Shodan簡介與應用

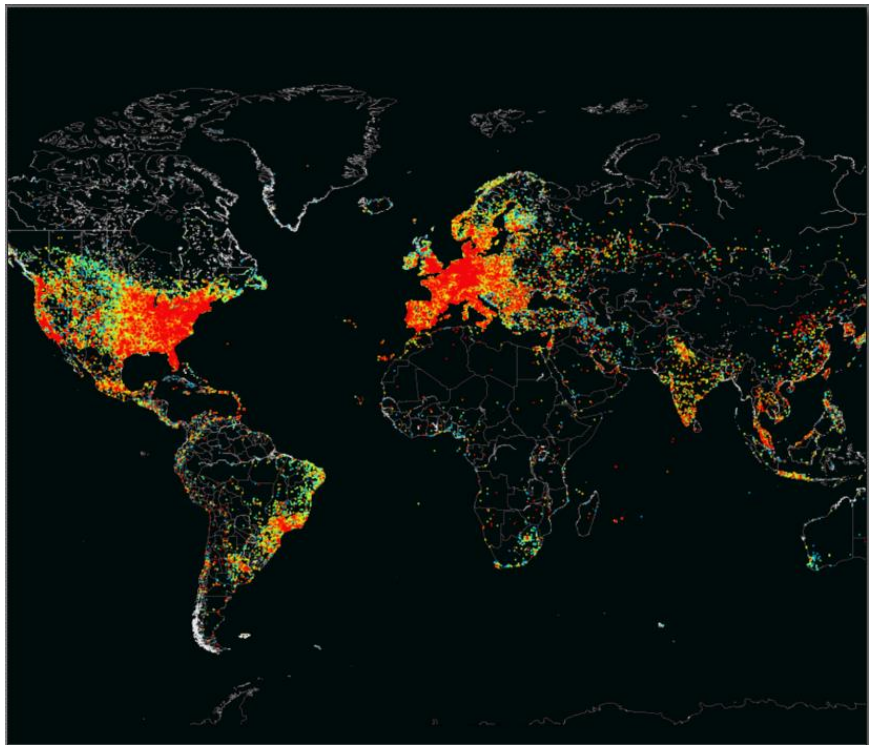
NASOC 二線工程師 林宜進

E-mail：tjline01@asoc.cc.ntu.edu.tw

大綱

1. Shodan簡介
2. 下載Shodan資料
3. 網路攝影機的特性
4. 結合Shodan尋找網路攝影機

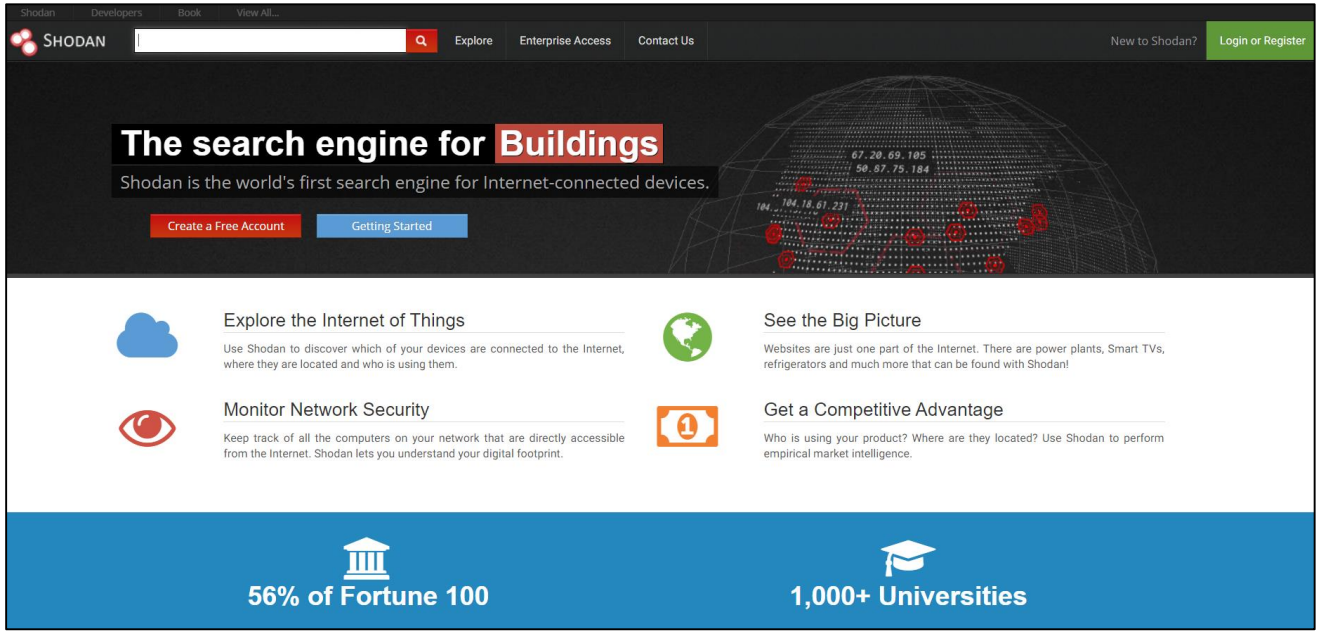
Shodan簡介



SHODAN網頁上的相關操作介紹

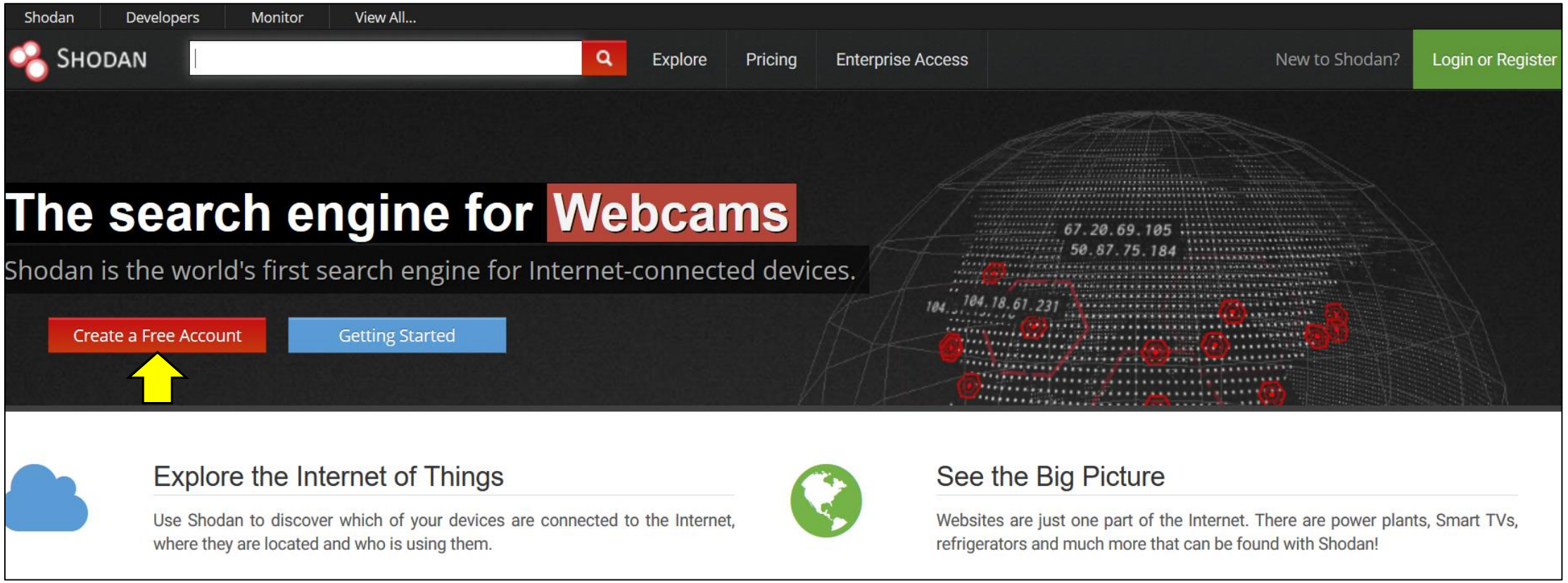
基本介紹

- Shodan是一個搜尋引擎，主要是搜索網路上的IoT設備
- 可以搜尋多種設備(例如：Webcam、SCADA、router、server)，有時會有詳細資訊
- 官方網址： https://www.shodan.io/

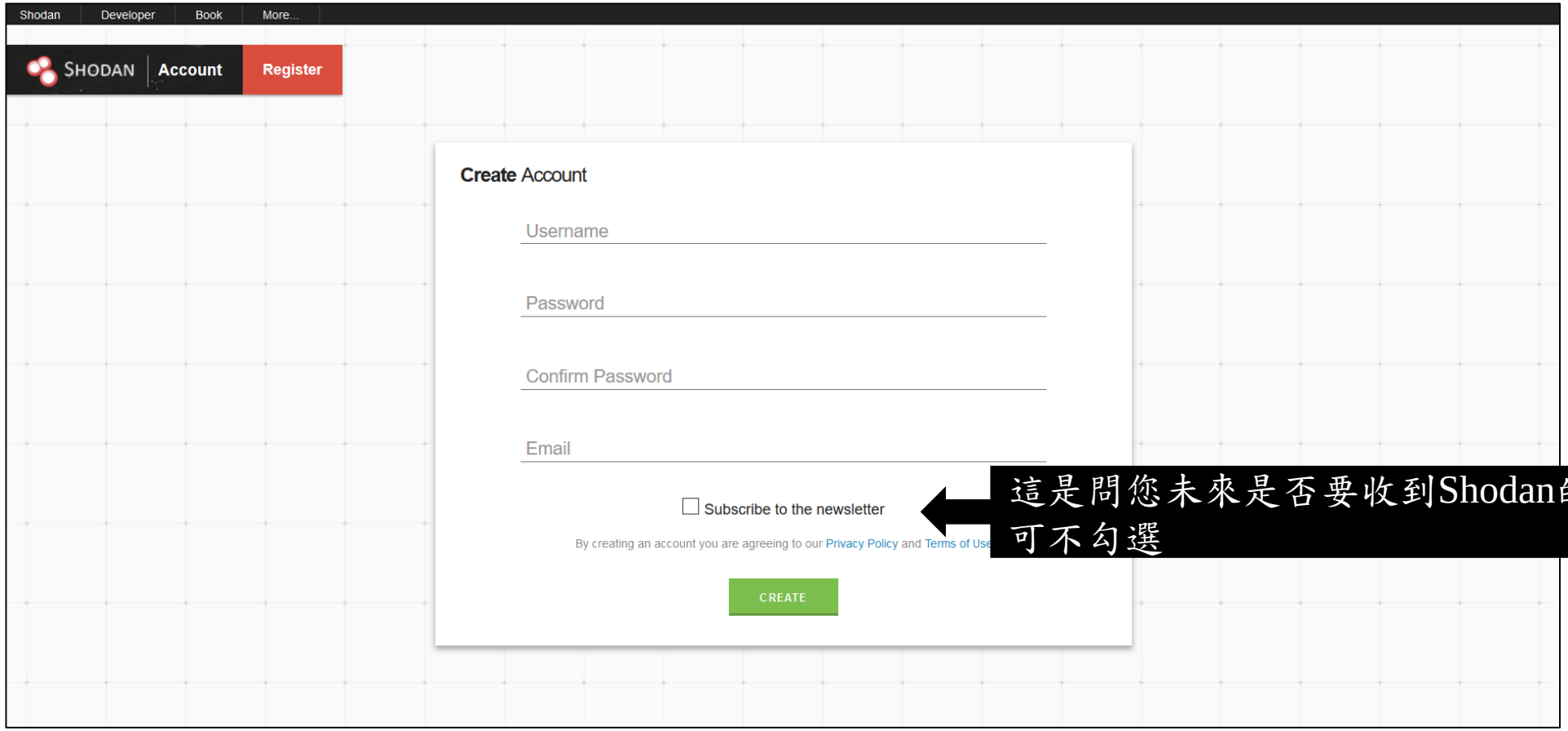


圖片來源：https://www.shodan.io/

帳號註冊(1/3)


Shodan
Developers
Monitor
View All...
SHODAN
Explore
Pricing
Enterprise Access
New to Shodan?
Login or Register
The search engine for Webcams
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
67.20.69.105
50.87.75.184
104.18.61.231
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

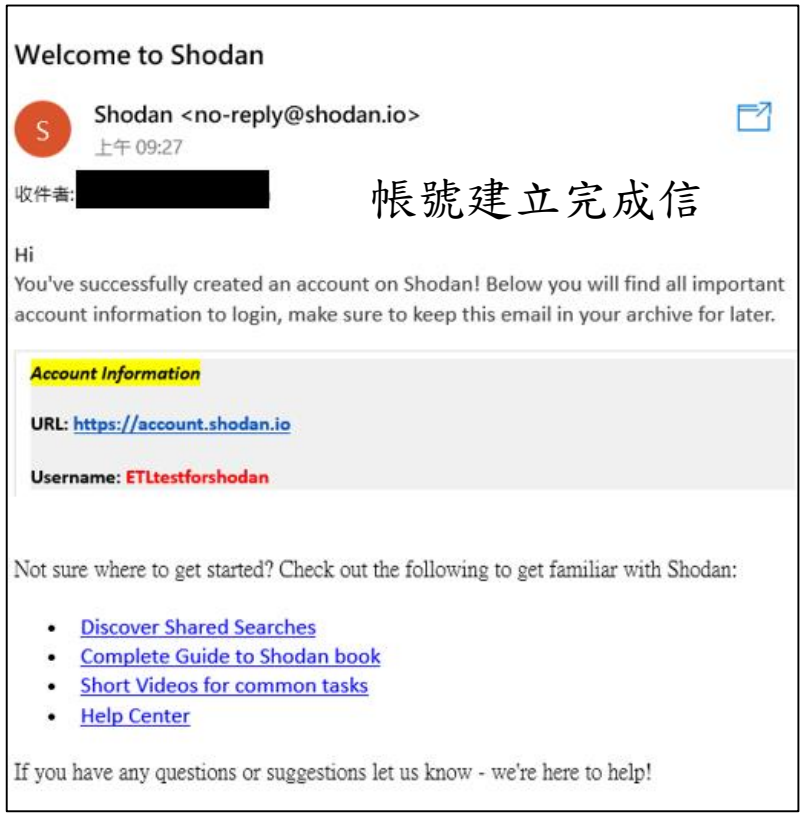
帳號註冊(2/3)



這是問您未來是否要收到Shodan的更新資訊，可不勾選

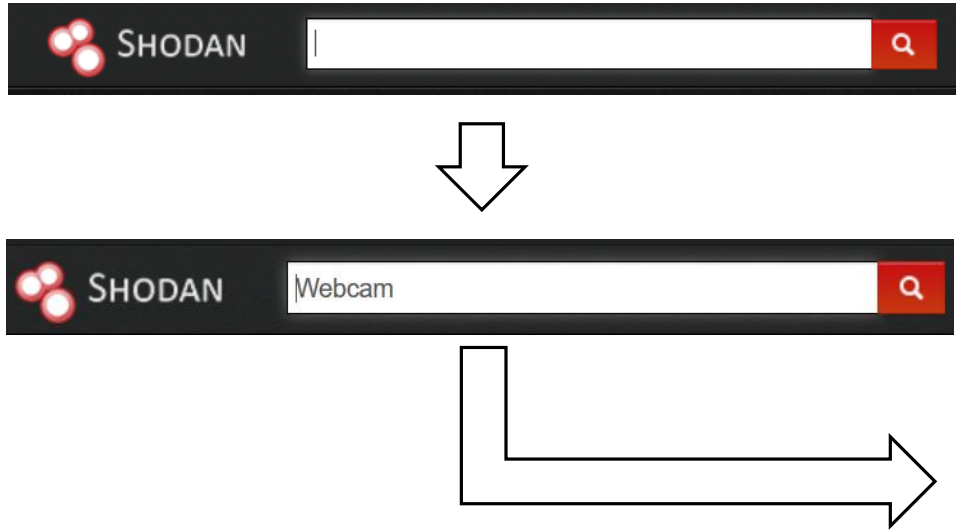
帳號註冊(3/3)

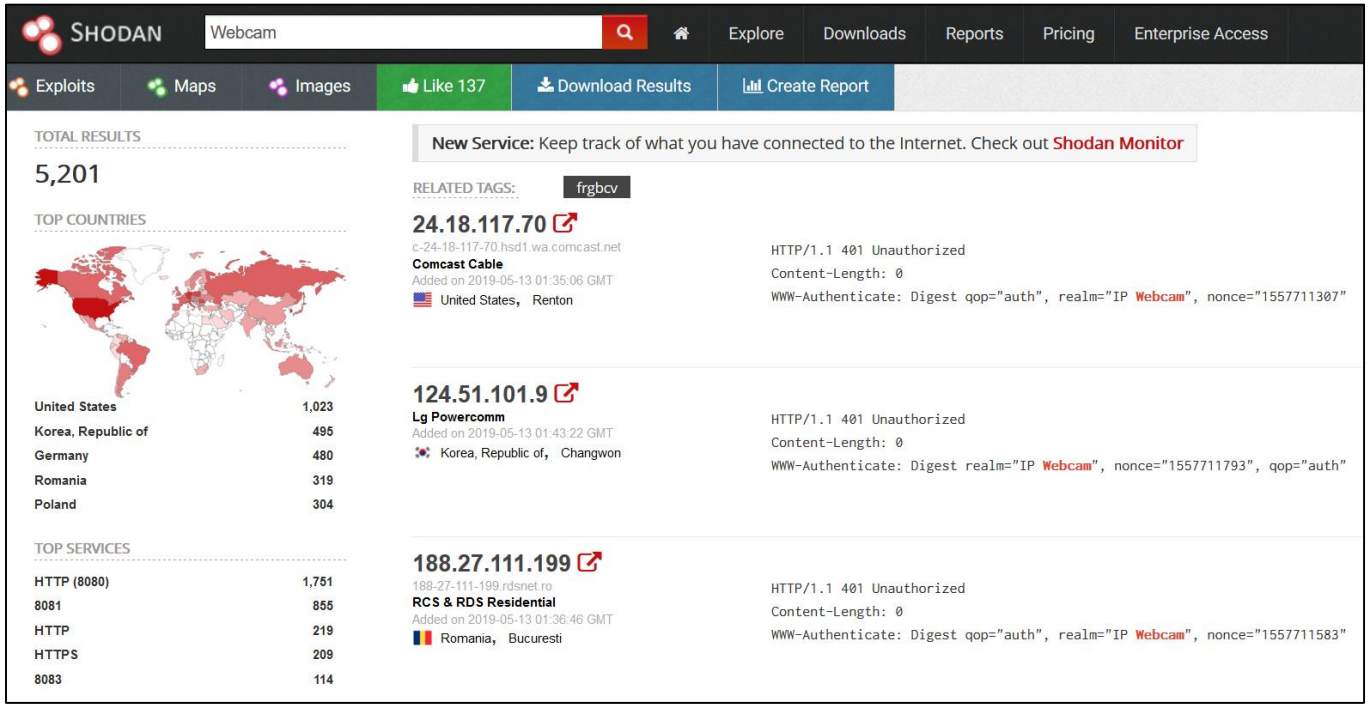
- 到註冊信箱收信，總共會收到兩封信。一封信是啟動確認信；另一封是帳號建立完成信



基本操作-搜尋欄位(1/2)

