GIS Application in Firewall Security Log Visualization

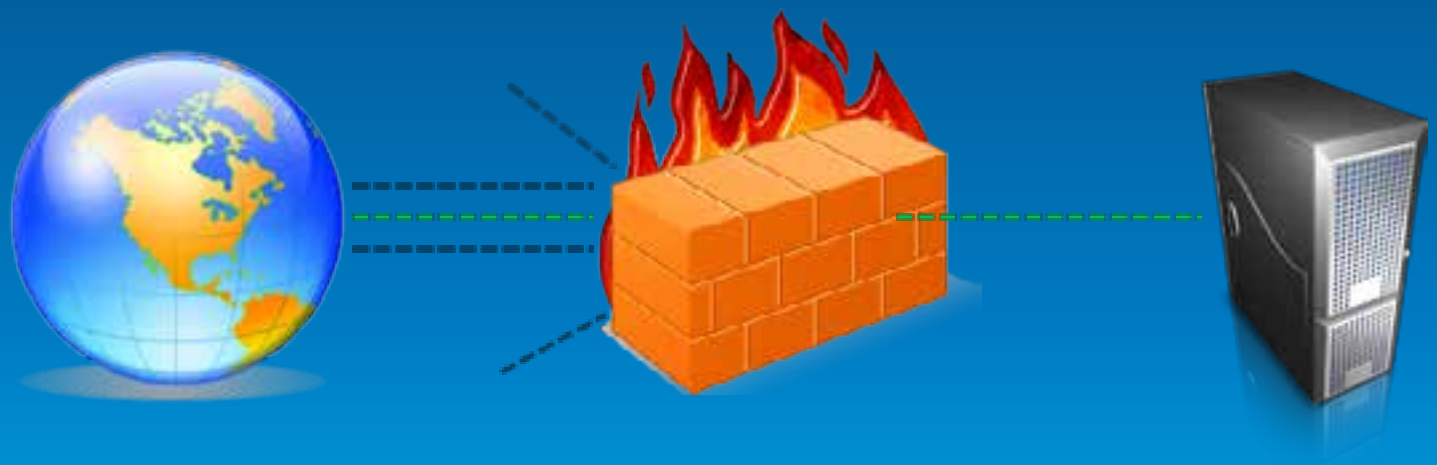
Juliana Lo

Presentation Outline

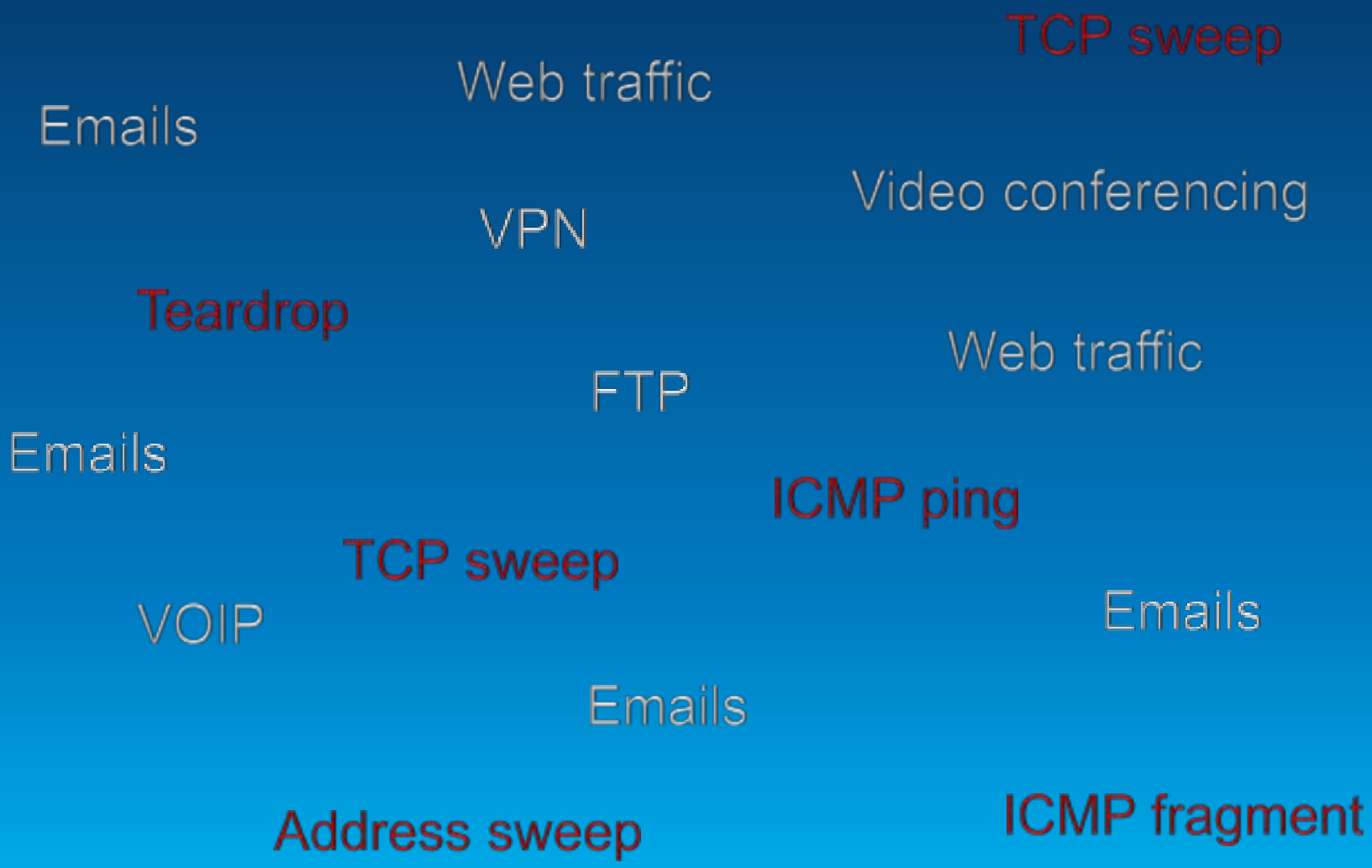
- What is a firewall
- Problem definition
- Project goal, objectives, constraints
- Framework and system components
- Solution
- Conclusions

Firewall Definition

A firewall is a hardware or software designed to permit or deny network traffic based on a set of rules
Protect networks from unauthorized access.



