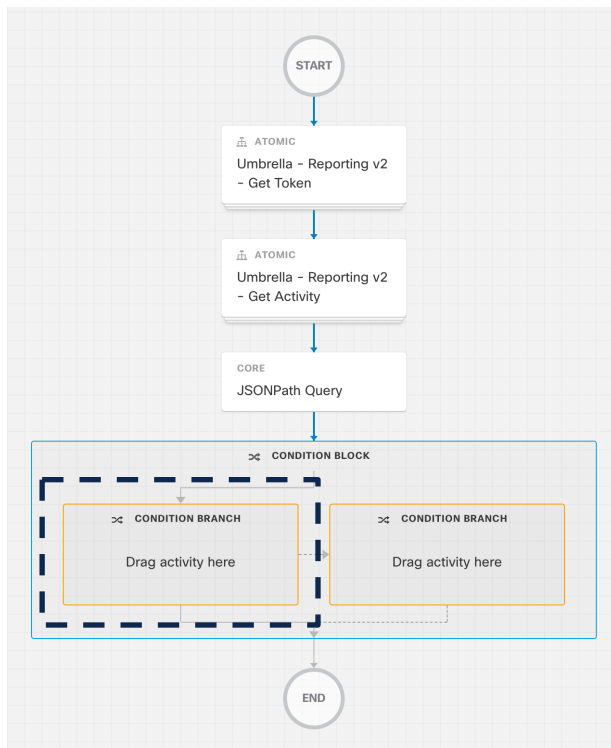
length関数を使用して、data配列の要素数を取得「\$.data.length()」を指定

保存先のプロパティ名称、タイプを指定

条件分岐を追加



第一条件 (左側) を指定



General

Display Name
data length eq 0

Description

Continue Workflow Execution On Failure
Continue Workflow Execution On Failure

Skip activity execution
Skip activity execution

Condition

Left Operand
[`$Activity.JSONPath Query.output.Jsonpath Queries.data_length$`]

Operator
Equals

Right Operand
0

+ ADD CONDITION

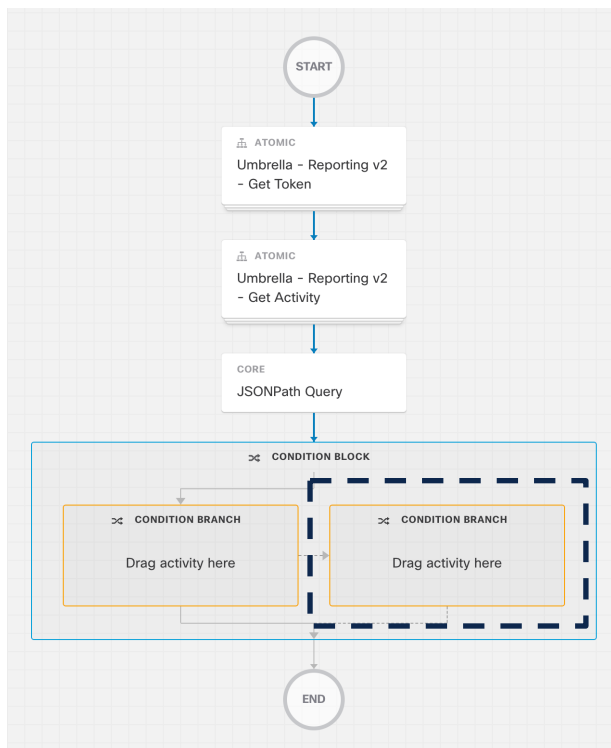
条件をフロー図から判別できるように表示名を変更

クリックして、Activities > JSONPath Query > Jsonpath Queries > data_lengthを選択

Equals (等価) を選択

data配列の要素がない場合を条件とするため、「0」を指定

第二条件 (右側) を指定



General

Display Name
data lengh not eq 0

Description

Continue Workflow Execution On Failure
Continue Workflow Execution On Failure

Skip activity execution
Skip activity execution

Condition

Left Operand
[`{activity.JSONPath Query.output.Jsonpath Queries.data_length$}` *]