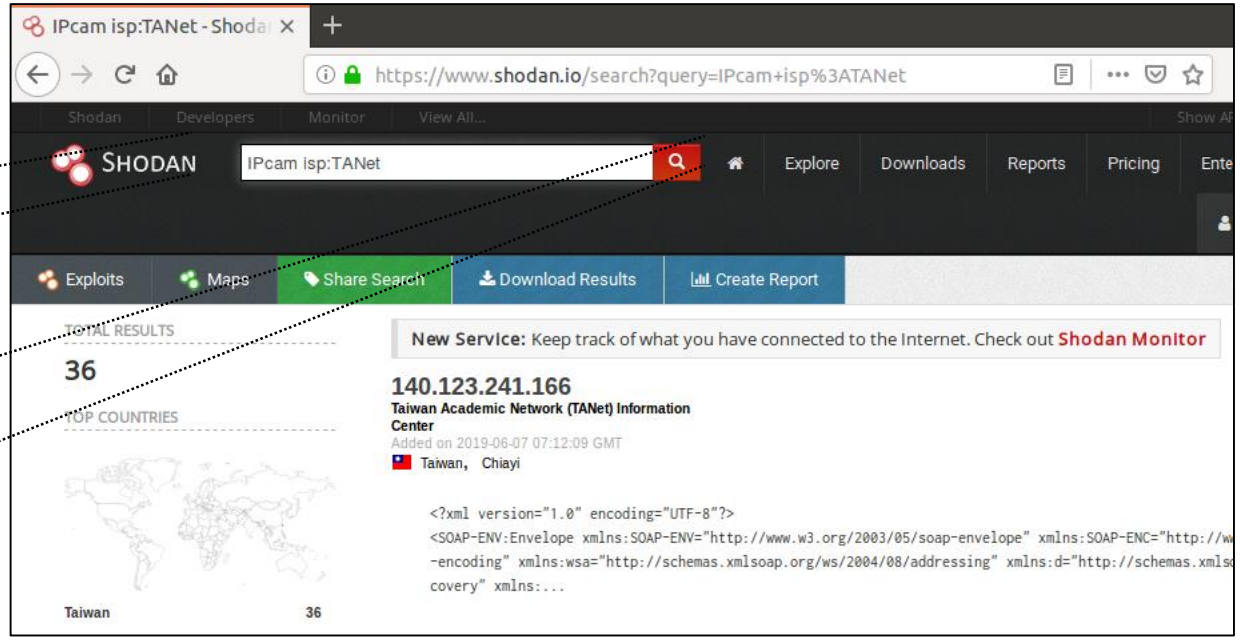
- 可任意輸入想查詢的設備(例如：Webcam、MySQL server…)





基本操作-搜尋欄位(2/2)

- 在輸入要查詢的設備名稱時，可搭配過濾器(filter)，減少無關的資料顯示
- 過濾器可以多種搭配使用，例如要找尋(1)IPcam (2)學術網路 的設備，欄位輸入：IPcam isp:TANet



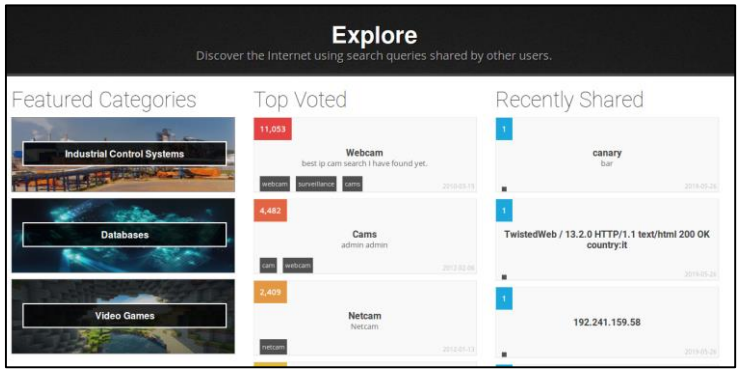
搜尋欄位過濾器

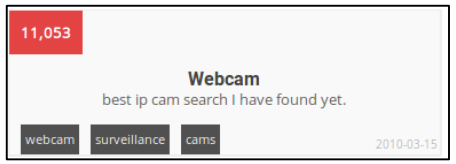
過濾器	說明	範例(輸入時可不加雙引號)
net	搜尋指定的ip 位置或是網段	net:"140.112.0.0/16"
port	搜尋指定的連接埠	port:"80"
product	搜尋指定的作業系統/軟體/產品名稱	product:"windows"
country	搜尋指定的國家	country:"TW"
city	搜尋指定的城市	city:"Taipei"
org	搜尋指定的組織或公司	org:"TANet"
isp	搜尋指定的isp業者	isp:"hinet"
hostname	搜尋指定的網域名稱	hostname:"ntu"
version	搜尋指定的軟體版本	version:"4.2"
geo	搜尋指定的地理位置(緯度，經度)	geo:"25, 121"
before/after	搜尋特定的時間前(後)的資料，格式dd-mm-yy	before:"01-01-18"

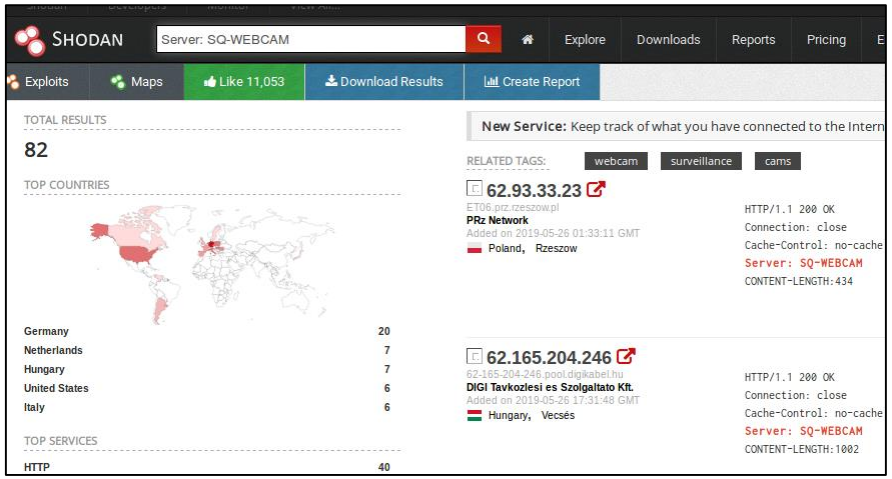
資料探索(Explore) (1/2)

- 如果想要知道目前熱門的查詢項目，可以點選Explore頁面

- 進入探索頁面，可以去找尋有興趣的設備類別

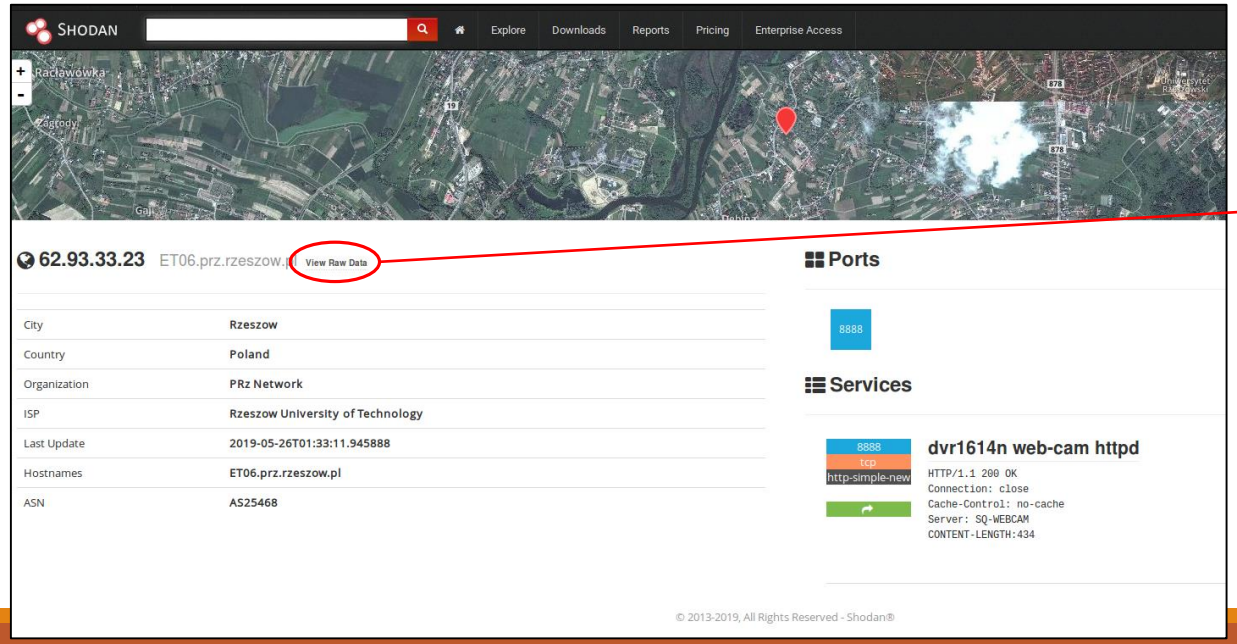


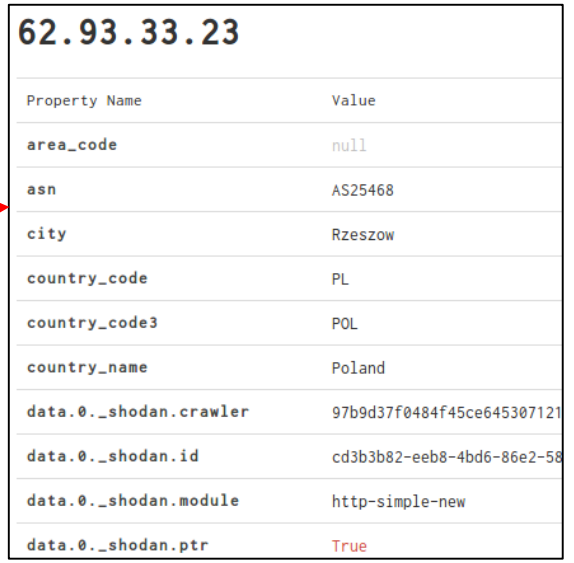




資料探索(Explore) (2/2)

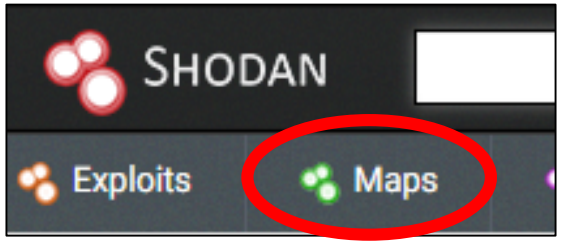
- 點擊IP，查看被Shodan紀錄的資訊
- 點擊View Raw Data，檢視完整的Shodan掃描資料
- 當越多的資訊被公開在網路上，就越有機會被入侵攻擊





地圖分布(Maps)

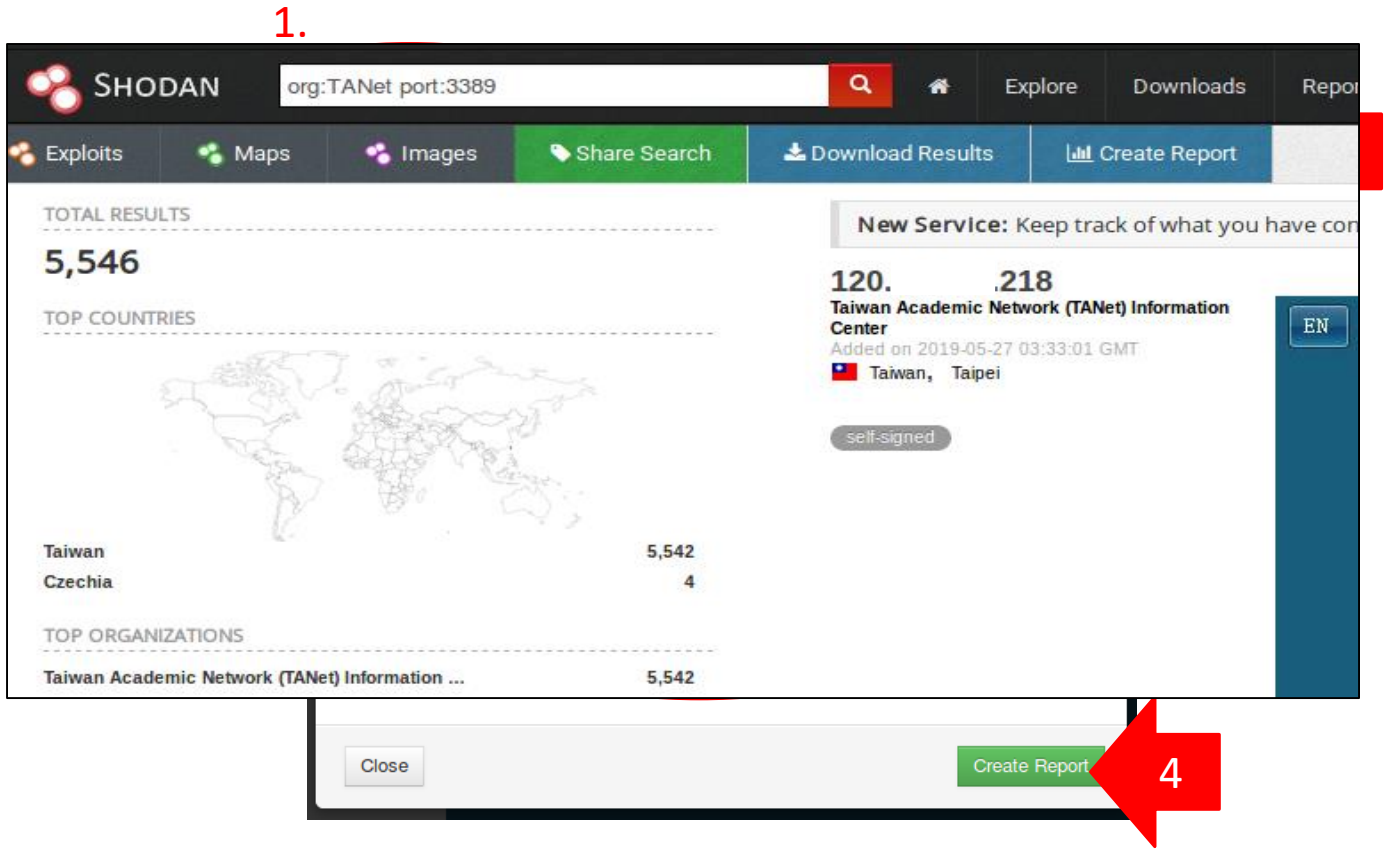
- 該功能是在Exploits的右邊，點擊Maps就會進入
- 這個功能可以查看關鍵字在全球的分布，一些使用者常利用此功能做一些分析，例如設備的分布密度、該設備全球分布狀況的推測等等



建立報告(Create Report) (1/2)

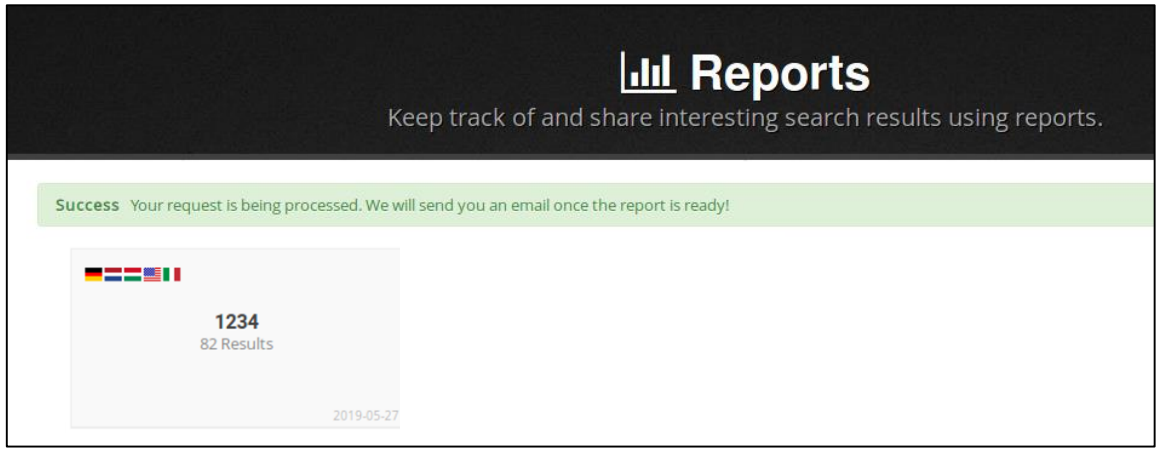
- 只要註冊會員後，都可以使用此功能
- 操作過程：

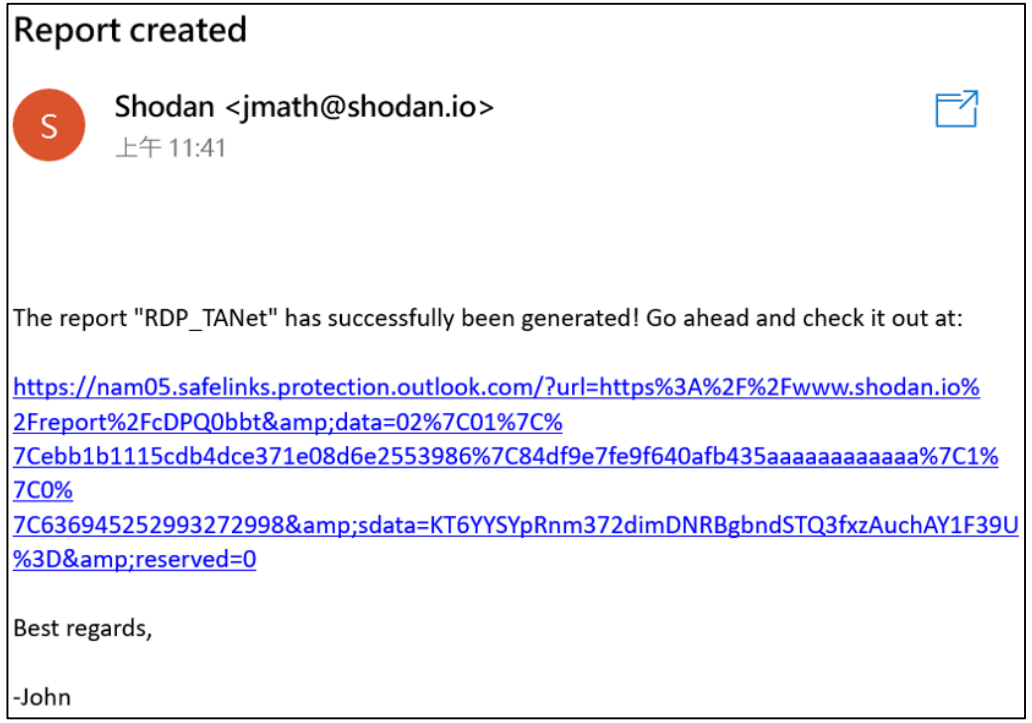
1. 查詢資訊
2. 按下Create Report
3. 建立Report標題
4. 按下綠框就開始建立報告



建立報告(Create Report) (2/2)