Good and Bad Firewall Traffic



Bad Firewall Traffic

ICMP ping

ICMP fragment

TCP sweep

Sync flood

Port scan

Address sweep

Log File

Jun 1 22:01:35 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:54886 to 2.3.4.5:406, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:03)
Jun 1 22:01:57 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:55181 to 2.3.4.5:1358, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:25)
Jun 1 22:02:10 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:55339 to 2.3.4.5:1515, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:38)
Jun 2 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436

Firewall Security Log File

Jun 1 22:01:35 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:54886 to 2.3.4.5:406, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:03)
Jun 1 22:01:57 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:55181 to 2.3.4.5:1358, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:25)
Jun 1 22:02:10 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:55339 to 2.3.4.5:1515, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:38)
Jun 2 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436

Important for

- System monitoring, compliance, forensics

Challenges

- Too much information to go through
- Can’t relate IP address to origin of traffic

Log File Transformation

Jun 1 22:01:35 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:54886 to 2.3.4.5:406, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:03)
Jun 1 22:01:57 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: Port scan! From 1.2.3.4:55181 to 2.3.4.5:1358, proto TCP (zone Untrust, int untrust). Occurred 1 times. (2004-06-01 22:09:25)

Desired Outcome

Project Goal, Objectives, Constraints

Goal

- Develop a geolocation map application to visualize firewall traffic in near-real time

Objectives

- Geolocate IP address into locations
- Near real-time events

Constraints

- Project duration - weeks not months
- Cost – low budget

Development Framework

- Data Collection
  - Server to capture firewall traffic
- Parsing Engine
  - Parser to extract IP addresses and other information
- Geolocation Service
  - Convert IPv4 address into location
- Database Service
  - Append features and search for records
- Visualization
  - Application to visualize IP locations

System Components

- Firewall
  Source of data Juniper Netscreen firewall

- IDE
  Windows 7 development server for data collection, parsing, geolocation, and data updates

- Database
  CartoDB's PostgreSQL database

- Map application
  Javascript, HTML, CartoDB API, Leaflet, jQuery

Solution - Data Automation

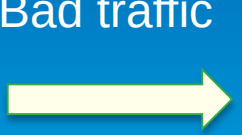
Step 1 - Firewall

Configure system logging messages

- **Emergency (severity 0)**—The system is unusable
- **Alert (severity 1)**—Immediate action is needed
- **Critical (severity 2)**—Critical condition
- **Error (severity 3)**—Error condition
- **Warning (severity 4)**—Warning condition
- **Notification (severity 5)**—Normal but significant condition
- **Informational (severity 6)**—Informational message
- **Debugging (severity 7)**—Debugging message