Operator
Not equals

Right Operand
0 *

+ ADD CONDITION

条件をフロー図から判別できるように表示名を変更

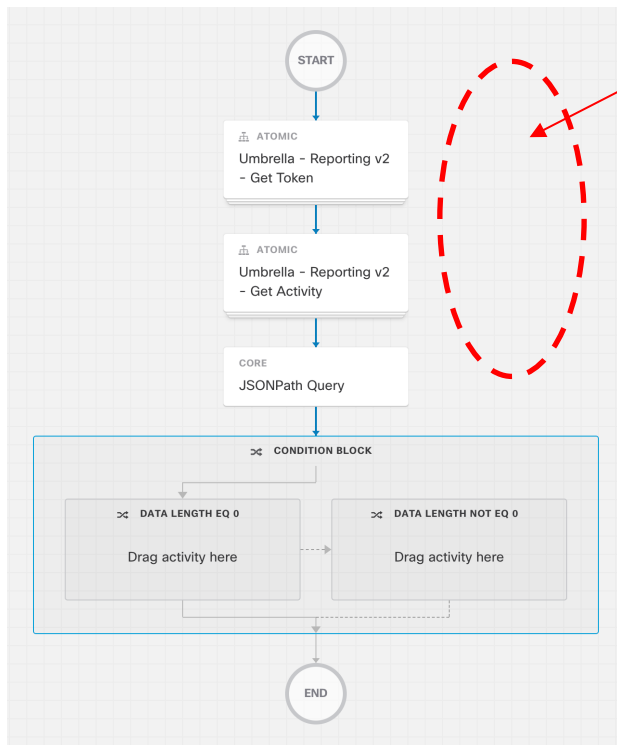
Condition blockではELSE条件が定義されていないため、何らかの条件を定義する必要があります。本例では第一条件の反意となる「data_length not eq 0」を指定。