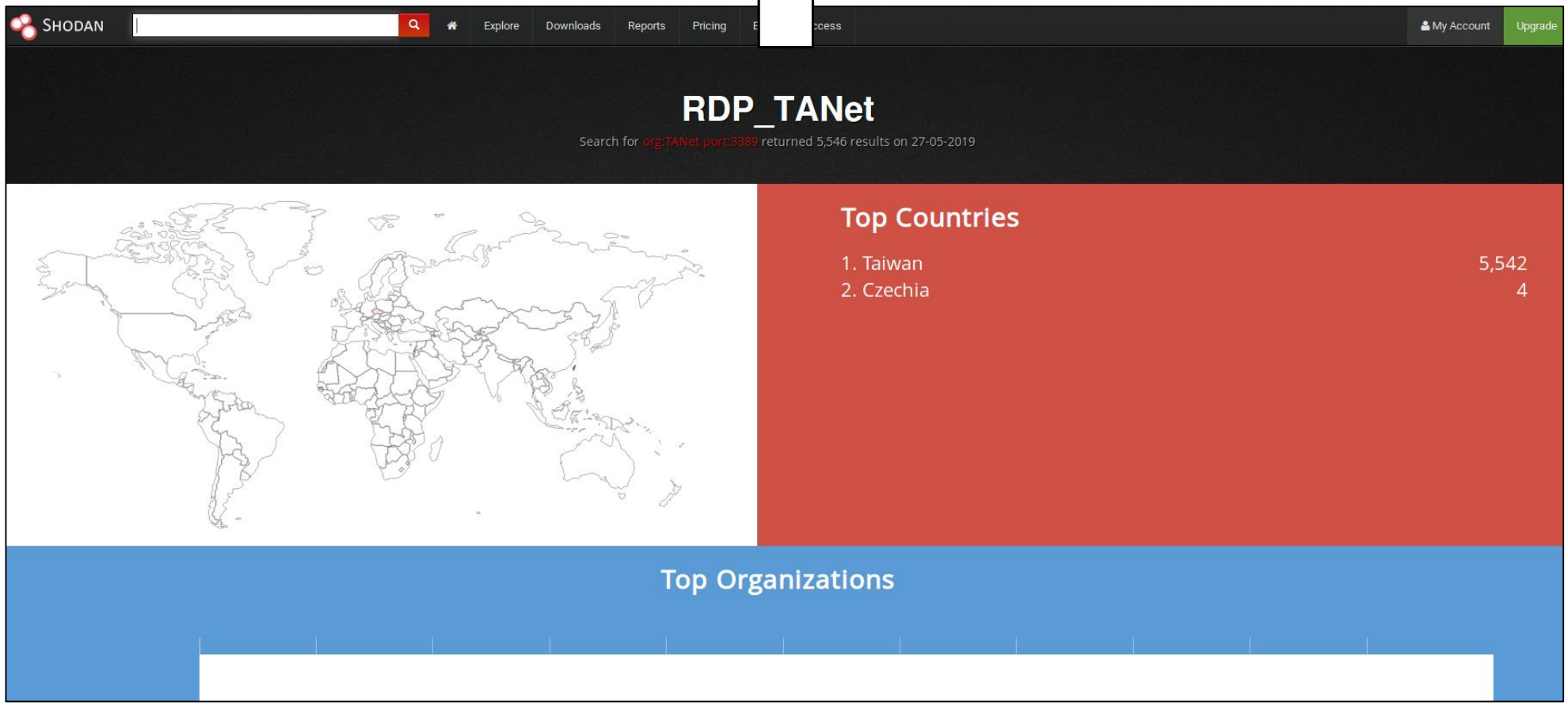
- 建立完成會出現成功訊息，並告訴使用者等待信件通知
- 進入信箱點連結就可以看到產生的Report資訊



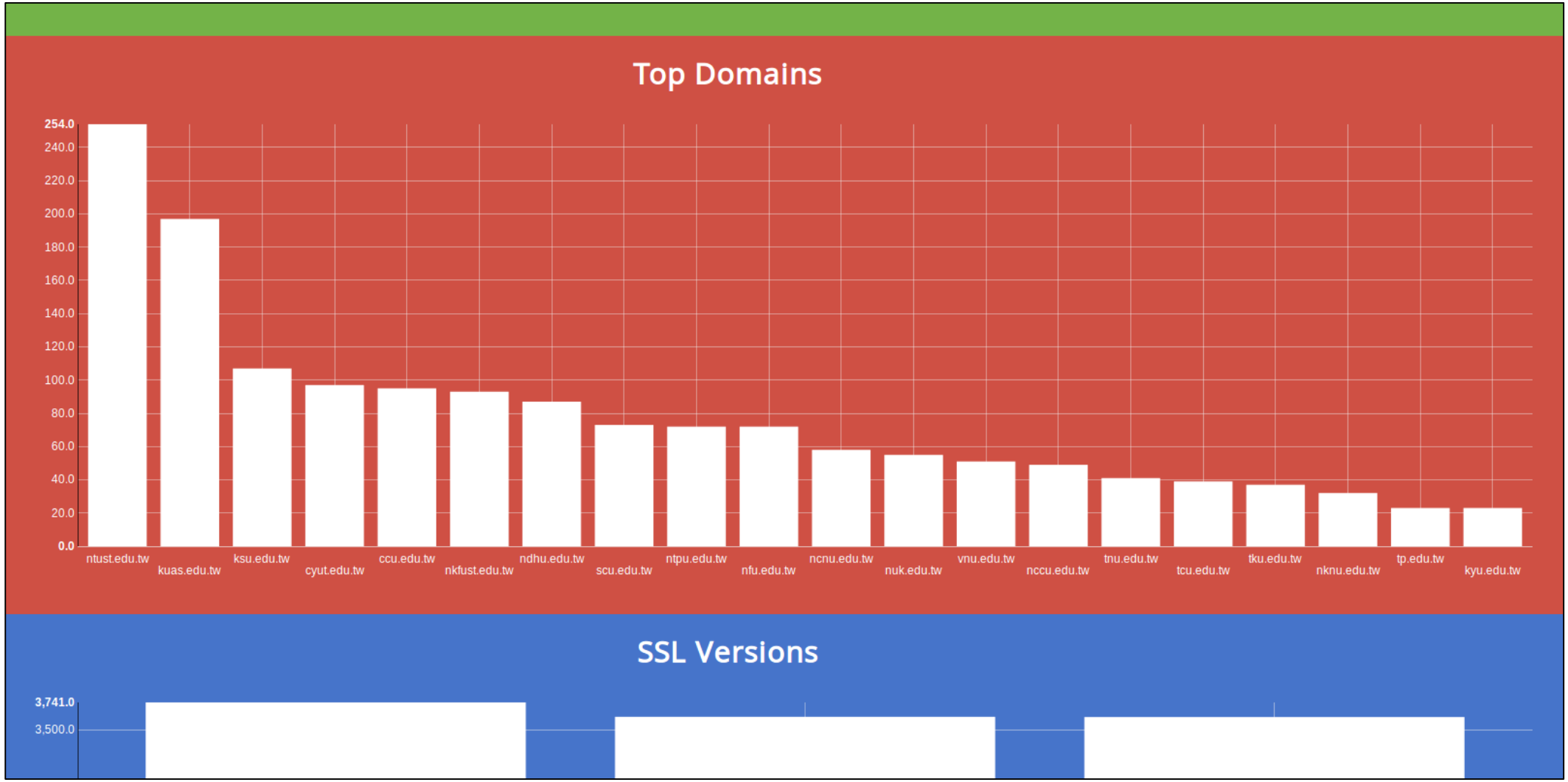


報告呈現(1/3)

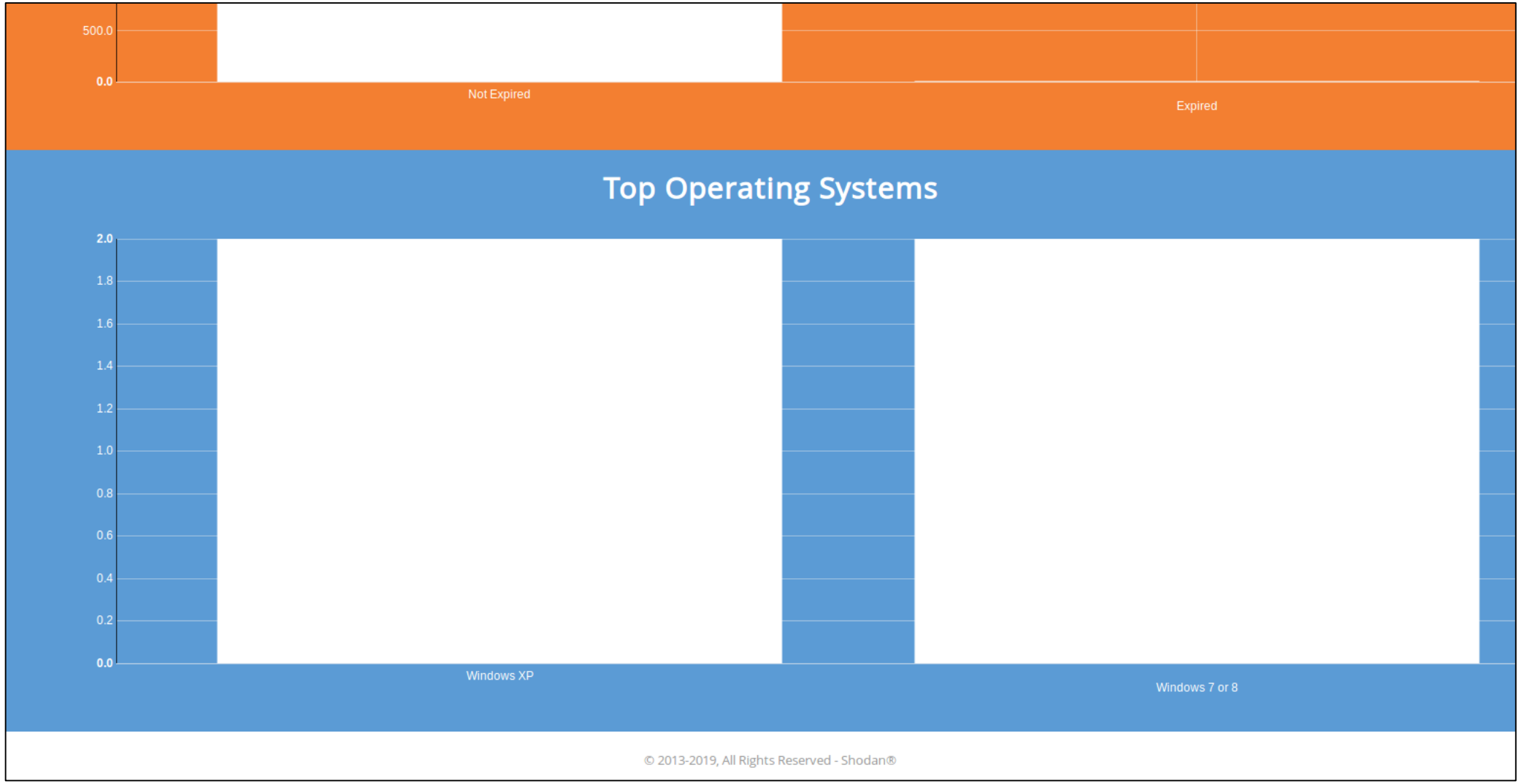

RDP_TANet
Search for org:TANet port:3389 returned 5,546 results on 27-05-2019


SHODAN
Explore
Downloads
Reports
Pricing
My Account
Upgrade
RDP_TANet
Search for org:TANet port:3389 returned 5,546 results on 27-05-2019
Top Countries
1. Taiwan 5,542
2. Czechia 4
Top Organizations

報告呈現(2/3)


Top Domains
254.0
240.0
220.0
200.0
180.0
160.0
140.0
120.0
100.0
80.0
60.0
40.0
20.0
0.0
ntust.edu.tw
kuas.edu.tw
ksu.edu.tw
cyut.edu.tw
ccu.edu.tw
nkfust.edu.tw
ndhu.edu.tw
scu.edu.tw
ntpu.edu.tw
nfu.edu.tw
ncnu.edu.tw
nuk.edu.tw
vnu.edu.tw
nccu.edu.tw
tnu.edu.tw
tcu.edu.tw
tku.edu.tw
nknu.edu.tw
tp.edu.tw
kyu.edu.tw
SSL Versions
3,741.0
3,500.0

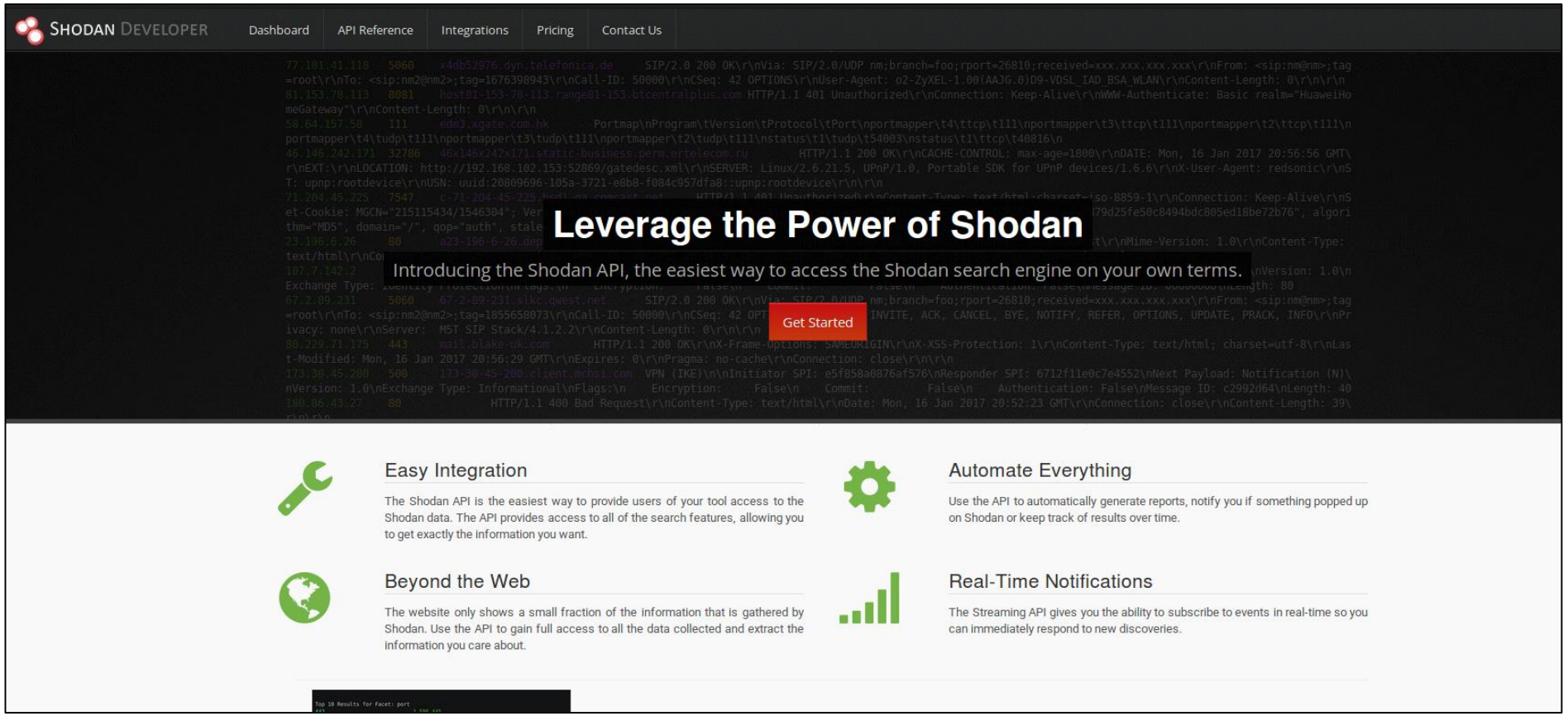
報告呈現(3/3)


500.0
0.0
Not Expired
Expired
Top Operating Systems
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
Windows XP
Windows 7 or 8
© 2013-2019, All Rights Reserved - Shodan®

其他項目補充-上半部

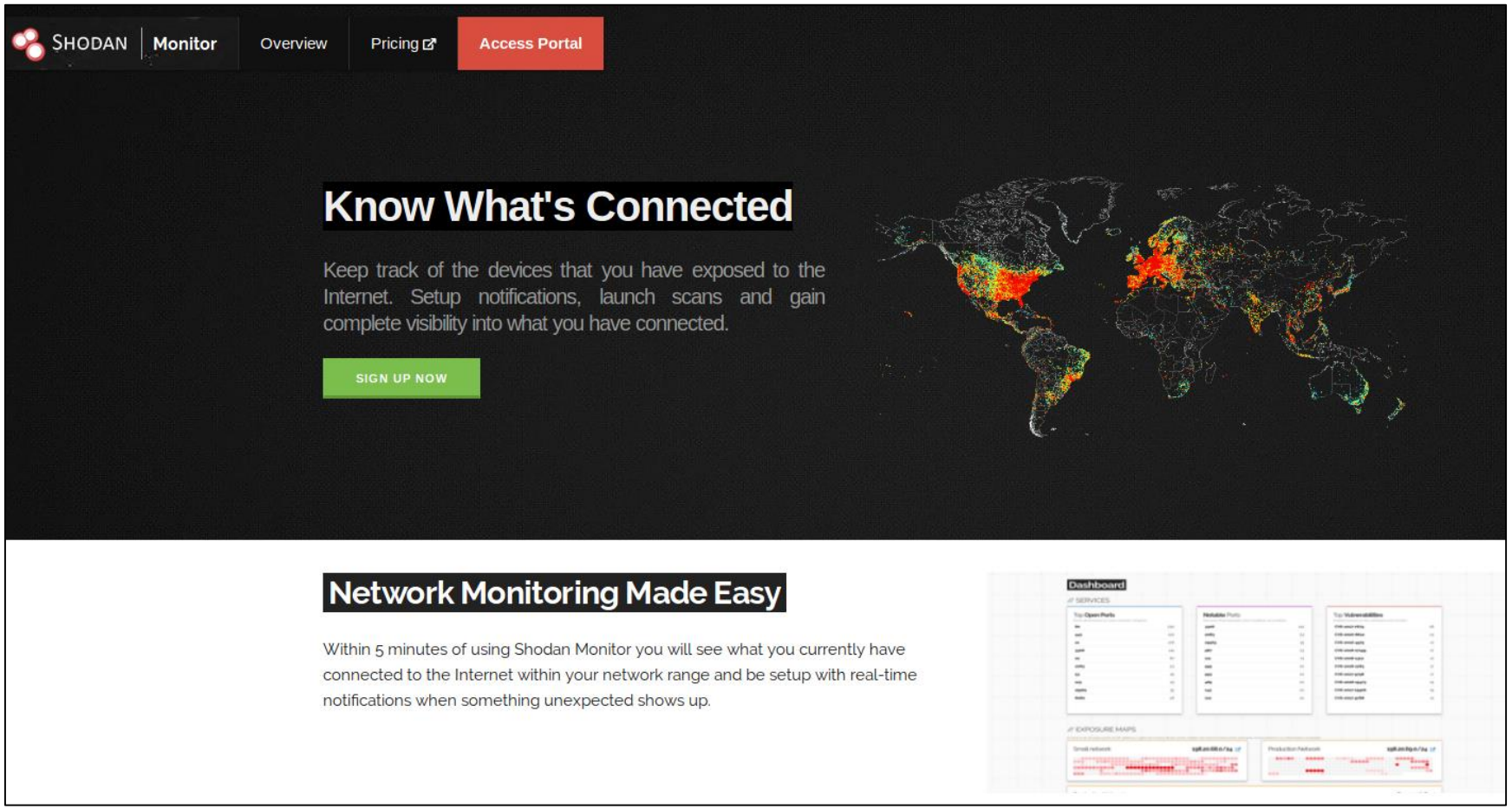

開發者頁面介紹，提供如何使用
其他程式語言使用Shodan服務
2019年3月上線的功能
可以監控設定的IP在網路上的活動
(付費使用)
回到首頁
查看Shodan提供的服務(連結)
Shodan
Developers
Monitor
View All...
SHODAN

Developers

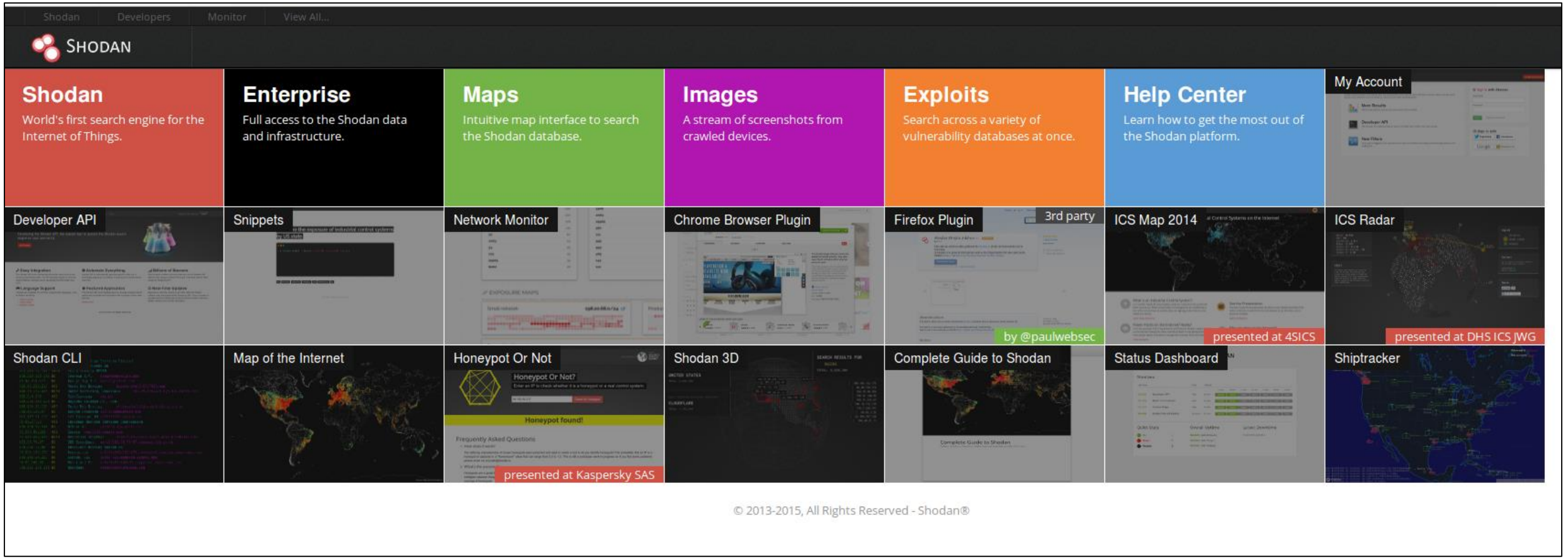

SHODAN DEVELOPER
Dashboard
API Reference
Integrations
Pricing
Contact Us
Leverage the Power of Shodan
Introducing the Shodan API, the easiest way to access the Shodan search engine on your own terms.
Get Started
Easy Integration
The Shodan API is the easiest way to provide users of your tool access to the Shodan data. The API provides access to all of the search features, allowing you to get exactly the information you want.
Automate Everything
Use the API to automatically generate reports, notify you if something popped up on Shodan or keep track of results over time.
Beyond the Web
The website only shows a small fraction of the information that is gathered by Shodan. Use the API to gain full access to all the data collected and extract the information you care about.
Real-Time Notifications
The Streaming API gives you the ability to subscribe to events in real-time so you can immediately respond to new discoveries.