Enable external data monitor

Bad traffic

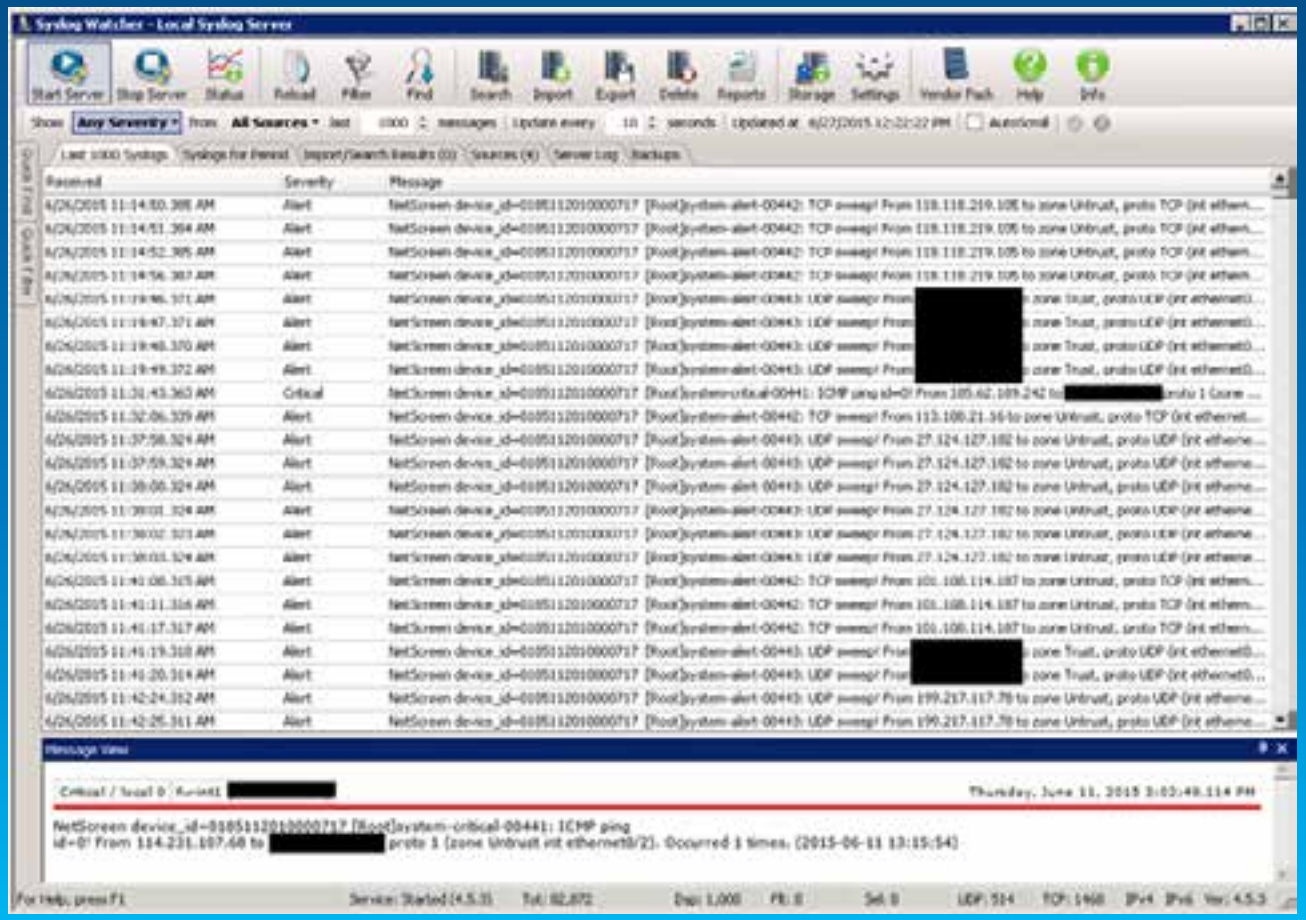


Syslog server

Solution - Data Automation

Step 2 – Data Collection

Install Syslog Watcher software on Windows machine to collect firewall traffic



Solution - Data Automation

Step 3 – Parser Engine

Simple data extraction program

```
6/27/2015 12:07 PM,1.2.3.4,Critical,2,NetScreen device_id=0185112010000717  [Root]system-critical-00441: ICMP ping id=0! From 167.114.210.98 to 1.2.3.82, pro
6/27/2015 12:07 PM,1.2.3.4,Critical,2,NetScreen device_id=0185112010000717  [Root]system-critical-00441: ICMP ping id=0! From 167.114.210.98 to 1.2.3.82, pro
6/27/2015 12:08 PM,1.2.3.4,Critical,2,NetScreen device_id=0185112010000717  [Root]system-critical-00441: ICMP ping id=0! From 167.114.210.98 to 1.2.3.90, pro
6/27/2015 12:14 PM,1.2.3.4,Critical,2,NetScreen device_id=0185112010000717  [Root]system-critical-00441: ICMP ping id=0! From 167.114.210.98 to 1.2.3.10, pro
6/27/2015 12:15 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 196.32.151.99 to zone Untrust, proto TCP
6/27/2015 12:15 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 196.32.151.99 to zone Untrust, proto TCP
6/27/2015 12:28 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00443: UDP sweep! From 62.75.145.240 to zone Untrust, proto UDP
6/27/2015 12:28 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00443: UDP sweep! From 62.75.145.240 to zone Untrust, proto UDP
6/27/2015 12:28 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00443: UDP sweep! From 62.75.145.240 to zone Untrust, proto UDP
6/27/2015 12:28 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00443: UDP sweep! From 62.75.145.240 to zone Untrust, proto UDP
6/27/2015 12:28 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00443: UDP sweep! From 62.75.145.240 to zone Untrust, proto UDP