クリックして、Activities > JSONPath Query > Jspath Queries > data_lengthを選択

Not equals (不等値) を選択

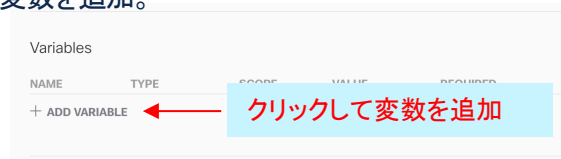
data配列の要素がない場合を条件とするため、「0」を指定

Webexに投稿する文字列を格納する変数を定義



【Workflowのローカル変数を追加】

編集画面の空白部分をクリックし、Workflow全体のプロパティ編集モードにした状態で以下の変数を追加。



New WebexPostString

Data Type

String

Stringを選択

General

Display Name

WebexPostString

変数名を指定

Description

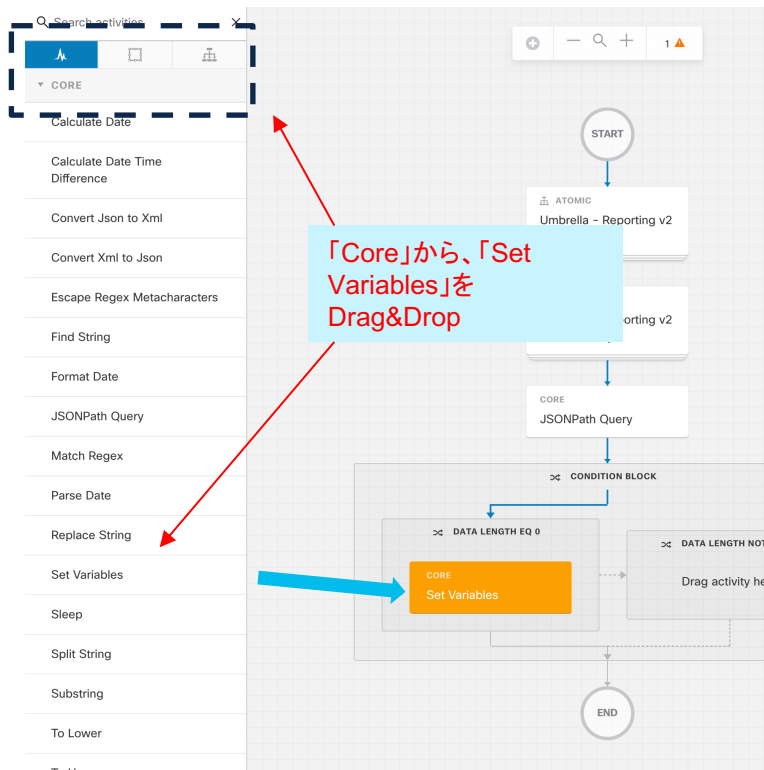
* Scope

Local

Workflowのローカル変数として定義

Value

脅威が観測されなかった場合のメッセージを指定



「Core」から、「Set Variables」を Drag&Drop

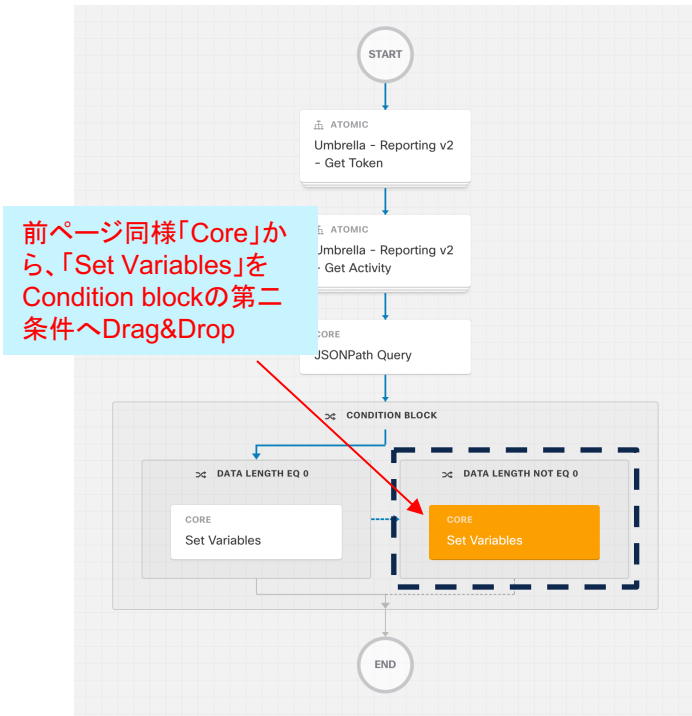
クリックして、更新する変数を追加

クリックして、Workflow > Local > WebexPostString を選択

The screenshot shows the 'Variables' configuration window. It has a section titled '*VARIABLES TO UPDATE'. Below this, there are two main fields: '* Variable to update' and 'New value'. The '* Variable to update' field contains the text `[$workflow.SecureX workflow - logic use case.local.WebexPostString$]`. The 'New value' field contains the Japanese text: '安心してください。最近悪意あるドメインにはアクセスしていません。'. Both fields have a gear icon to their right. Below these fields is a '+ ADD' button. Red arrows point from the text boxes above to these specific elements.

data配列の長さが0の場合、Report APIで取得した時間の範囲では、悪意あるサイトへのアクセスが観測されなかったことを示すため、その旨を通知するメッセージを指定。

脅威が観測された場合のメッセージを指定



クリックして、更新する変数を追加

クリックして、Workflow > Local > WebexPostStringを選択

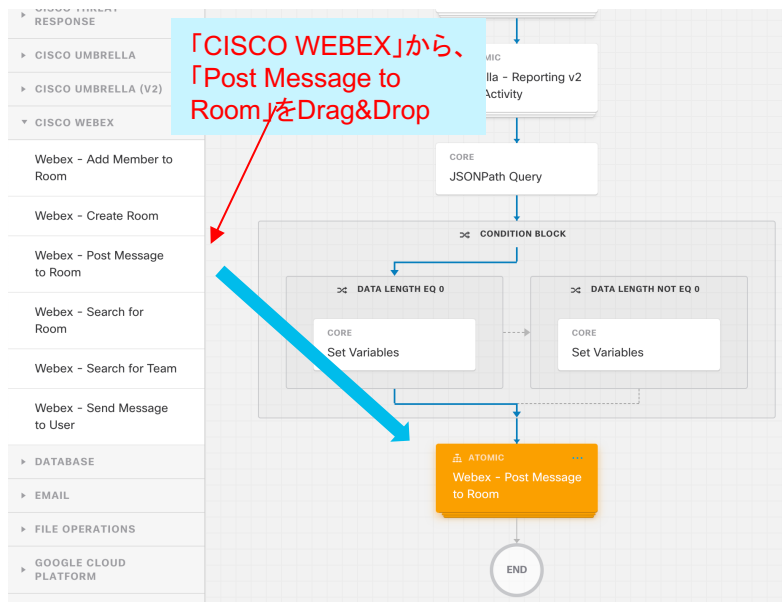
* Variable to update
[`${workflow.SecureX workflow - logic use case.local.WebexPostString$}`]

New value
悪意あるドメインに対するアクセスが発生した可能性があります。
Umbrellaのログ情報を確認してください。

+ ADD

data配列の長さが0の場合、Report APIで取得した時間の範囲では、悪意あるドメインへのアクセスが観測されなかったことを示すため、その旨を通知するメッセージを指定。
Python版ではアクセス先ドメインや、アクセス元IPアドレスをメッセージに含めていましたが、処理の簡素化のため、ログの確認を促す内容に変更。

脅威が観測された場合のメッセージを指定



Workflow configuration form for 'Webex - Post Message to Room'. The form includes an 'INPUT' section for 'Markdown Message'. Below this, there are two red-bordered boxes highlighting configuration fields: '* Access Token' and '* Room ID', both with values starting with '\$[workflow.SecureX workflow - logic use case.static.Webex Bot Access Token\$]'. Below these is the 'Plain Text Message' field, also with a value starting with '\$[workflow.SecureX workflow - logic use case.local.WebexPostString\$]'. There is also an 'Attachments' field.

Python版と同じToken, Room IDを指定

投稿する文字列を格納するために定義した、Workflowのローカル変数を指定
Workflow > Local > WebexPostString

Target configuration section. It includes fields for '* Target' and '* Target Type'. Below these is the 'HTTP Endpoint' section with radio buttons for 'No target', 'Execute on this target', and 'Use workflow target'. The 'Override workflow target' option is selected. Below this, there is a dropdown menu for '* Target' with 'Webex_Teams' selected. This section is highlighted with a red border.

Targetとして、デフォルトで登録されているWebex TeamsのTargetを選択

参考資料

- SecureX コンフィギュレーションガイド
 - https://www.cisco.com/c/ja_jp/support/security/securex/products-installation-and-configuration-guides-list.html
- Umbrella API
 - <https://developer.cisco.com/docs/cloud-security/#!umbrella-api-introduction/introduction>
- Webex API
 - <https://developer.webex.com/docs/getting-started>



SECURE