支援
python
Powershell
Ruby
A Programmer's Best Friend
node
php

Monitor

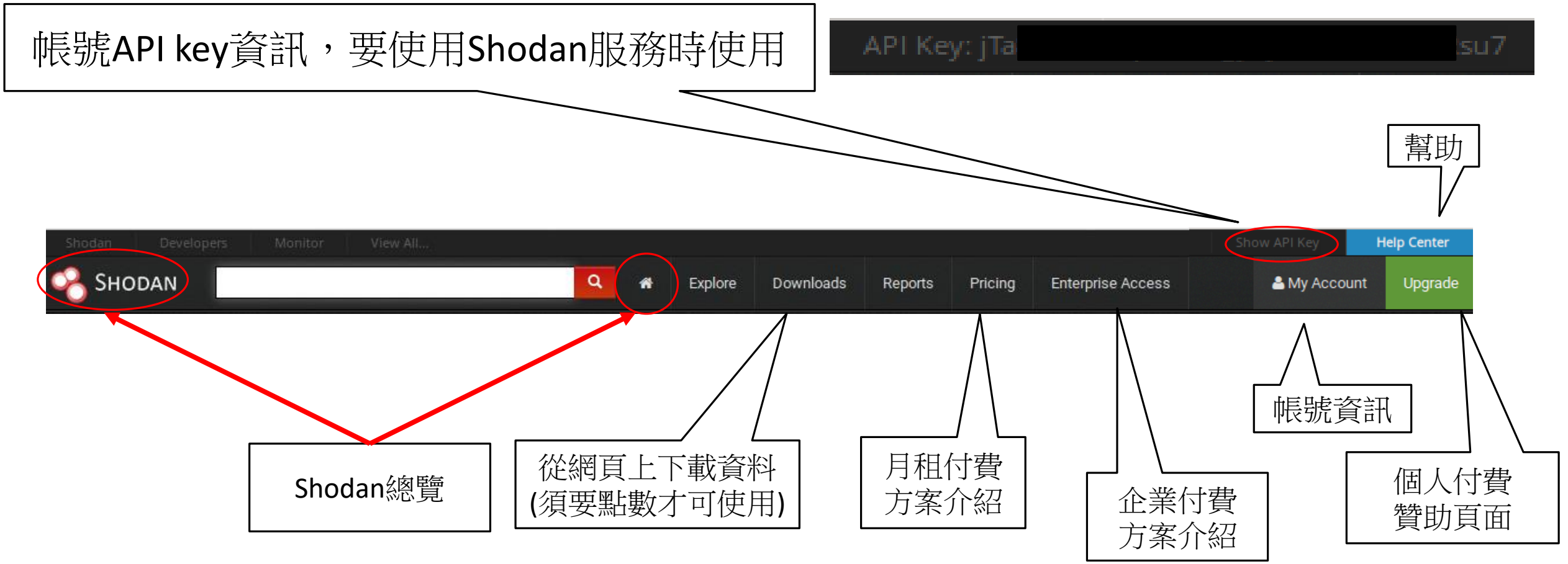

SHODAN
Monitor
Overview
Pricing
Access Portal
Know What's Connected
Keep track of the devices that you have exposed to the Internet. Setup notifications, launch scans and gain complete visibility into what you have connected.
SIGN UP NOW
Network Monitoring Made Easy
Within 5 minutes of using Shodan Monitor you will see what you currently have connected to the Internet within your network range and be setup with real-time notifications when something unexpected shows up.
Dashboard

View ALL

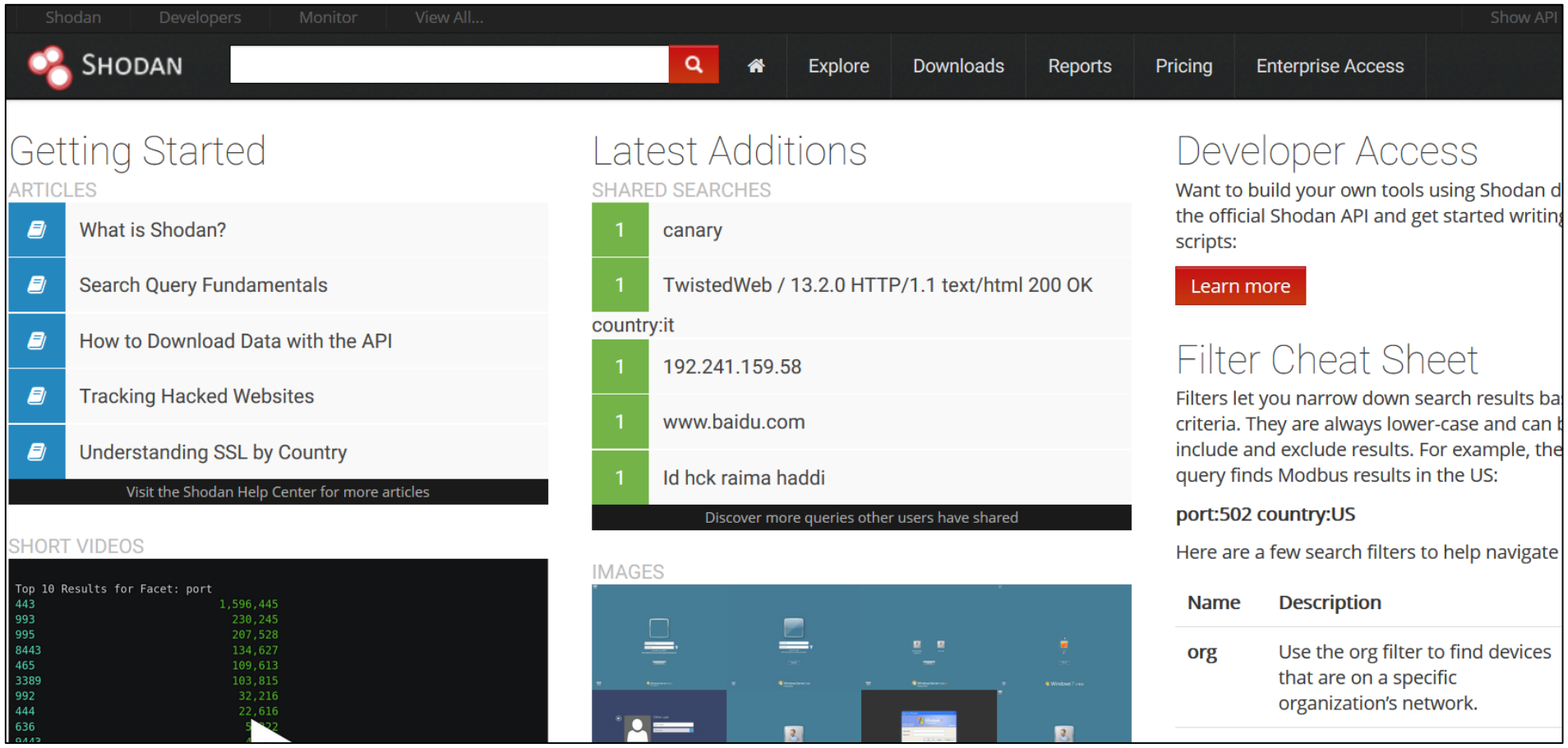

Shodan
Developers
Monitor
View All...
SHODAN
Shodan
World's first search engine for the Internet of Things.
Enterprise
Full access to the Shodan data and infrastructure.
Maps
Intuitive map interface to search the Shodan database.
Images
A stream of screenshots from crawled devices.
Exploits
Search across a variety of vulnerability databases at once.
Help Center
Learn how to get the most out of the Shodan platform.
My Account
Developer API
Snippets
Network Monitor
Chrome Browser Plugin
Firefox Plugin
3rd party
by @paulwebsec
ICS Map 2014
presented at 4SICS
ICS Radar
presented at DHS ICS JWG
Shodan CLI
Map of the Internet
Honeypot Or Not
Honeypot found!
presented at Kaspersky SAS
Shodan 3D
Complete Guide to Shodan
Status Dashboard
Shiptracker
© 2013-2015, All Rights Reserved - Shodan®

其他欄位補充

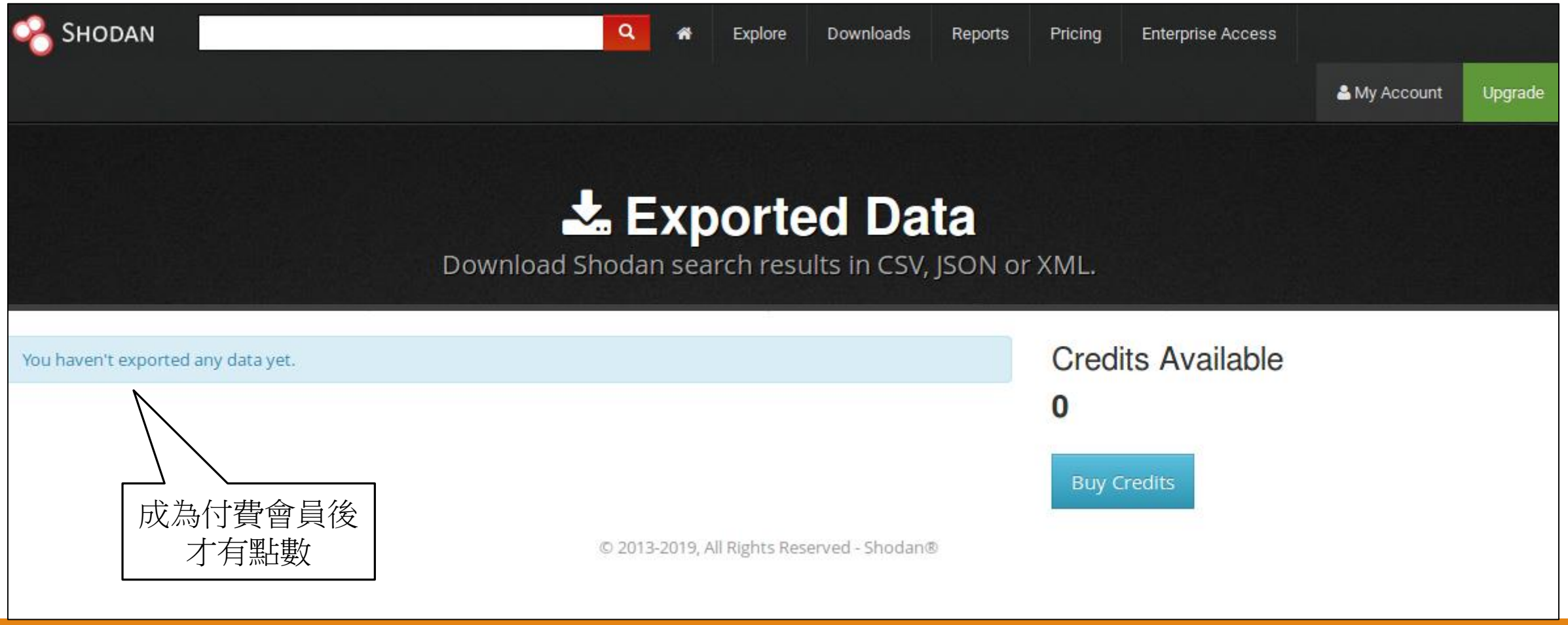
帳號API key資訊，要使用Shodan服務時使用



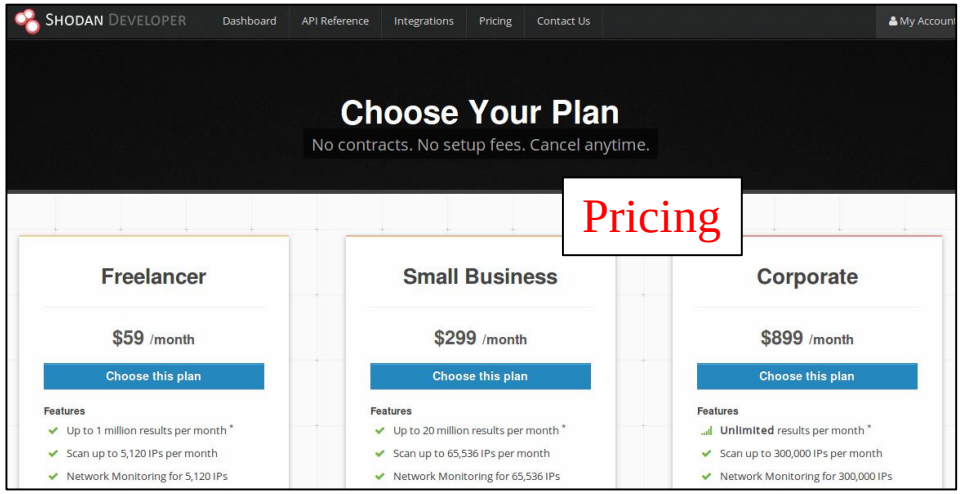
Shodan總覽

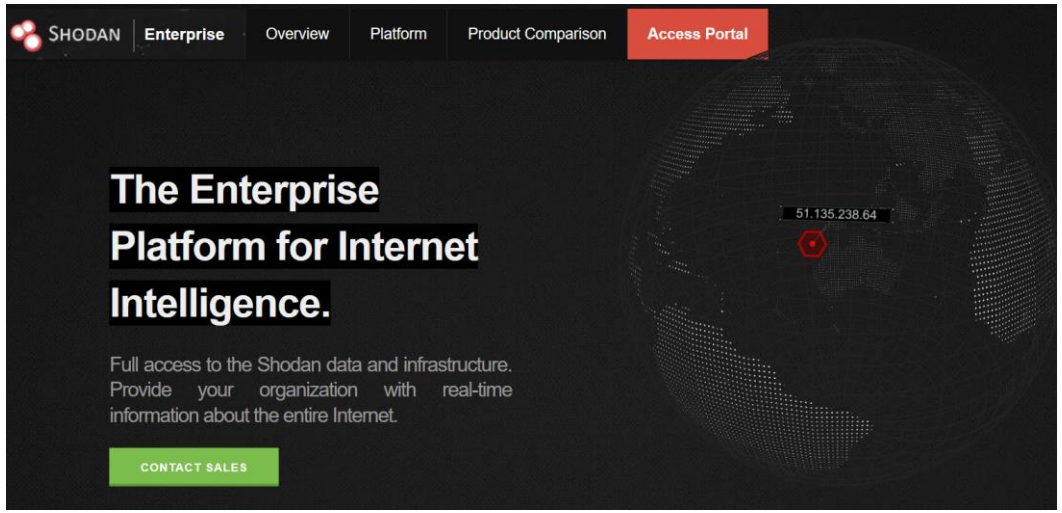

Shodan
Developers
Monitor
View All...
Show API
SHODAN
Explore
Downloads
Reports
Pricing
Enterprise Access
Getting Started
ARTICLES
What is Shodan?
Search Query Fundamentals
How to Download Data with the API
Tracking Hacked Websites
Understanding SSL by Country
Visit the Shodan Help Center for more articles
SHORT VIDEOS
Top 10 Results for Facet: port
443 1,596,445
993 230,245
995 207,528
8443 134,627
465 109,613
3389 103,815
992 32,216
444 22,616
Latest Additions
SHARED SEARCHES
1 canary
1 TwistedWeb / 13.2.0 HTTP/1.1 text/html 200 OK
country:it
1 192.241.159.58
1 www.baidu.com
1 Id hck raima haddi
Discover more queries other users have shared
IMAGES
Developer Access
Want to build your own tools using Shodan d
the official Shodan API and get started writin
scripts:
Learn more
Filter Cheat Sheet
Filters let you narrow down search results ba
criteria. They are always lower-case and can b
include and exclude results. For example, the
query finds Modbus results in the US:
port:502 country:US
Here are a few search filters to help navigate
Name
Description
org
Use the org filter to find devices that are on a specific organization's network.

