Criminal IP FDS for Splunk Usage Guide

AISpera, Inc

Version 1.0.0

Table of Contents

1. Dictionary Key information according to API response

A. Log: {"datetime": "2022-09-28 13:46:34", "ip_score": "Moderate", "IP": "223.38.40.211", "country": "Korea", "as_name": "SK Telecom", "mobile": true, "tag_category": "mobile, vpn", "ip_category": "ddos (Medium), tor"}

i. ***datetime: Date accessed***

ii. ***ip_score: score results of searched IP / API: score***

① inbound: Used when inbound IP verification is required

② outbound: Used when outbound IP verification is required

③ Maps API request responses numerically, as returning responses are in number format API return/ score_mapping = {1:'Safe',2:'Low',3:'Moderate',4:'Dangerous',5:'Critical'}

iii. ***IP: IP address of intended search / API: ip***

iv. ***country: IP country / API: ['whois']['data'][0]['org_country_code']***

① Presented with country codes (KU, CN, US) in API / Just use as is

② Use pycountry library if country names are needed

v. ***as_name: ["whois"]['data'][0]['as_name']***

vi. ***tag: value that indicates whether the IP is tor, vpn, mobile etc. / API: tags***

1. Return key only if results are true
2. Cases where all API:tag values are false and returns empty field result may exist

vii. ***ip_category: Additional information regarding scanned IP / API: ip_category***

1. There could be no data involved

2. API Processing Code

```
def make_log(request_ip,request_time): ip_result = {}
    tag_list = [] vpn_list =
    [] ip_category_list = []
    ids_list = []
    try:
        result = getipdata(request_ip) score_int =
        result['score']['inbound'] score_mapping =
{1:'Safe',2:'Low',3:'Moderate',4:'Dangerous',5:'Critical'}

        score = score_mapping[score_int]
        if result['whois']['count'] != 0:
            country_code = result['whois']['data'][0]['org_country_code'] as_name =
            result["whois"]['data'][0]['as_name']
            country = pycountry.countries.get(alpha_2=country_code).name.split(',')[0]
        else:
            as_name = "" country
            = ""

        ip_result['datetime'] = request_time
        ip_result['ip_score'] = score ip_result['IP']
        = result['ip'] ip_result['country'] = country
        ip_result['as_name'] = as_name
        tags = result['tags']

        for key, value in tags.items():
            if value == True:
                key = key.split('_')[1]
                ip_result[key]=value
                tag_list.append(key)

        ip_result['tag_category'] = ','.join(tag_list)

        if result['vpn']['count'] != 0:
            for i in range(len(result['vpn']['data'])):
                vpn_name = result['vpn']['data'][i]['vpn_name'] vpn_list.append(vpn_name)
            vpn_list = list(set(vpn_list)) ip_result['vpn_name'] =
            ','.join(vpn_list)

        if result['ip_category']['count'] != 0:
            for i in range(len(result['ip_category']['data'])): ip_type =
                result['ip_category']['data'][i]['type']
                ip_category_list.append(ip_type)
            ip_category_list = list(set(ip_category_list)) ip_result['ip_category'] =
            ','.join(ip_category_list)

        if result['ids']['count'] != 0:
            for i in range(len(result['ids']['data'])):
                calssfication = result['ids']['data'][i]['classification']
                ids_list.append(calssfication)
            ids_list = list(set(ids_list)) ip_result['ip_classification'] =
            ','.join(ids_list)

        return ip_result except
    Exception as e:
        print('api error')
        print(e)
```

Download the python file from Github (Optional) / For those that want the entire file (https://github.com/criminalip/CIP-FDS)

i. ***Needs revision***

①Edit ‘input file_location’ in ‘make_file’ at main.py

②Add API value in core.api.criminalip.py

ii. ***Requirements***

①pycountry install