6/27/2015 12:28 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00443: UDP sweep! From 62.75.145.240 to zone Untrust, proto UDP
6/27/2015 12:28 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00443: UDP sweep! From 62.75.145.240 to zone Untrust, proto UDP
6/27/2015 12:30 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 117.192.37.121 to zone Untrust, proto TCP
6/27/2015 12:30 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 117.192.37.121 to zone Untrust, proto TCP
6/27/2015 12:30 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 117.192.37.121 to zone Untrust, proto TCP
6/27/2015 12:30 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 117.192.37.121 to zone Untrust, proto TCP
6/27/2015 12:30 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 117.192.37.121 to zone Untrust, proto TCP
6/27/2015 12:30 PM,1.2.3.4,Alert,1,NetScreen device_id=0185112010000717  [Root]system-alert-00442: TCP sweep! From 117.192.37.121 to zone Untrust, proto TCP
```

Python program extracts time stamp, firewall host, message level, error, from host, and number of occurrences

Solution - Data Automation

Step 4 – Geolocation Service

Program to look up location from IP address

Uses MaxMind GeoLite City Database

Python API

```
import pygeoip
gi = pygeoip.GeoIP('C:\\geocode\\GeoLiteCity.dat', pygeoip.MEMORY_CACHE)
from_ip = '123.184.114.169'
rec = gi.record_by_addr(from_ip)
city =rec['city']
country = rec['country_name']
latitude = rec['latitude']
longitude = rec['longitude']
print city, country, latitude, longitude

>>> 'Shenyang','China',41.7922,123,4328
```

Solution - Data Automation

Step 5 – Database Update

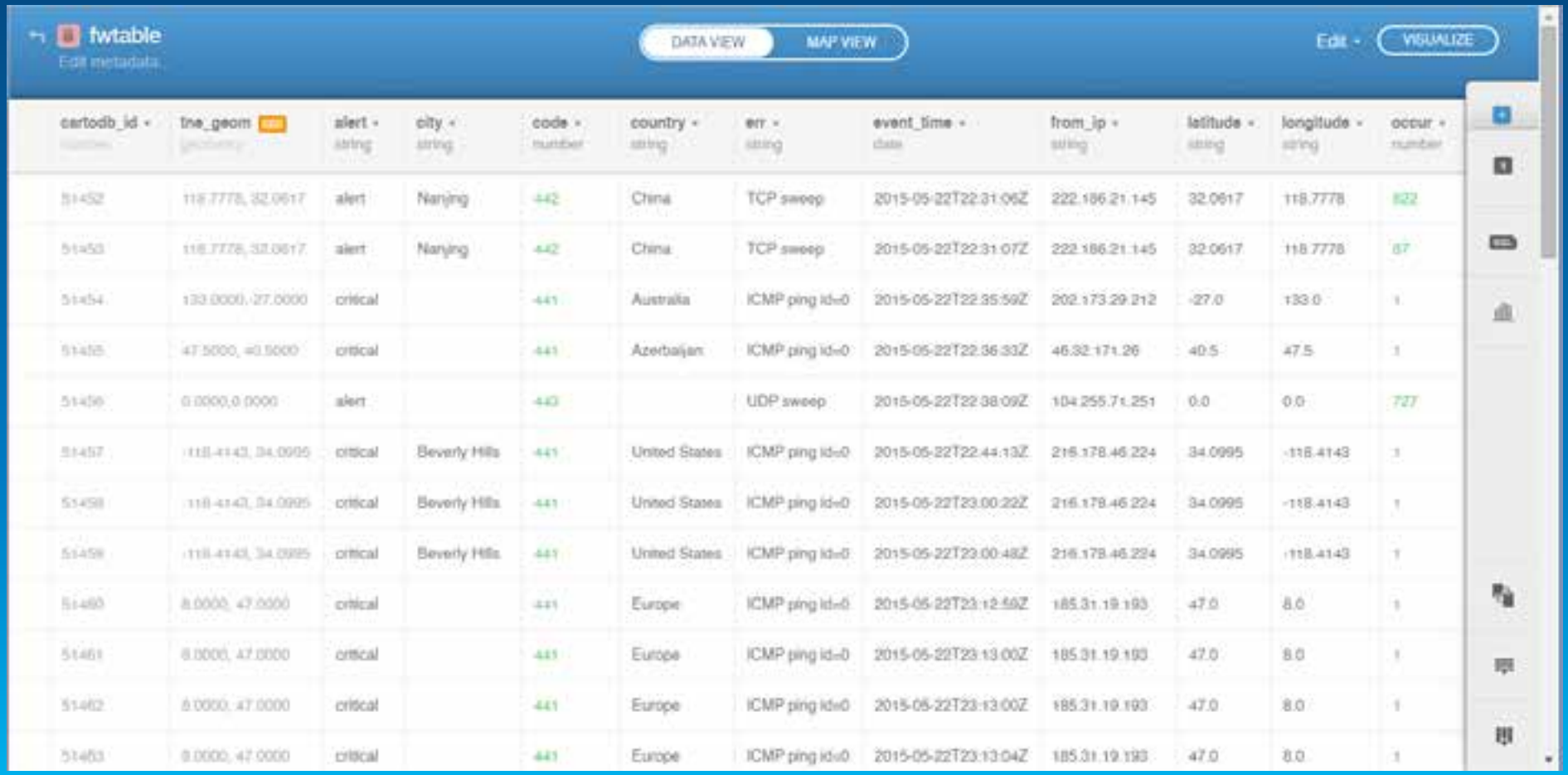
Program to append new features to CartoDB's PostGRES database