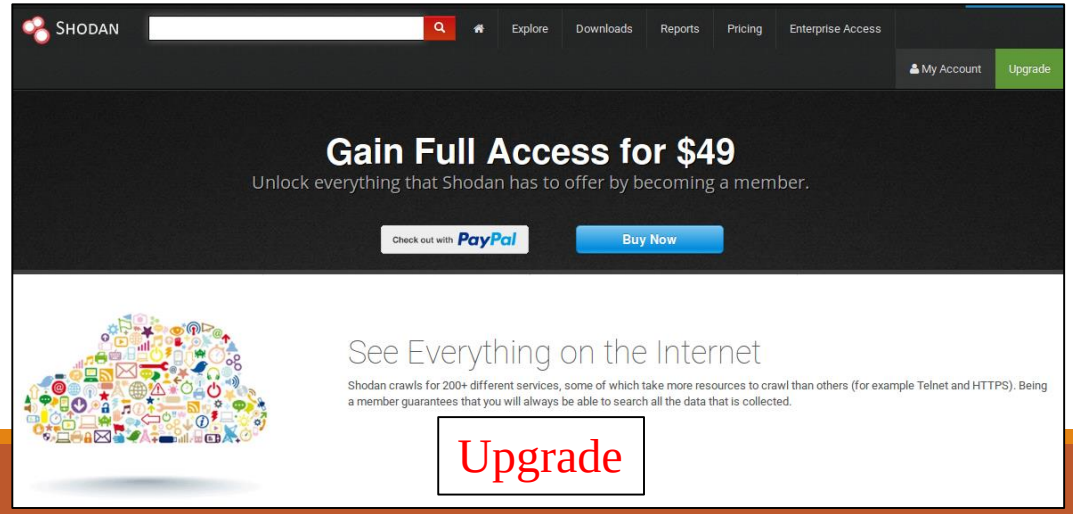
Downloads


SHODAN
Explore
Downloads
Reports
Pricing
Enterprise Access
My Account
Upgrade
Exported Data
Download Shodan search results in CSV, JSON or XML.
You haven't exported any data yet.
Credits Available
0
Buy Credits
© 2013-2019, All Rights Reserved - Shodan®
成為付費會員後
才有點數

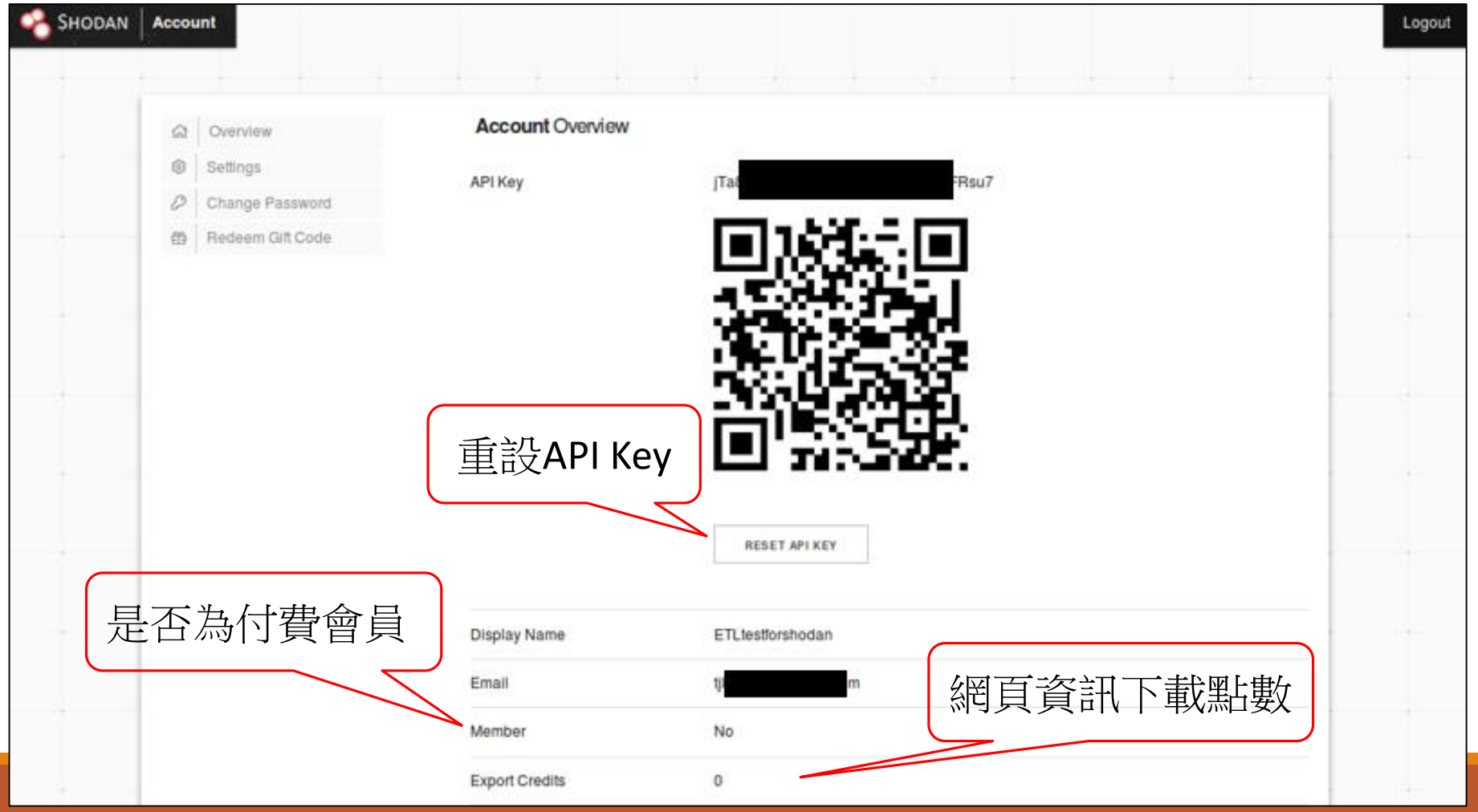
Pricing & Enterprise Access & Upgrade



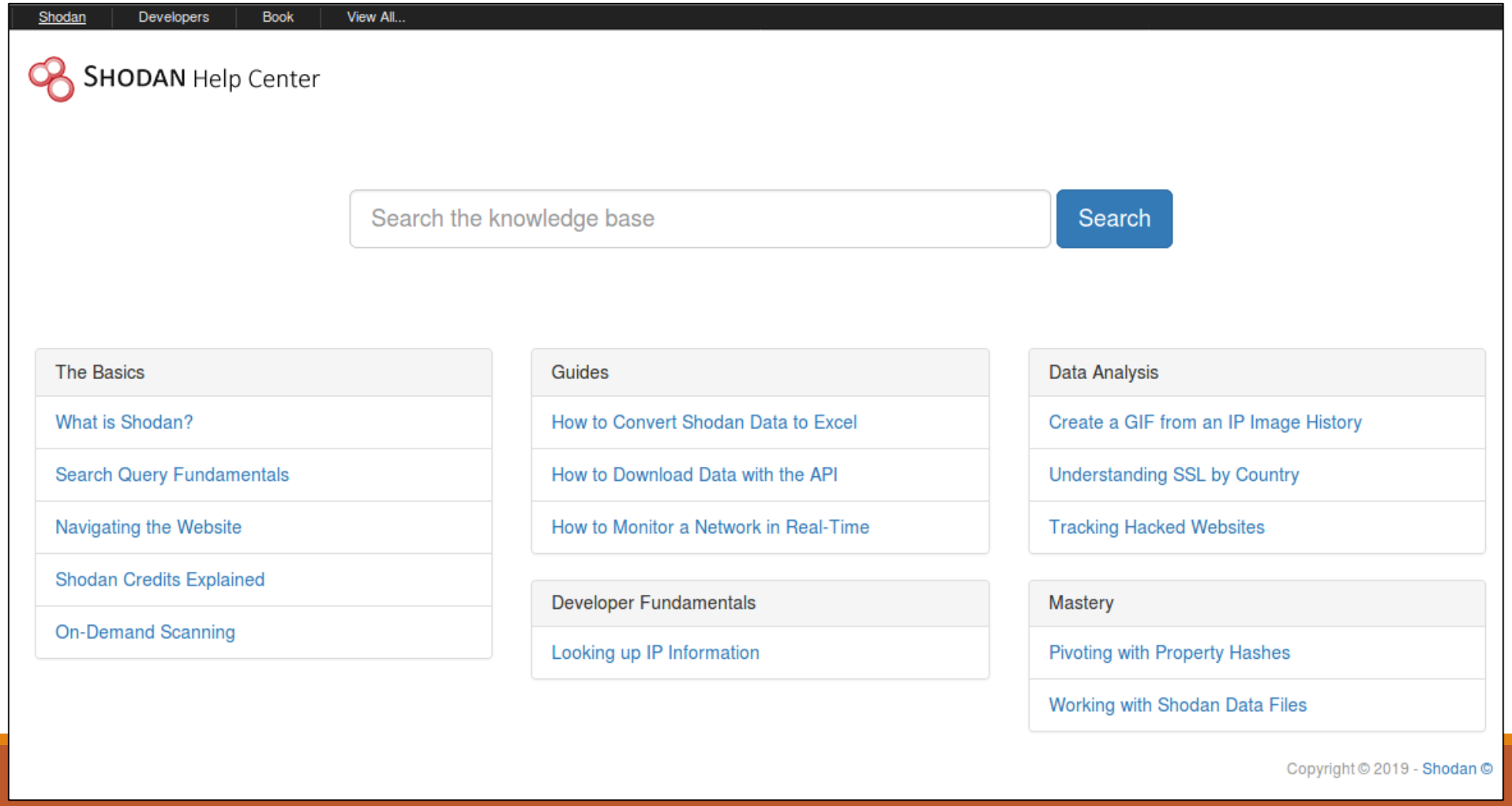


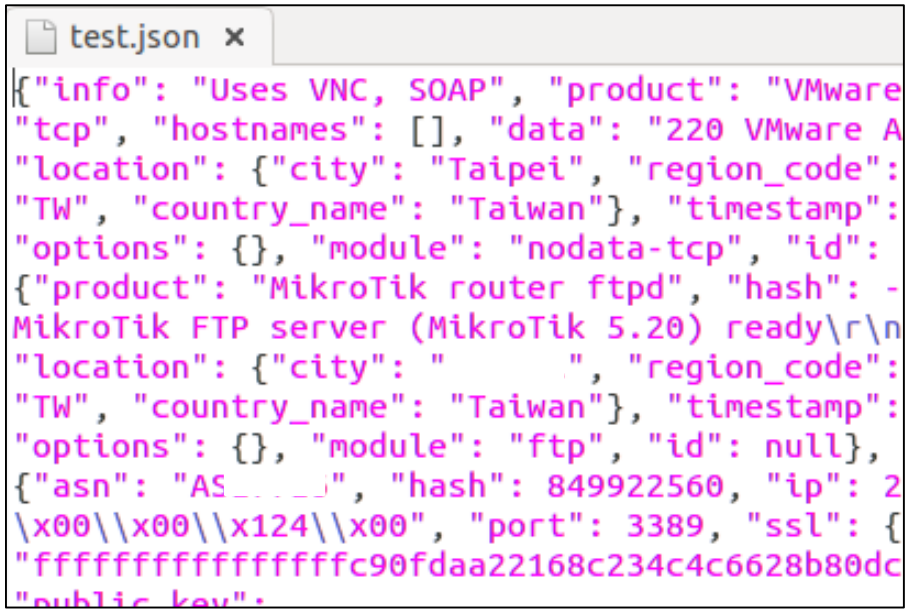


My Account


SHODAN
Account
Logout
Overview
Settings
Change Password
Redeem Gift Code
Account Overview
API Key
RESET API KEY
重設API Key
是否為付費會員
網頁資訊下載點數
Display Name
ETLtestforshodan
Email
Member
No
Export Credits
0

Help Center


Shodan
Developers
Book
View All...
SHODAN Help Center
Search the knowledge base
Search
The Basics
What is Shodan?
Search Query Fundamentals
Navigating the Website
Shodan Credits Explained
On-Demand Scanning
Guides
How to Convert Shodan Data to Excel
How to Download Data with the API
How to Monitor a Network in Real-Time
Developer Fundamentals
Looking up IP Information
Data Analysis
Create a GIF from an IP Image History
Understanding SSL by Country
Tracking Hacked Websites
Mastery
Pivoting with Property Hashes
Working with Shodan Data Files
Copyright © 2019 - Shodan ©



下載Shodan資料

從SHODAN下載資料去分析

前言

- Shodan官方有提供python套件，讓使用者選擇用CLI(命令列) 或是在寫python程式碼去使用Shodan服務
- 下載網址: https://github.com/achillean/shodan-python
- 本次操作以CLI為主

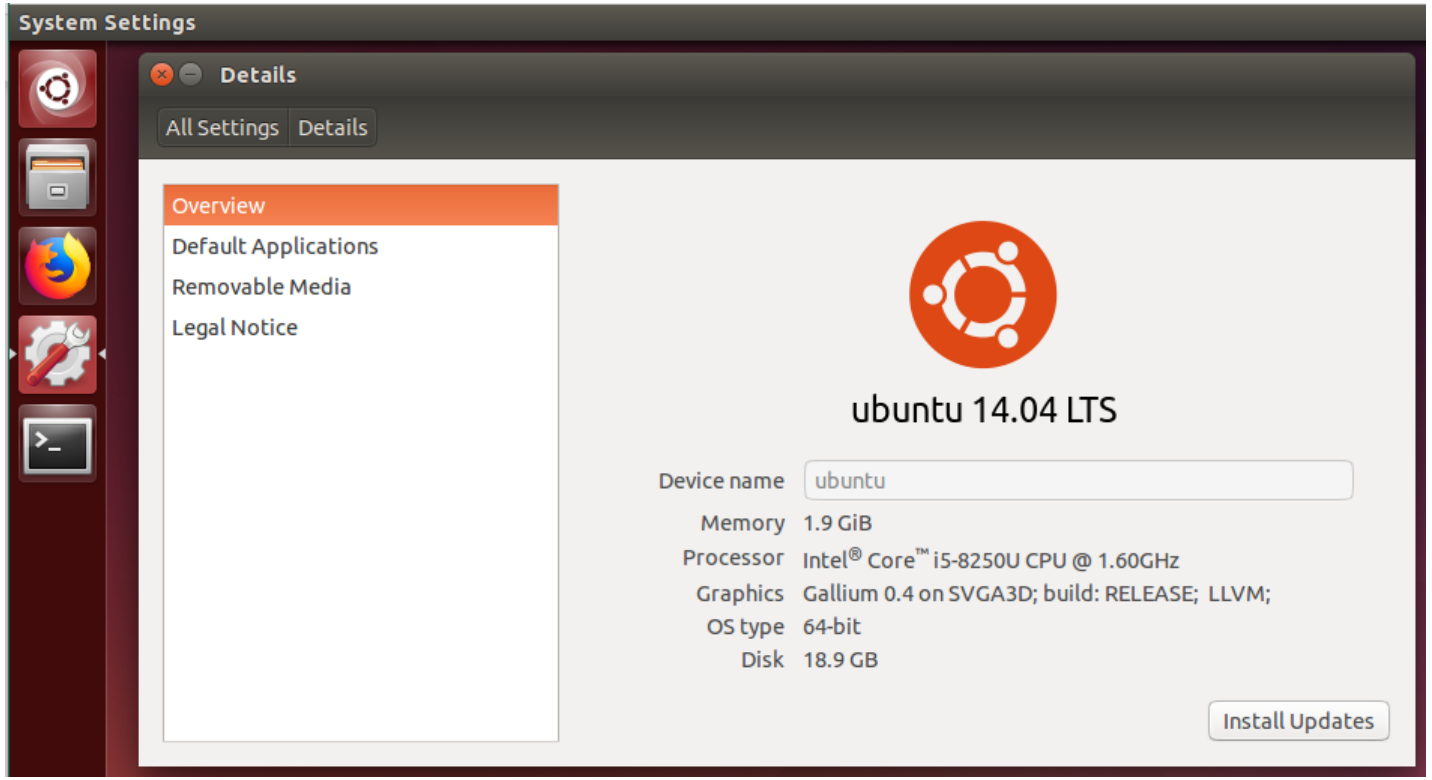
```
achillean@demo:~$
achillean@demo:~$ # Lets see which ports are running
achillean@demo:~$ shodan stats --facets ssl.version,port country:de has_ssl:true

Top 10 Results for Facet: port
443                           1,596,445
993                             230,245
995                             207,528
8443                            134,627
465                             109,613
3389                            103,815
992                              32,216
444                              22,616
```

圖片來源：https://asciinema.org/a/48143

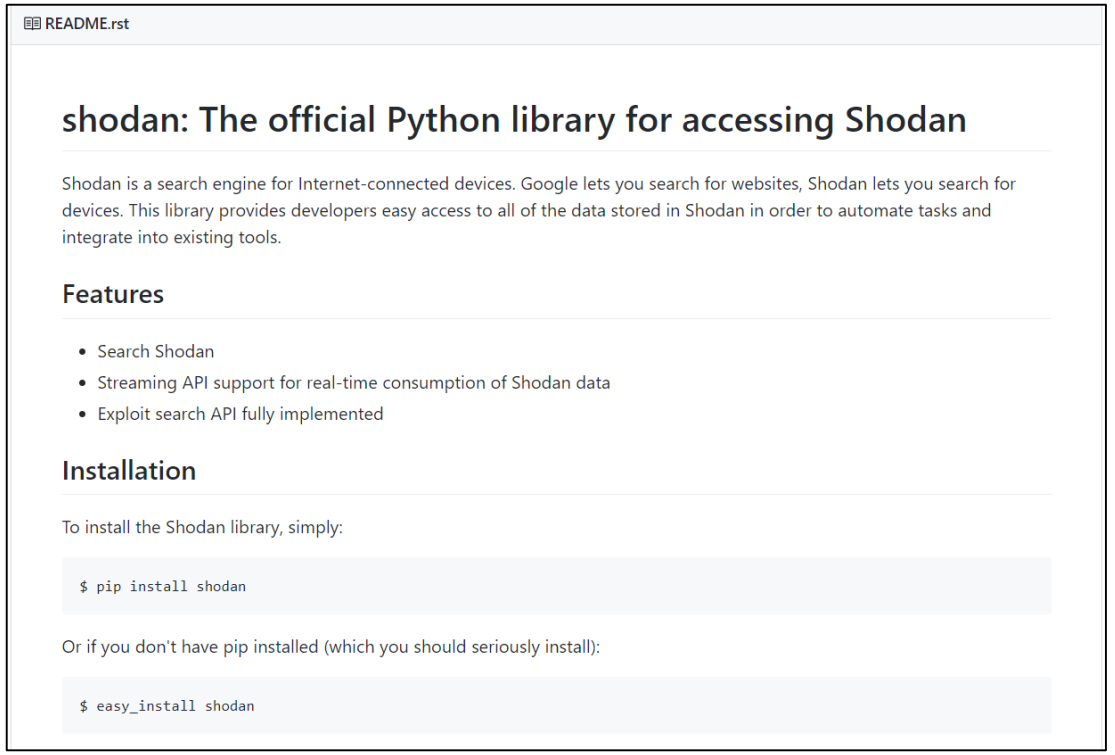
虛擬機環境

- OS:Ubuntu 14.04 LTS
- CPU: 1 core
- Memory: 2GB
- HD: 20GB
- Python版本: 2.7.6



安裝Shodan 套件

- 有兩種安裝指令可以安裝，兩個安裝方式差異不大
  - easy_install shodan
  - pip install shodan



README.rst

shodan: The official Python library for accessing Shodan

Shodan is a search engine for Internet-connected devices. Google lets you search for websites, Shodan lets you search for devices. This library provides developers easy access to all of the data stored in Shodan in order to automate tasks and integrate into existing tools.

Features

- Search Shodan
- Streaming API support for real-time consumption of Shodan data
- Exploit search API fully implemented

Installation

To install the Shodan library, simply:

```
$ pip install shodan
```

Or if you don't have pip installed (which you should seriously install):

```
$ easy_install shodan
```

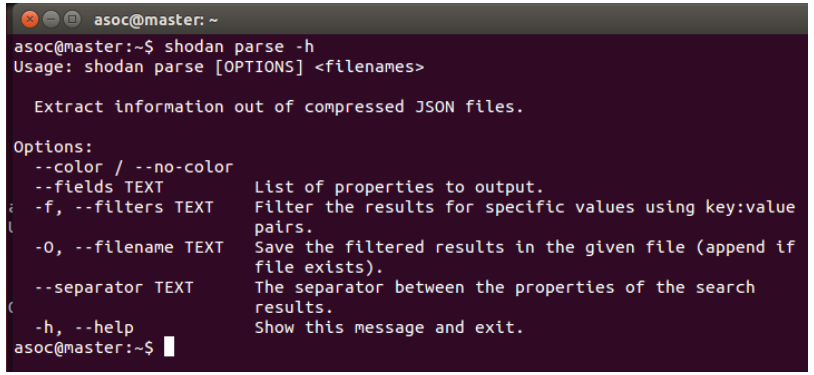
備註：

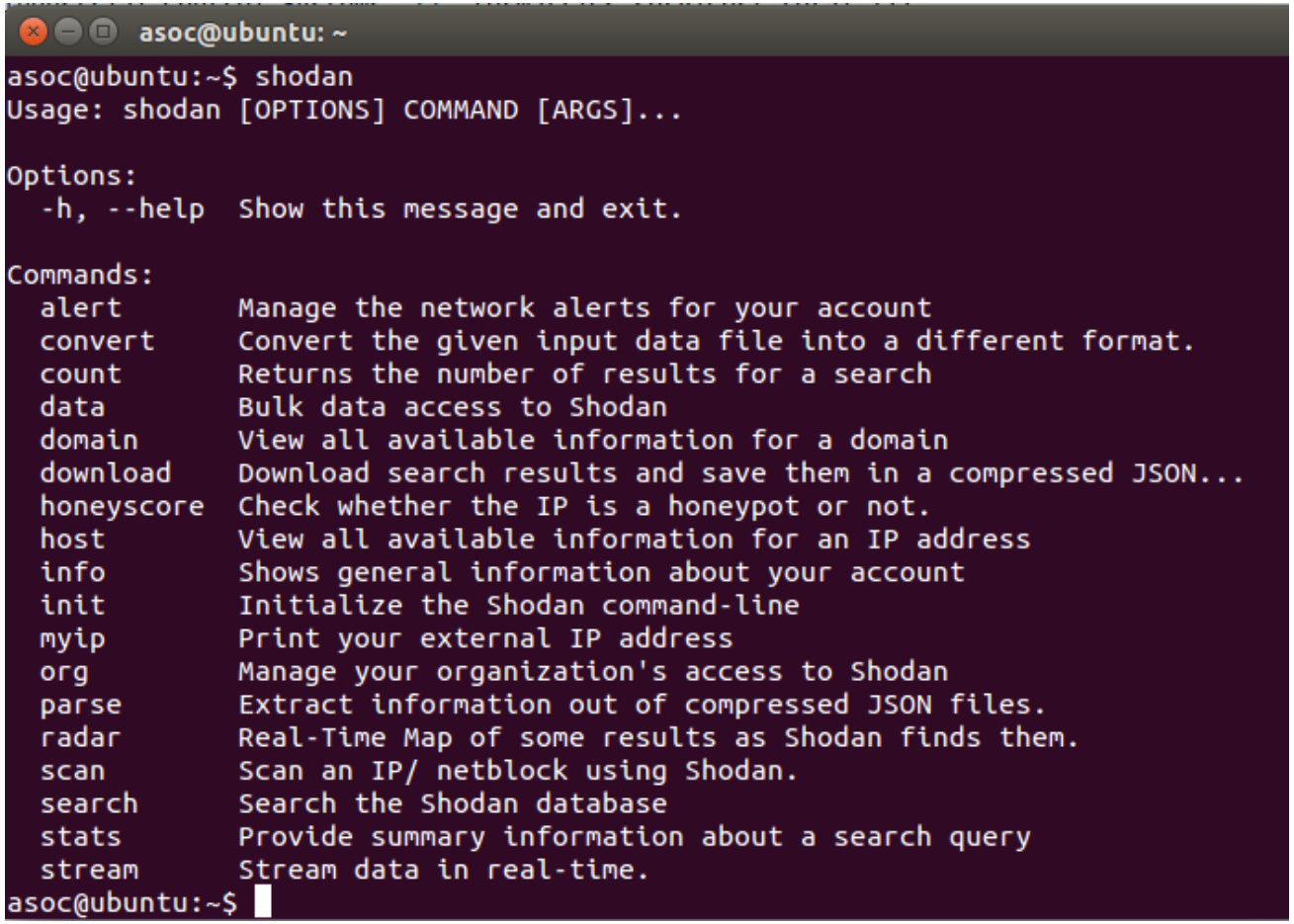
1. easy_install 要安裝python-setuptools
2. pip 要安裝python-pip

圖片來源：https://github.com/achillean/shodan-python

Shodan指令(1/2)

- 查詢可用指令
  - shodan
- 指令詳細用法
  - shodan <指令> -h
- 可用指令介紹可參考下一頁





Shodan指令(2/2)

Commands (基礎)	
指令	功能
init	帳號初始化
info	顯示帳號的資訊
myip	顯示使用者的IP
host	顯示一個IP所有可用的詳細資訊
count	回傳查詢結果數量
download	下載查詢結果*1
convert	轉換輸入文件到其他格式(csv、xlsx等)
honeyscore	檢查 IP 是否為蜜罐(Honeypot) *2
parse	解析提取壓縮的JSON資訊
search	查詢Shodan資料庫
stats	提供搜索結果的總結資訊

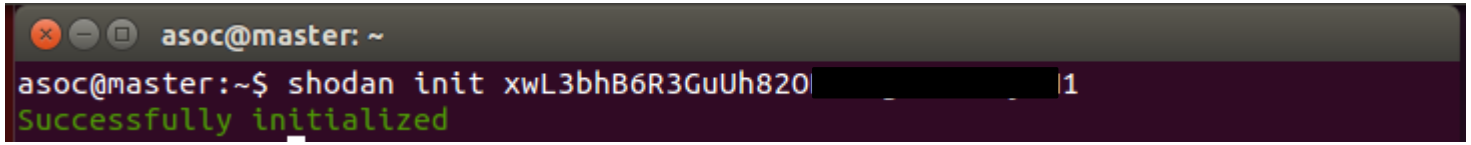
Commands (進階)	
指令	功能
alert	管理帳戶的網路告警事件(shodan monitor)
stream(企業)	即時顯示資料流
scan	使用Shodan掃描一個IP或網段*3
domain	查詢Domain的ip資訊*4
org (企業)	管理組織內部的shodan帳號
radar (企業)	即時觀看Shodan掃描資訊

1. 如果要下載大量資料，可能要花費query點數才能下載
2. 此分數僅供參考，Shodan並沒有公布判斷方式與標準
3. scan指令要花費scan點數；另外無法在短時間內scan同一個目標
4. domain指令要花費query點數

備註：
Shodan的指令data，因為測試時發現無法單獨使用，要搭配其他指令操作，怕混淆而不列在上面

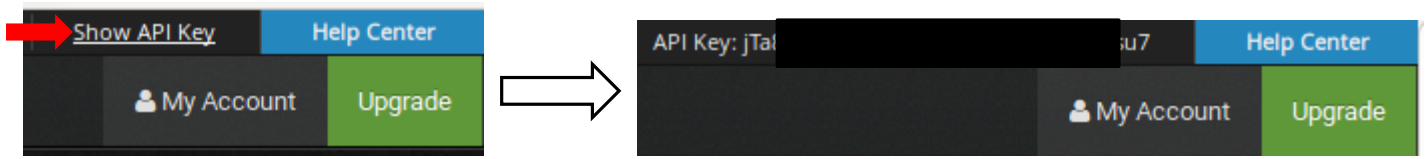
下載Shodan資料操作(1/3)

- 使用shodan指令前，要先輸入API Key
  - shodan init <API Key>



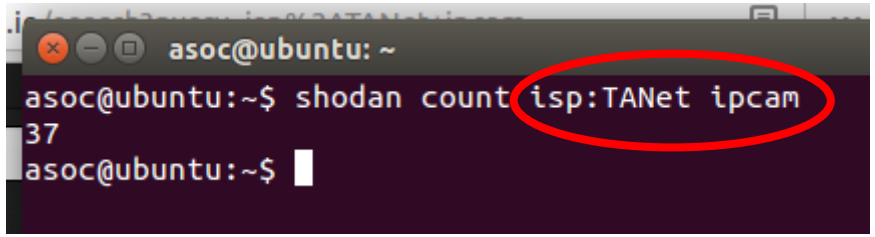
- 兩種方式取得API Key

1. 點選右上角Show API Key，之後會顯示個人帳號的API Key
2. 點選My Account，就可以看到了

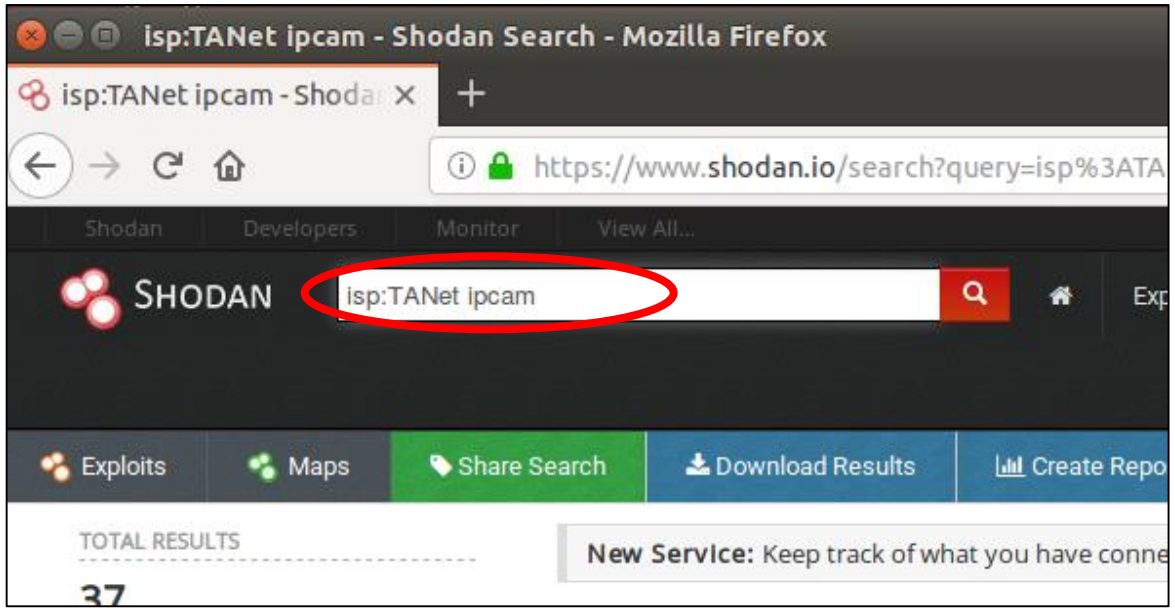


下載Shodan資料操作(2/3)

- 要調查校內有多少資料筆被Shodan紀錄，可以用count去查詢
  - shodan count <Key Word> (這裡關鍵字查詢跟網頁版相同)



備註：查詢的關鍵字先後順序不會影響查詢結果



下載Shodan資料操作(3/3)

- 要下載shodan的資料，用download指令；下載壓縮格式是.gz；儲存資訊為.json
- 指令為 shodan download <filename> <Key Word>
  - shodan download IPcam_TANet IPcam isp:TANet

```
asoc@ubuntu: ~
asoc@ubuntu:~$ shodan download IPcam_TANet IPcam isp:TANet
Search query:                    IPcam isp:TANet
Total number of results:         36
Query credits left:              0
Output file:                     IPcam_TANet.json.gz
  [########################################-]   97%  00:00:01
Saved 36 results into file IPcam_TANet.json.gz
asoc@ubuntu:~$
```

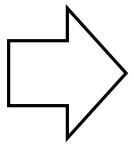
Shodan轉檔

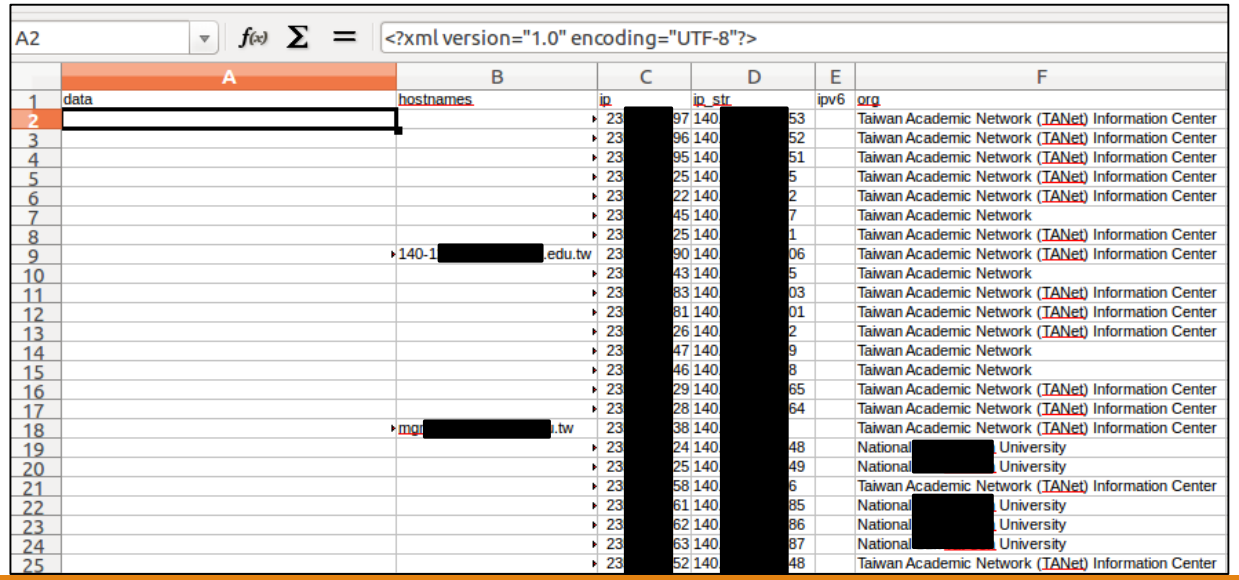
- 轉換輸入的文件到其他格式(可轉換格式有: kml、 csv、geo.json、images、xlsx)

➢ shodan convert <檔名.json.gz> <要轉換的格式>

➢ shodan convert TANet_ipcam.json.gz csv

```
asoc@ubuntu: ~
asoc@ubuntu:~$ shodan convert TANet_ipcam.json.gz csv
Successfully created new file: TANet_ipcam.csv
asoc@ubuntu:~$
```





	A	B	C	D	E	F
1	data	hostnames	ip	ip_str	ipv6	org
2			23[redacted]97	140[redacted]53		Taiwan Academic Network (TANet) Information Center
3			23[redacted]96	140[redacted]52		Taiwan Academic Network (TANet) Information Center
4			23[redacted]95	140[redacted]51		Taiwan Academic Network (TANet) Information Center
5			23[redacted]25	140[redacted]5		Taiwan Academic Network (TANet) Information Center
6			23[redacted]22	140[redacted]2		Taiwan Academic Network (TANet) Information Center
7			23[redacted]45	140[redacted]7		Taiwan Academic Network
8			23[redacted]25	140[redacted]1		Taiwan Academic Network (TANet) Information Center
9		140-1[redacted].edu.tw	23[redacted]90	140[redacted]06		Taiwan Academic Network (TANet) Information Center
10			23[redacted]43	140[redacted]5		Taiwan Academic Network
11			23[redacted]83	140[redacted]03		Taiwan Academic Network (TANet) Information Center
12			23[redacted]81	140[redacted]01		Taiwan Academic Network (TANet) Information Center
13			23[redacted]26	140[redacted]2		Taiwan Academic Network (TANet) Information Center
14			23[redacted]47	140[redacted]9		Taiwan Academic Network
15			23[redacted]46	140[redacted]8		Taiwan Academic Network
16			23[redacted]29	140[redacted]65		Taiwan Academic Network (TANet) Information Center
17			23[redacted]28	140[redacted]64		Taiwan Academic Network (TANet) Information Center
18		mgt[redacted].tw	23[redacted]38	140[redacted]		Taiwan Academic Network (TANet) Information Center
19			23[redacted]24	140[redacted]48		National[redacted] University
20			23[redacted]25	140[redacted]49		National[redacted] University
21			23[redacted]58	140[redacted]6		Taiwan Academic Network (TANet) Information Center
22			23[redacted]61	140[redacted]85		National[redacted] University
23			23[redacted]62	140[redacted]86		National[redacted] University
24			23[redacted]63	140[redacted]87		National[redacted] University
25			23[redacted]52	140[redacted]48		Taiwan Academic Network (TANet) Information Center

備註：
kml：經過查詢後是用在地圖製作上，目前應用在google map或google地球
Image：提出影像檔案，通常是RDP影像
geo.json：提出經緯度資訊，但是測試結果都是顯示錯誤，此功能疑似有問題

CSV的資料欄位

- 總共有31個欄位，可參考下圖
- 某些欄位的值可能為空(Null)，可能是當時掃描沒有抓到資訊

1	2	3	4	5	6	7	8	9
data	hostnames	ip	ip_str	ipv6	org	isp	location.country_code	location.city
10	11	12	13	14	15	16	17	18
location.country_name	location.latitude	location.longitude	os	asn	port	tags	timestamp	transport
19	20	21	22	23	24	25	26	27
product	version	vulns	ssl.cipher.version	ssl.cipher.bits	ssl.cipher.name	ssl.alpn	ssl.versions	ssl.cert.serial
28	29	30	31					
ssl.cert.fingerprint.sha1	ssl.cert.fingerprint.sha256	html	title					

CSV範例(部分敏感資訊已經刪除)

1	2	3	4	5	6	7	8	9
Data	hostnames	ip	ip_str	ipv6	org	isp	location.country_code	location.city
HTTP/1.0 401 Unauthorized Date: Thu, 01 Jan 1970 00:00:00 GMT Connection: close WWW-Authenticate: Basic realm="webcam" Content-Type: text/html		2XXXXXXX0	140.XXX.XXX.14		National X X University	Taiwan Academic Network (TANet) Information Center	TW	
10	11	12	13	14	15	16	17	18
location.country_name	location.latitude	location.longitude	os	asn	port	tags	timestamp	transport
Taiwan	23.5	121		ASXXXX7	80		2019-06-05T16:20:50.861880	tcp
19	20	21	22	23	24	25	26	27
product	version	vulns	ssl.cipher.version	ssl.cipher.bits	ssl.cipher.name	ssl.alpn	ssl.versions	ssl.cert.serial
28	29	30	31					
ssl.cert.fingerprint.sha1	ssl.cert.fingerprint.sha256	html	title					

xlsx的資料格式

- 總共有17個欄位，可參考下圖
- 某些欄位的值可能為空(Null)，可能是當時掃描沒有抓到資訊

1	2	3	4	5	6	7	8	9
IP	Port	Timestamp	Data	Hostnames	Organization	ISP	Country	Country ISO Code
10	11	12	13	14	15	16	17	
City	OS	ASN	Transport	Product	Version	Web Server	Website Title	

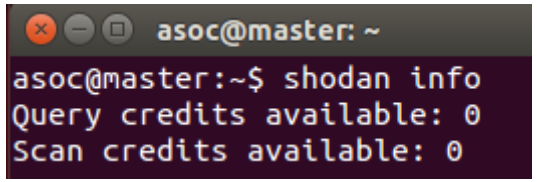
xlsx範例(部分敏感資訊已經刪除)

1	2	3	4	5	6	7	8	9
IP	Port	Timestamp	Data	Hostnames	Organization	ISP	Country	Country ISO Code
140.XXX.XXX.14	80	2019-06-05T16:20:50.861880	HTTP/1.0 401 Unauthorized Date: Thu, 01 Jan 1970 00:00:00 GMT Connection: close WWW-Authenticate: Basic realm="webcam" Content-Type: text/html		National X X University	Taiwan Academic Network (TANet) Information Center	Taiwan	TW

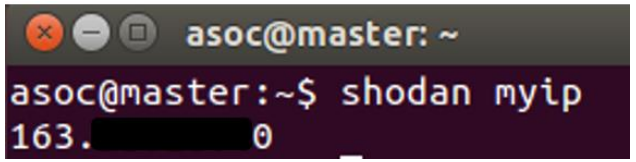
10	11	12	13	14	15	16	17
City	OS	ASN	Transport	Product	Version	Web Server	Website Title
		ASXXX7	tcp				401 Unauthorized