Python API

```
from cartodb import CartoDBAPIKey, CartoDBException

API_KEY ='<api_key''
DOMAIN = '<user_name>'
TABLE = 'table_name'

COLUMNS = 'the_geom,alert,city,code,country,err,event_time,from_ip,latitude,longitude,
                    occur'
cl = CartoDBAPIKey(API_KEY, DOMAIN)
vals  = "CDB_LatLng(%s,%s),'%s','%s',%s,'%s','%s','%s','%s','%s','%s','%s',%s,%s

sql = 'INSERT into %s (%s) VALUES (%s);' % (TABLE,COLUMNS,vals)
cl.sql(sql)
```

Solution - Data Automation

Step 5 – Database Table View

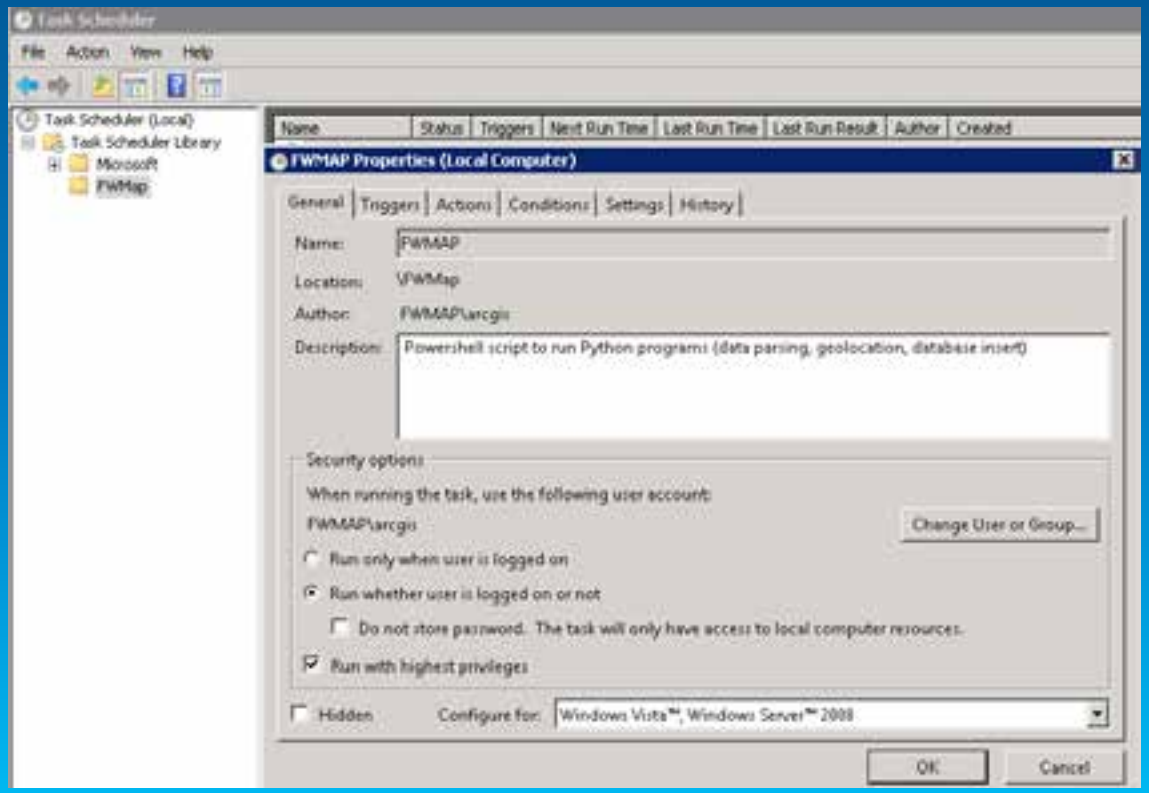


Solution - Data Automation

Step 6 – Automated Updates

Use Window's Task Scheduler to automate the programs

Auto-start every 5 minutes



Solution - Application Development

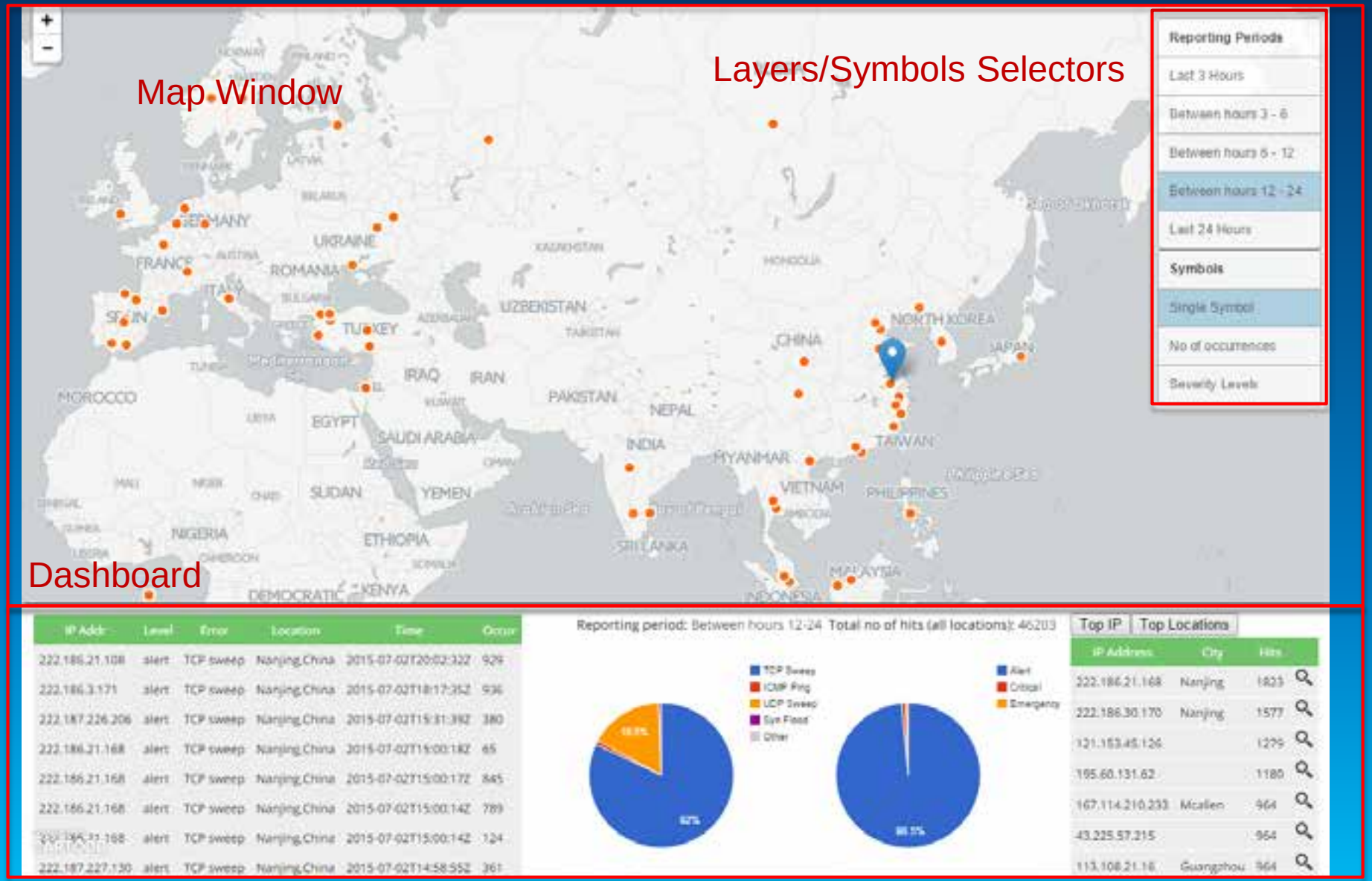
Language: JavaScript

Libraries: CartoDB API, Leaflet, jQuery

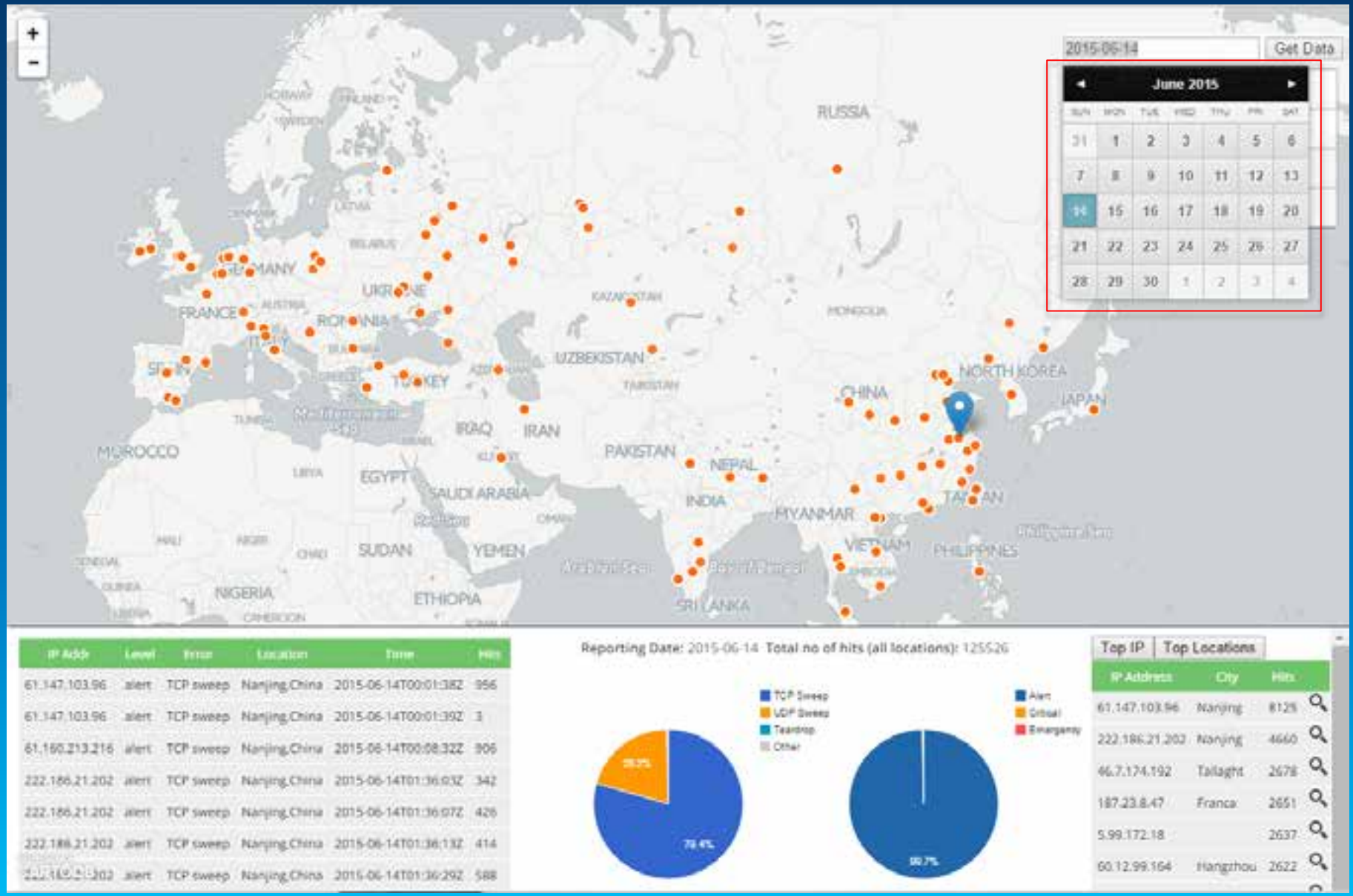
Editor: NotePad+

Debugging tool: Google Chrome JavaScript Console

Results - Hits from Last 24 Hours



Results – Select a date



Results – Clickable Features

Click on a feature in the map to show details

IP Addr	Level	Error	Location	Time	Occur
222.186.31.178	alert	TCP sweep	Nanjing,China	2015-06-27T20:32:19Z	85
222.186.31.178	alert	TCP sweep	Nanjing,China	2015-06-27T20:32:19Z	787
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-27T20:26:08Z	556
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-27T20:25:33Z	642