其他常用的Shodan指令

- 顯示目前帳號的資訊
  - shodan info



- 顯示使用者的IP
  - shodan myip



- 顯示一個IP所有可用的詳細資訊
  - shodan host <IP>

Shodan資料來源

- Shodan的掃描伺服器在全世界都有建置
- 每天都有在更新資料
- 資料限制：
  1. 不保證可以在短時間內獲得最新資訊，最晚一個月內會更新資料
  2. 每次更新時，上次的資料不一定馬上刪除

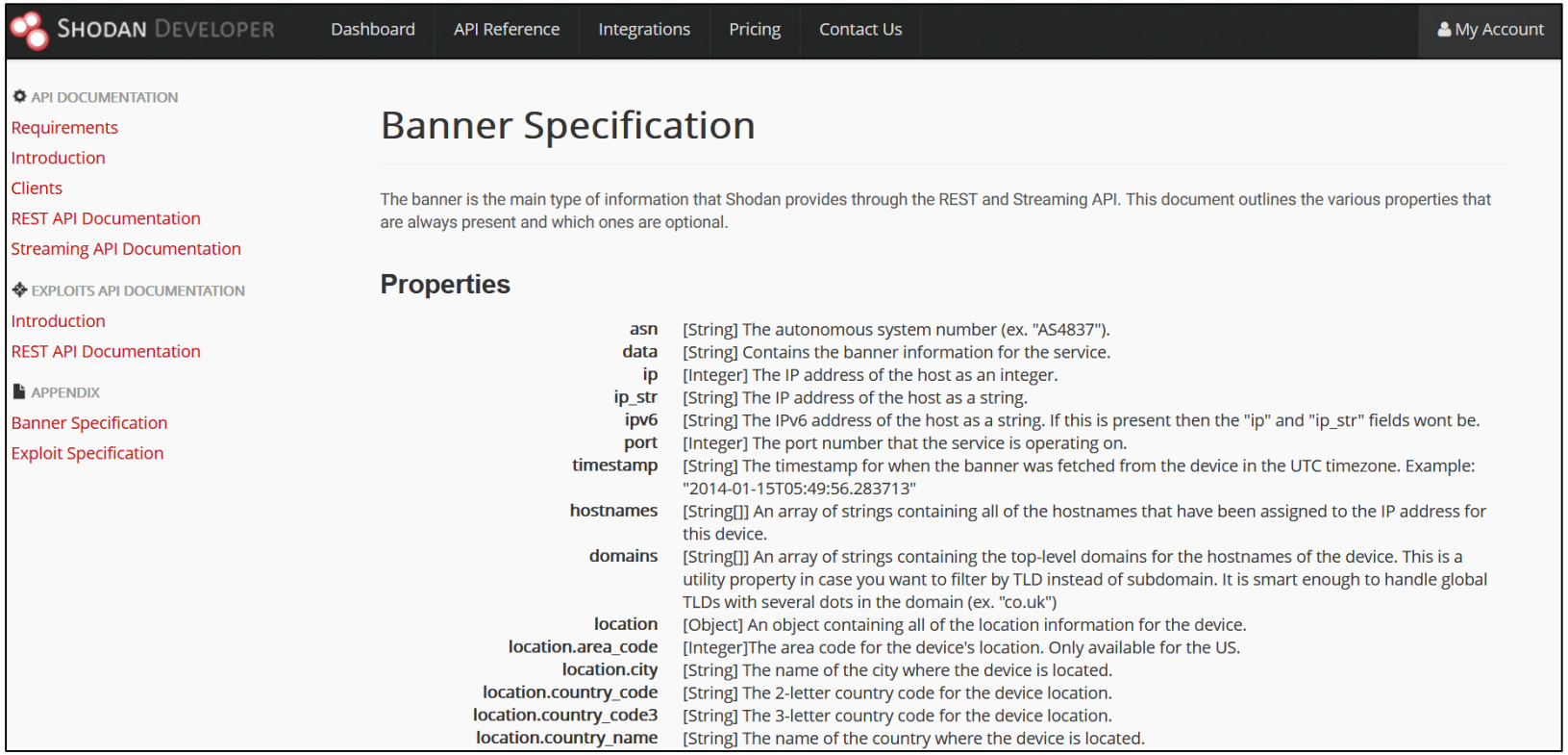
原始資料內容(部分敏感資訊已經刪除)

{"_shodan": {"id": "0528b36c-30d0-4d85-a7da-1caeeca532c1", "options": {}, "ptr": true, "module": "onvif", "crawler": "f7946cbe2dc20c40fcbcb81ad90aa01731b690ab"}, "hash": -512260510, "os": null, "opts": {}, "ip": 2OOOOOOO8, "isp": "Taiwan Academic Network (TANet) Information Center", "port": 3702, "hostnames": [], "location": {"city": “XXXXX", "region_code": "06", "area_code": null, "longitude": 120.44889999999998, "country_code3": "TWN", "country_name": "Taiwan", "postal_code": null, "dma_code": null, "country_code": "TW", "latitude": 23.47919999999999}, "timestamp": "2019-05-08T03:20:14.291096", "domains": [], "org": "Taiwan Academic Network (TANet) Information Center", "data": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<SOAP-ENV:Envelope xmlns:SOAP-ENV=\"http://www.w3.org/2003/05/soap-envelope\" xmlns:SOAP-ENC=\"http://www.w3.org/2003/05/soap-encoding\" xmlns:wsa=\"http://schemas.xmlsoap.org/ws/2004/08/addressing\" xmlns:d=\"http://schemas.xmlsoap.org/ws/2005/04/discovery\" xmlns:dn=\"http://www.onvif.org/ver10/network/wsdl\"><SOAP-ENV:Header><wsa:MessageID>uuid:1419d68a-1dd2-11b2-a105-001655099A2B</wsa:MessageID><wsa:To SOAP-ENV:mustUnderstand=\"true\">urn:schemas-xmlsoap-org:ws:2005:04:discovery</wsa:To><wsa:Action SOAP-ENV:mustUnderstand=\"true\">http://schemas.xmlsoap.org/ws/2005/04/discovery/Hello</wsa:Action></SOAP-ENV:Header><SOAP-ENV:Body><d:Hello><wsa:EndpointReference><wsa:Address>urn:uuid:1419d68a-1dd2-11b2-a105-001655099A2B</wsa:Address></wsa:EndpointReference><d:Types>dn:NetworkVideoTransmitter</d:Types><d:Scopes>onvif://www.onvif.org/type/video_encoder onvif://www.onvif.org/name/IPCam onvif://www.onvif.org/hardware/VIH_Series onvif://www.onvif.org/location onvif://www.onvif.org/Profile/Streaming</d:Scopes><d:XAddrs>http://140.XXX.XX.206:81/onvif/device_service</d:XAddrs><d:MetadataVersion>1</d:MetadataVersion></d:Hello></SOAP-ENV:Body></SOAP-ENV:Envelope>\n", "asn": "ASXXX9", "transport": "udp", "ip_str": "140.XXX.XX.206"}

備註：紅色字體是較為重要的資訊；綠色字體內容大多無固定格式，建議要自行挑出重要關鍵字，例如：IPCam

原始資料欄位介紹 (json格式)

- Shodan儲存的資料為Banner資訊，在Developers頁面中有詳細說明



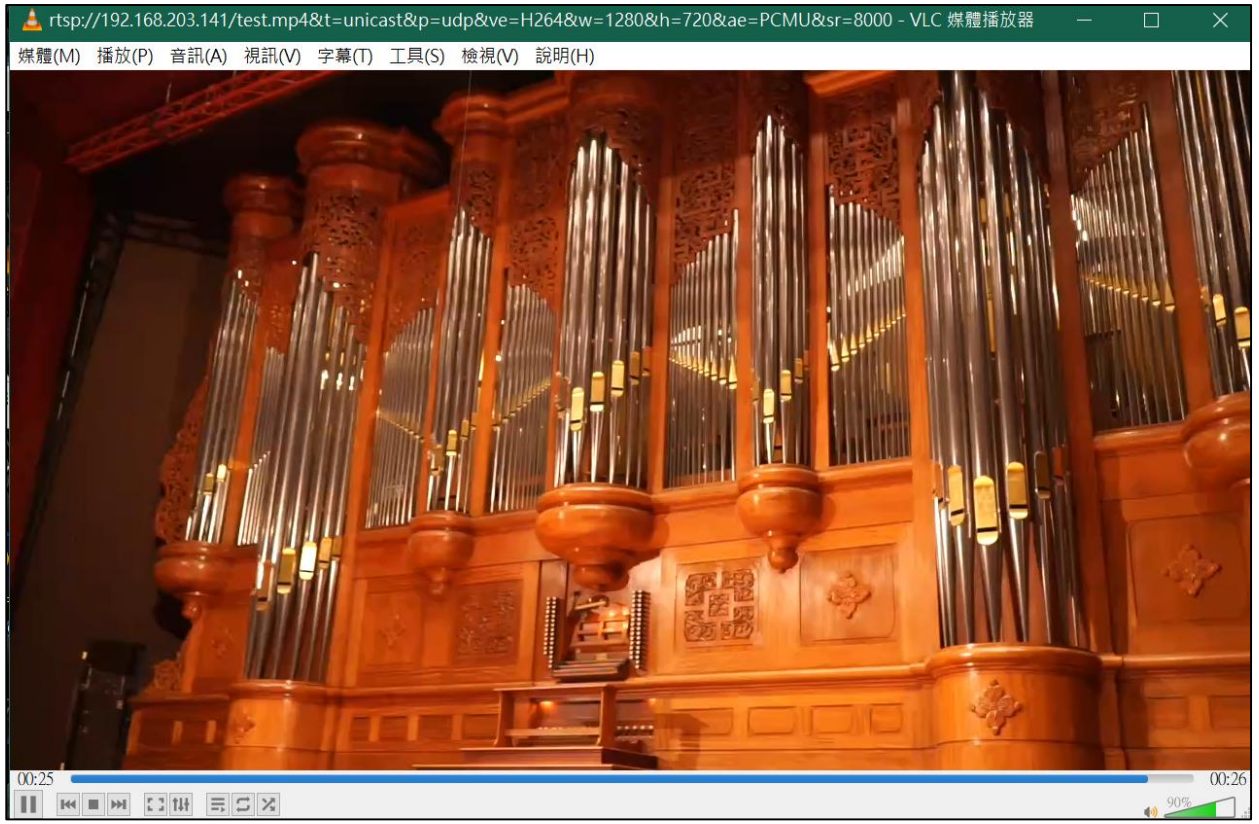
來源網址：https://developer.shodan.io/api/banner-specification

網路攝影機的特性

近期上課所學到的資訊，經過整理後的重點

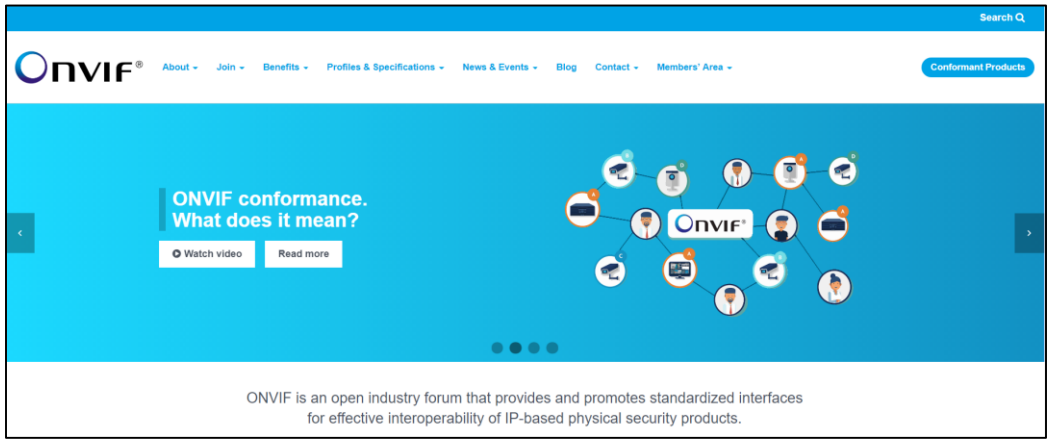
主要特徵

1. 支援ONVIF協定
2. 即時影音串流



ONVIF簡介

- ONVIF(英文全名：Open Network Video Interface Forum)，由Axis 、Bosch Security Systems以及Sony等三家公司在2008年合作建立的全球開放性論壇
- 其宗旨是促進不同廠牌的監控設備與系統的整合，幫助生產製造商、軟體開發商及獨立軟體供應商之間的可互通性
- ONVIF採用統一開放的標準作為IoT設備、儲存設備與管理系統之間的溝通協定，易於整合及擴充，因此逐漸為國內外視訊監控系統建置單位採用



圖片來源： https://www.onvif.org/

ONVIF規範

- 大部分的網路攝影機會遵守ONVIF規範(可參考下面兩張圖)
- 此規範規定要符合和支援XML及WSDL格式
- 影音串流則是透過 RTP(Real-time Transport Protocol) / RTSP (Real-time Streaming Protocol)協定

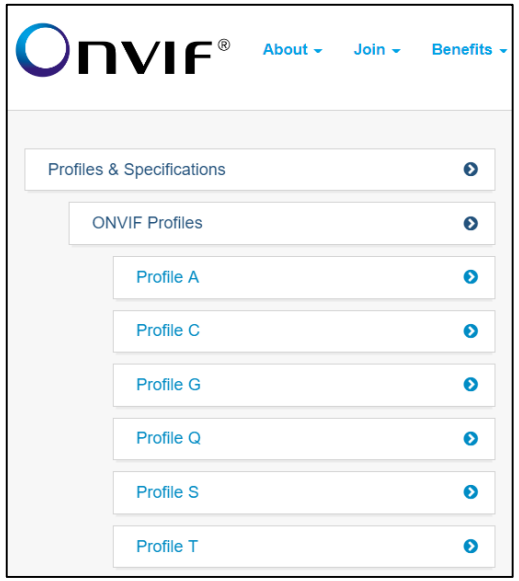
商品規格

型號:[redacted]		
系　統	操作系統	嵌入式RROS設計，雙核心32位DSP(H3518E)完美壓縮
	系統安全	三級用戶權限管理
	最大用戶數	4個用戶同時觀看
感應器	圖像傳感器	1/4英吋100萬像素運行CMOS Sensor 1280x720 Pixels
	傳感器性能	支援自動白平衡，自動加強控制，自動背光補償
	雜訊比	小於50dB
	鏡頭	f=3.6mm/F=2.0 標準紅外線鏡頭
	夜視	11顆850nmΦ5mm紅外線燈，夜視10-15公尺
	最低照度	0.1Lux/F1.6（彩色模式）,0.01Lux/F1.6（黑白模式）
视频	壓縮標示	H.264視訊編碼，支持ONVIF協定
	分辨率	支持雙編碼流, 主碼流：1280*720 子碼流：640*480

商品名稱：網路攝影機
商品型號：[redacted]
商品型態：IP Camera
感應器：CMOS
Technology：紅外線
特色：室外攝影機
解析度：1080P
速率：15fps、25fps
格式：H.264、MJPEG
鏡頭：3.6mm(固定焦距)、2.4mm(光圈)
夜視距離：5~10公尺
影像感應器：1/2.7" CMOS
ONVIF 2.0 協議 新增 NVR 產品
儲存：TF卡 64G (MAX)
網路連接(有線、WiFi)
1個RJ45以太網介面,10/100M自適應
支援 P2P
支援 AP
支援 HTTP、FTP、TCP/IP、UDP、SMTP、PPPOE、DHCP、DDNS、UPnP等網路協議

ONVIF配置文件說明

- ONVIF現今制定了六種配置文件(Profile)，英文大寫字母作區別(A、C、G、Q、S、T)
- 有定義門禁系統、網路監控設備、視訊儲存及管理系統的通訊方式與資料流
- 定義網路攝影機相關的協議是 Profile S



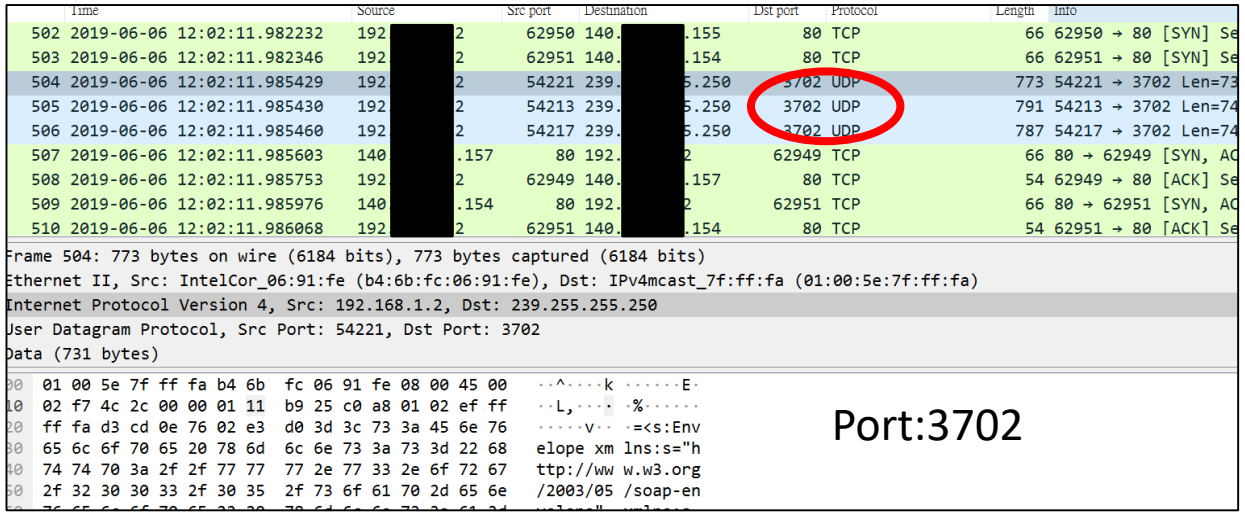
圖片來源：https://www.onvif.org/profiles/

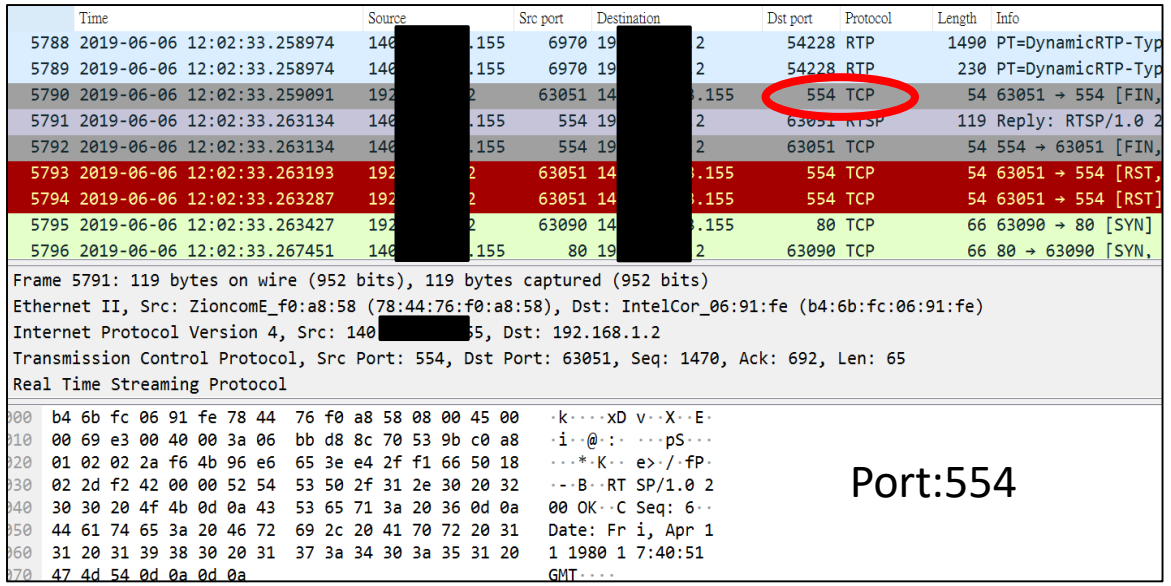
Profile S說明

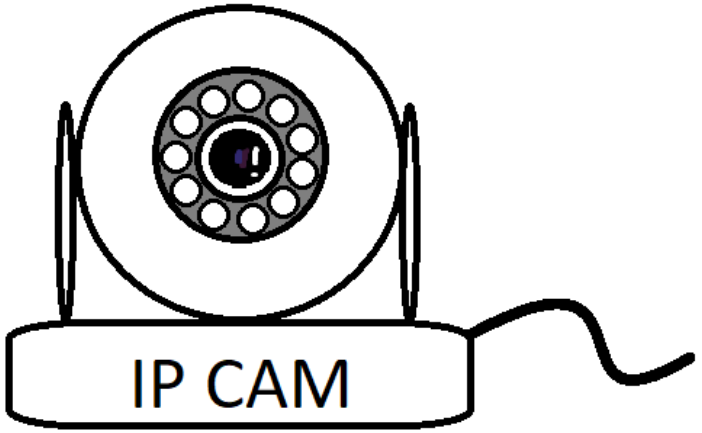
- 規範相容ONVIF協定中影像管理系統和裝置共用的共用功能，這些系統和裝置包括通過IP網路發送、配置、請求或控制媒體資料流程的IP攝影機或編碼器
- 有規範IP攝影機特定功能，例如搖攝(攝影機的方向控制)、變焦控制(鏡頭)、音訊流(輸入或輸出聲音)和指定中繼點輸出影像

網路攝影機相關特徵

1. 可能出現的關鍵字：ONVIF、IP cam、Webcam、RTSP、RTP
2. 特殊專用port：udp 3702
3. 影像串流port：tcp 554







結合Shodan尋找網路攝影機

根據前一頁的網路攝影機特徵資料，搭配SHODAN資料找出IP CAM

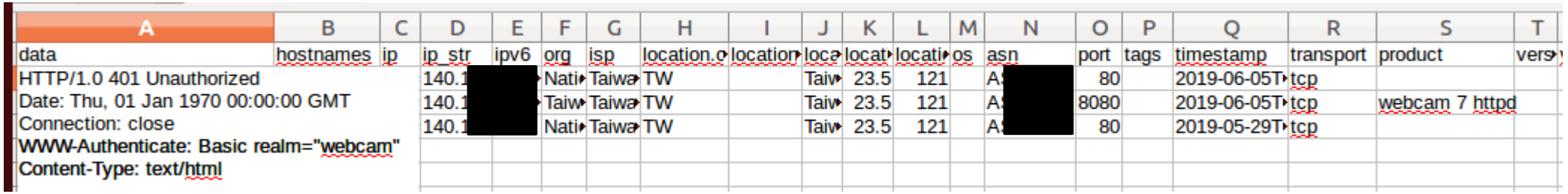
收集資料

1. 用掃描工具去掃IP，得到資料(例如：nmap)
   - 優點：資料可以隨時更新
   - 缺點：可能會被阻擋、視為網路攻擊等

2. 從Shodan下載資料
   - 優點：省時間去取得資訊(全世界)
   - 缺點：資料不能隨時更新、需要點數(金錢)

分析資料

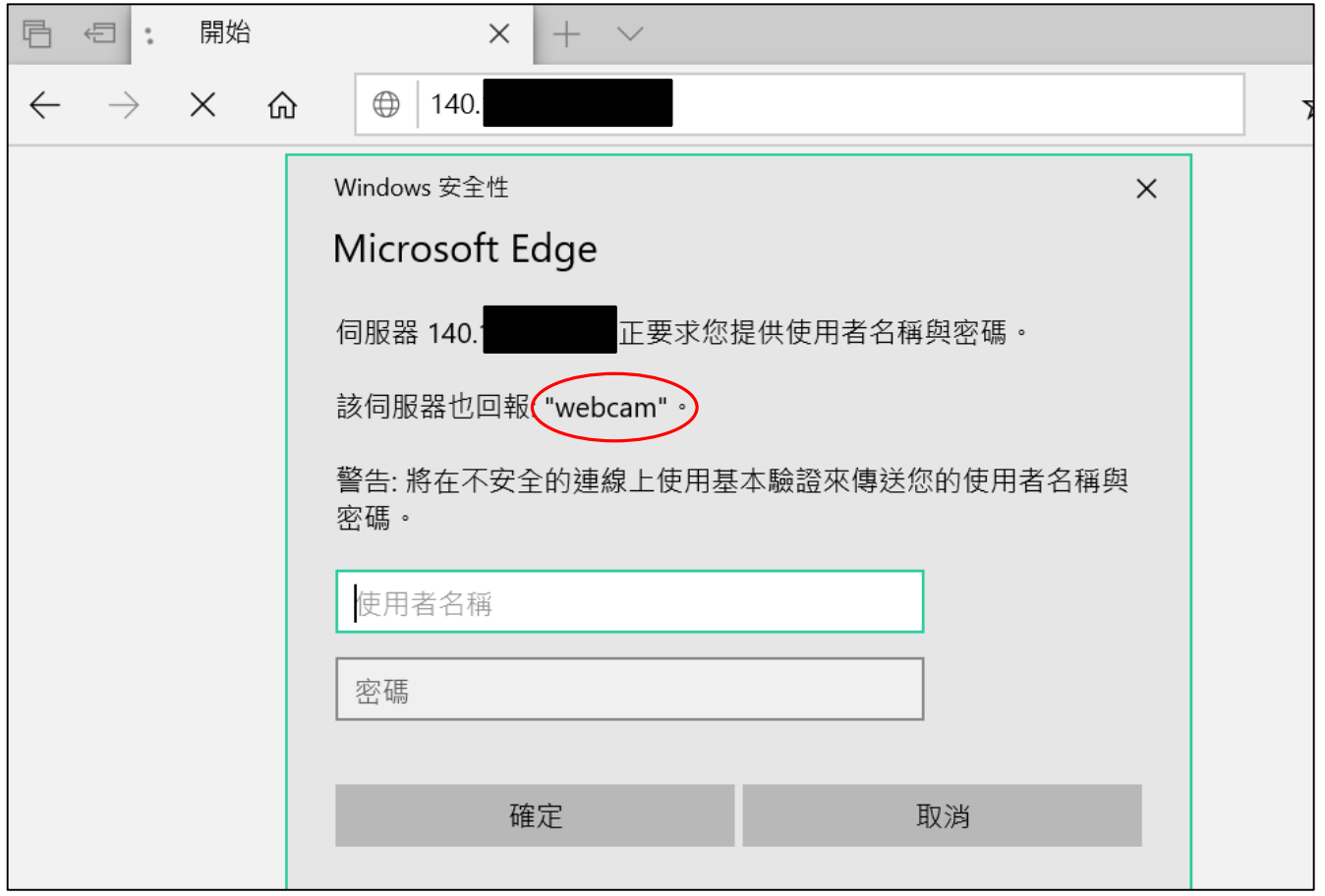
1. 轉成csv、xlsx等格式，做後續的資料分析
2. 參考**網路攝影機相關特徵**，對幾個欄位找尋相關的特徵，列出可能是網路攝影機的IP



data	hostnames	ip	ip_str	ipv6	org	isp	location.c	location	loca	locat	locati	os	asn	port	tags	timestamp	transport	product	vers
HTTP/1.0 401 Unauthorized			140.1[redacted]		Nati	Taiwa	TW		Taiw	23.5	121		A[redacted]	80		2019-06-05T	tcp		
Date: Thu, 01 Jan 1970 00:00:00 GMT			140.1[redacted]		Taiw	Taiwa	TW		Taiw	23.5	121		A[redacted]	8080		2019-06-05T	tcp	webcam 7 httpd	
Connection: close			140.1[redacted]		Nati	Taiwa	TW		Taiw	23.5	121		A[redacted]	80		2019-05-29T	tcp		
WWW-Authenticate: Basic realm="webcam"																			
Content-Type: text/html																			

3. 針對這些IP列表，利用瀏覽器、ONVIF相關程式檢驗這些IP是否為網路攝影機

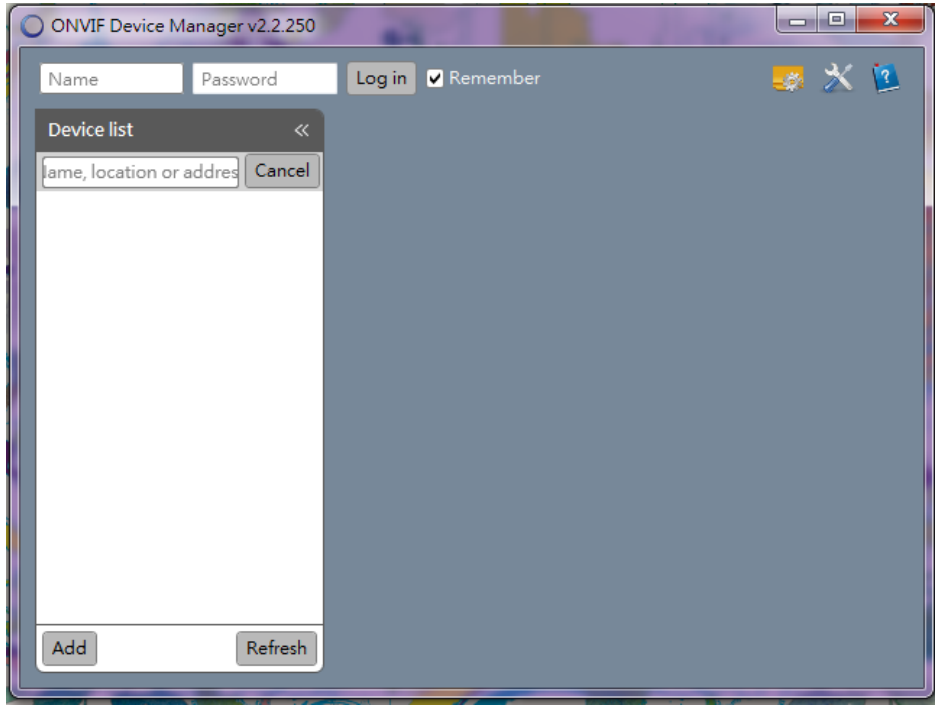
驗證資料(瀏覽器)


開始
140.[redacted]
Windows 安全性
Microsoft Edge
伺服器 140.[redacted]正要求您提供使用者名稱與密碼。
該伺服器也回報: "webcam"。
警告: 將在不安全的連線上使用基本驗證來傳送您的使用者名稱與密碼。
使用者名稱
密碼
確定
取消

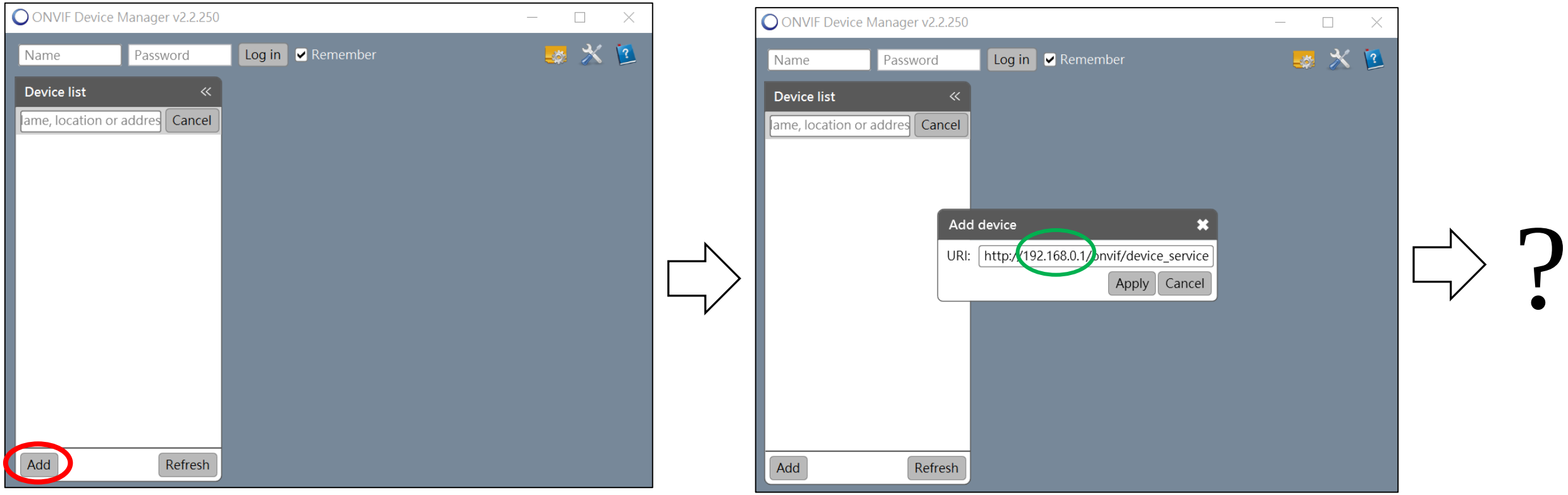
ONVIF檢查程式：ONVIF Device Manager介紹

- 是一個可以檢查網路中的網路視訊設備(如IP cam)、網路儲存系統(如NAS)是否有符合ONVIF協議的程式(程式名稱縮寫ODM)
- 是用C#開發，支援英語、俄語兩種語系
- 免費軟體，有開放原始碼
- 目前找到的最新版本是2.2.250 (2016.11.15)
- 預設會檢查內網網段(EX：192.168.X.X/24)，

如果在內網中找到ONVIF協定設備，它會自動列在Device list中



ODM操作過程



1. 按下Add
2. 新增要連線的IP(修改綠圈處)
3. 根據跳出的訊息，決定下一步

狀況一：沒有出現ONVIF標誌

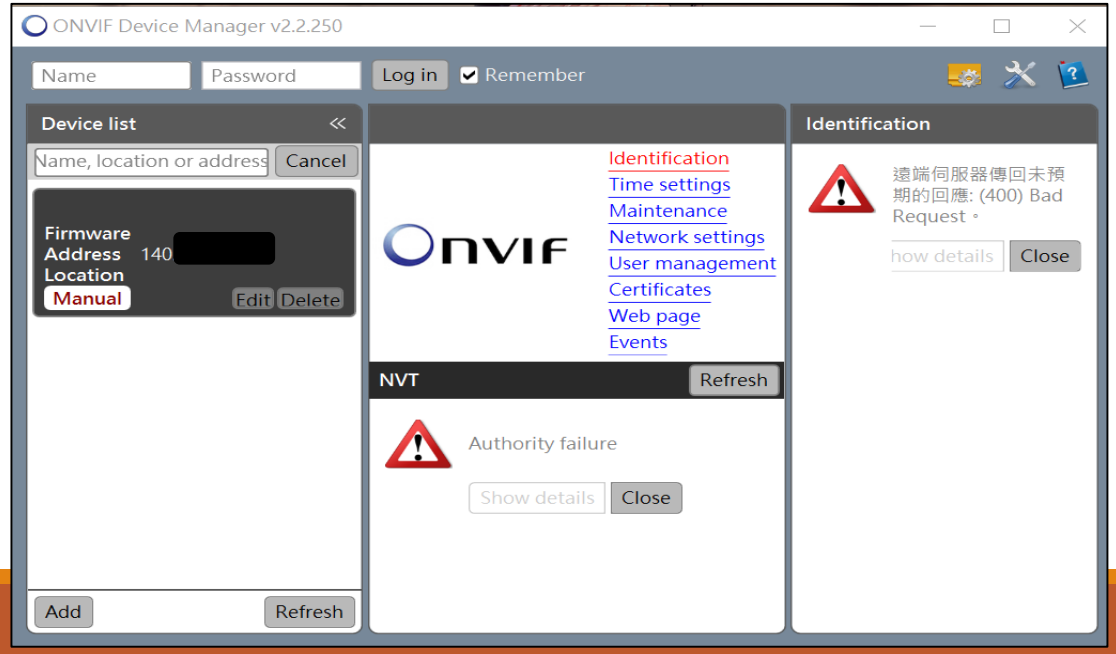
- 出現這個訊息，可能有兩種情況：

1. 連線被阻擋
2. 不是IP Cam

- 可能要配合瀏覽器登入檢查，來確認此IP是否為IP Cam

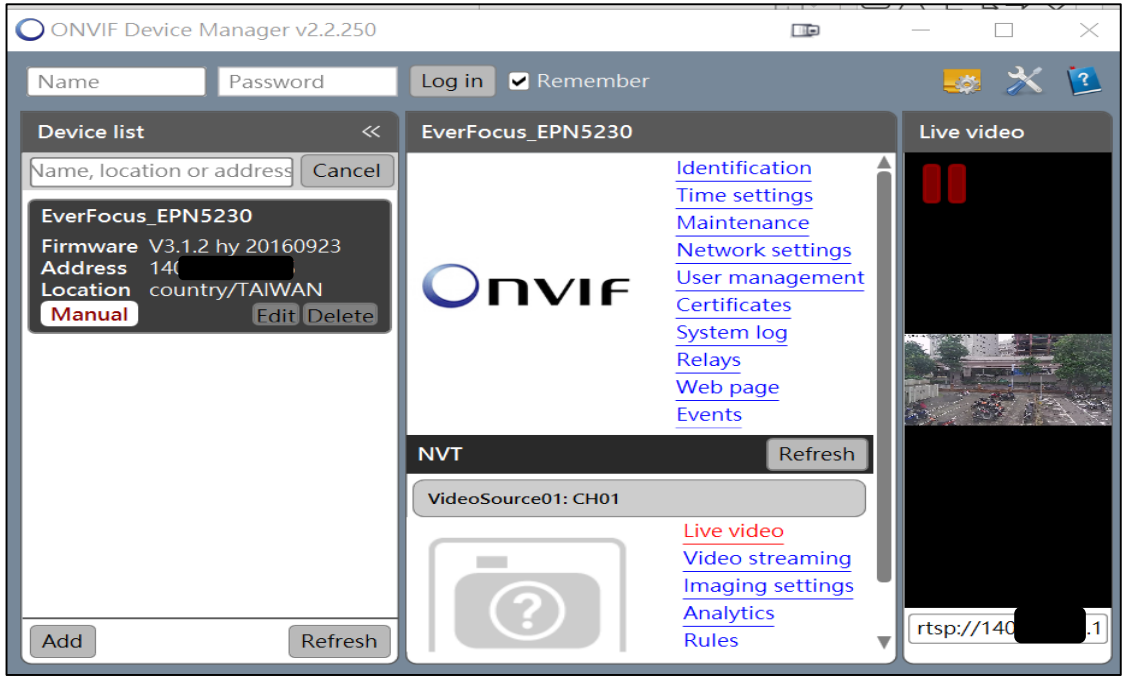
狀況二：需要登入設備

- 出現ONVIF標誌及一些連結，但是出現授權(登入)相關問題，此時這個IP有高機率是IP Cam
- 如果要更詳細檢查，則可以用一些預設帳號密碼去嘗試登入
- 一旦用預設帳號密碼登入該設備，請盡快提醒設備負責人修改帳號密碼



狀況三：直接登入IP Cam

- 此狀況較為嚴重，這說明這個設備可以利用ODM直接觀看攝影機內容、修改帳號密碼權限，需要立即通知設備負責人做出修正。



總結

- Shodan是一個非常適合找尋IoT設備的大資料庫
- 業界也是利用ONVIF協定去找網路攝影機
- 目前還沒有找到可自動化且大量確認網路攝影機的方法

報告完畢　　謝謝大家