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-27T20:25:09Z	764
61.132.13.10	alert	TCP sweep	Nanjing,China	2015-06-27T20:06:55Z	553
222.186.21.48	alert	TCP sweep	Nanjing,China	2015-06-27T19:58:11Z	963
222.187.227.130	alert	TCP sweep	Nanjing,China	2015-06-27T16:21:47Z	942
61.160.223.78	alert	TCP sweep	Nanjing,China	2015-06-27T15:39:35Z	539
58.221.4.182	alert	TCP sweep	Nanjing,China	2015-06-27T15:28:41Z	394
58.221.4.182	alert	TCP sweep	Nanjing,China	2015-06-27T15:28:40Z	496
58.215.49.13	alert	TCP sweep	Nanjing,China	2015-06-27T15:10:54Z	365
58.215.49.13	alert	TCP sweep	Nanjing,China	2015-06-27T15:10:53Z	564
222.186.31.161	alert	TCP sweep	Nanjing,China	2015-06-27T13:24:48Z	620
222.186.31.161	alert	TCP sweep	Nanjing,China	2015-06-27T13:24:47Z	283
222.186.21.208	alert	TCP sweep	Nanjing,China	2015-06-27T10:16:46Z	964
222.186.21.208	alert	TCP sweep	Nanjing,China	2015-06-27T10:16:38Z	869
222.186.21.208	alert	TCP sweep	Nanjing,China	2015-06-27T10:15:18Z	846
222.186.30.214	alert	TCP sweep	Nanjing,China	2015-06-27T09:29:41Z	257
222.186.30.214	alert	TCP sweep	Nanjing,China	2015-06-27T09:29:41Z	696

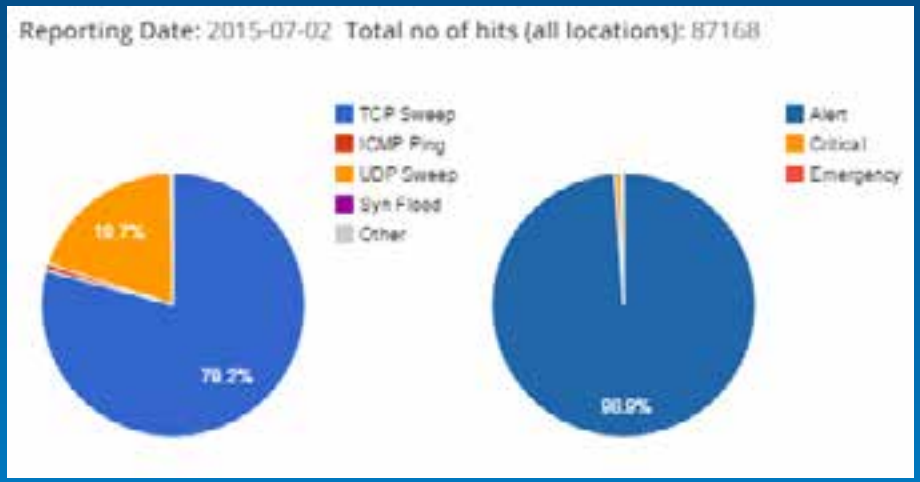
Top hosts or locations

Top IP | Top Locations

IP Address	City	Hits
222.186.21.208	Nanjing	2679
222.186.21.202	Nanjing	1862
107.160.45.216		1828
61.176.221.52	Shenyang	1825
107.161.82.240		964
104.233.142.219		964
27.254.44.45		964
222.186.21.48	Nanjing	963
222.186.30.214	Nanjing	953
222.187.227.130	Nanjing	942

Results – Application Features

Pie charts show the distribution of hits by error types and by severity levels



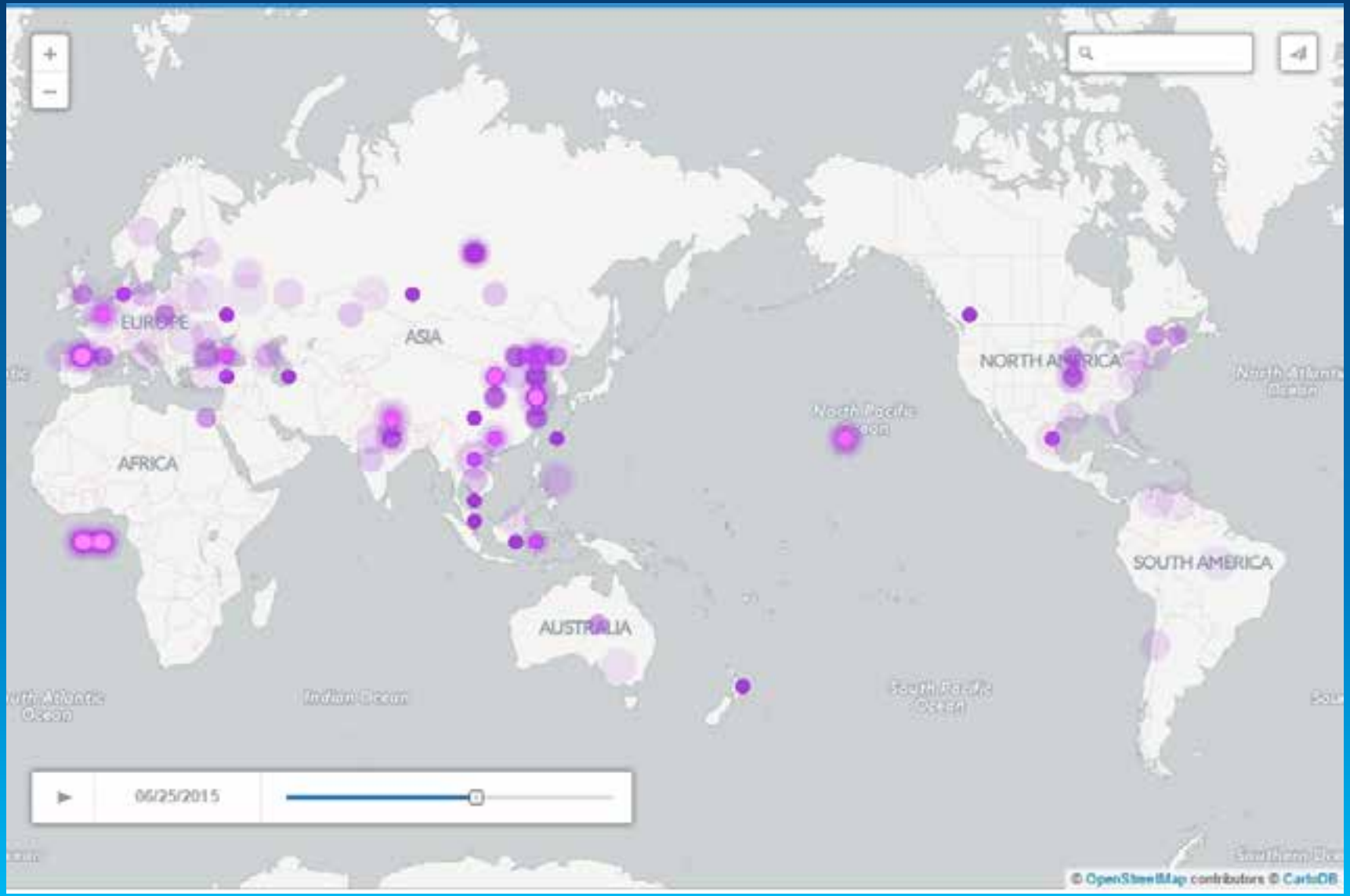
Results – Different Symbols

Single symbol

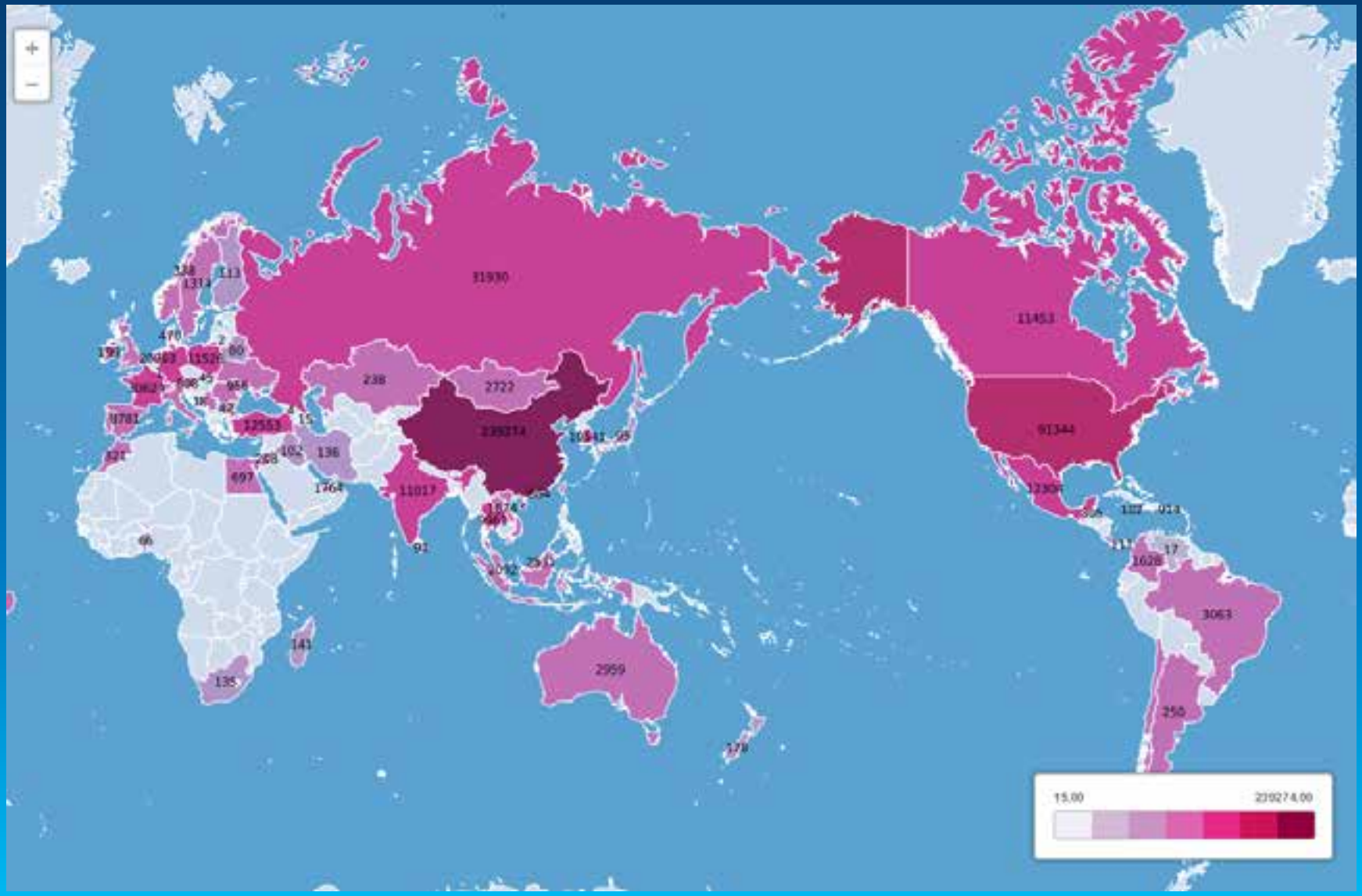
Number of occurrences

Severity Levels

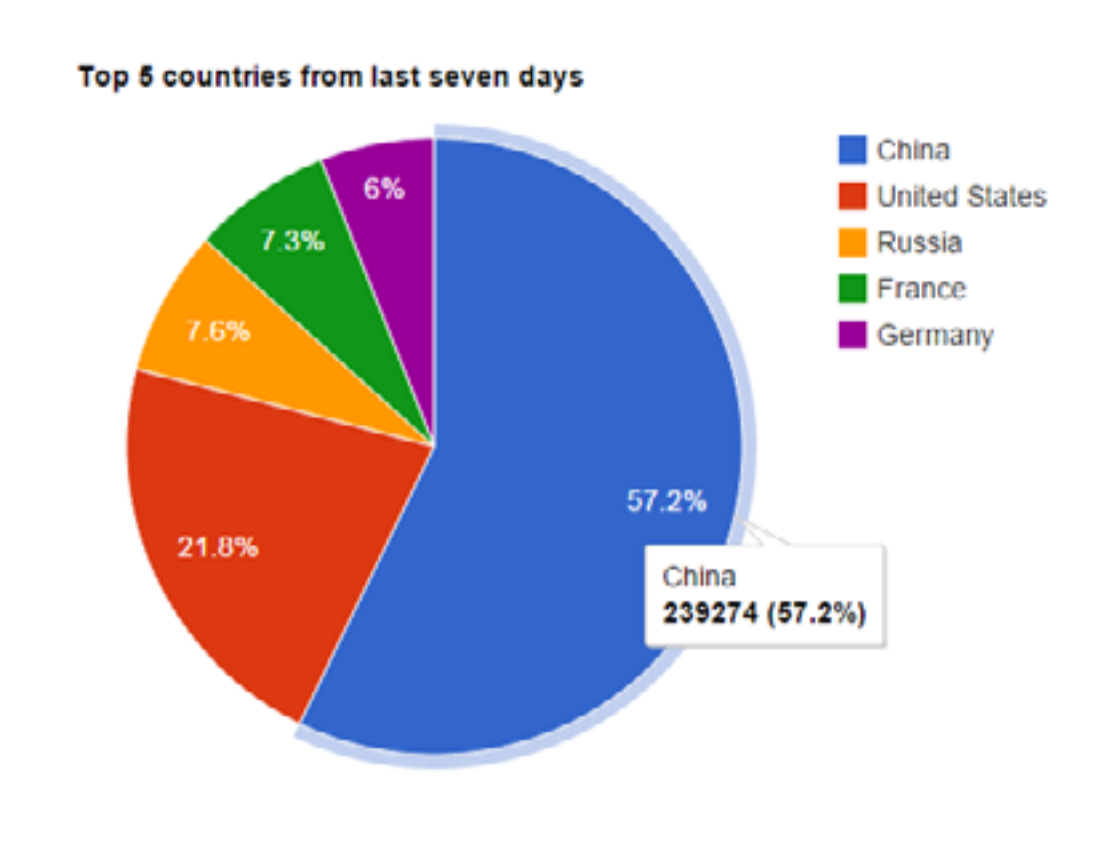
Results – Animated temporal map



Results – Country breakdowns, last 7 days



Results – Top 5 hits from last 7 days



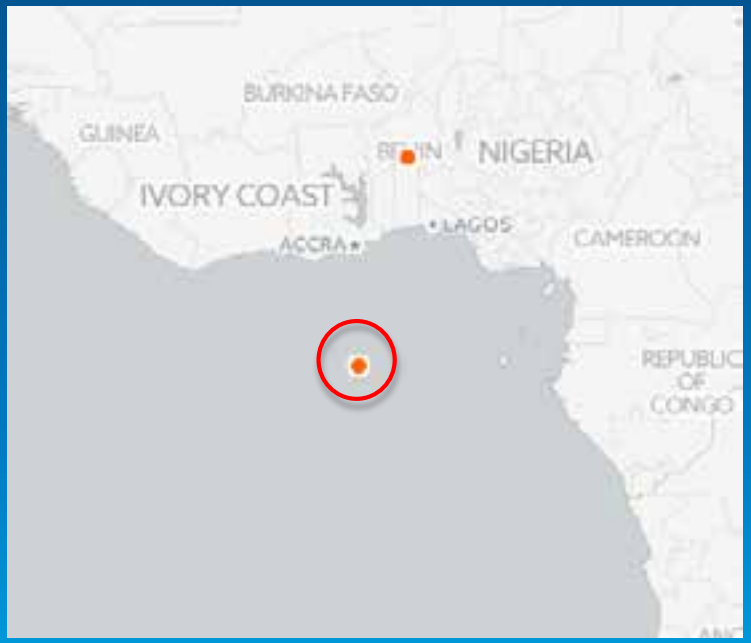
Conclusions

- ü Web-based GIS map application
- ü Live dynamic data
- ü Leverage cloud infrastructure
- ü Low-cost solution

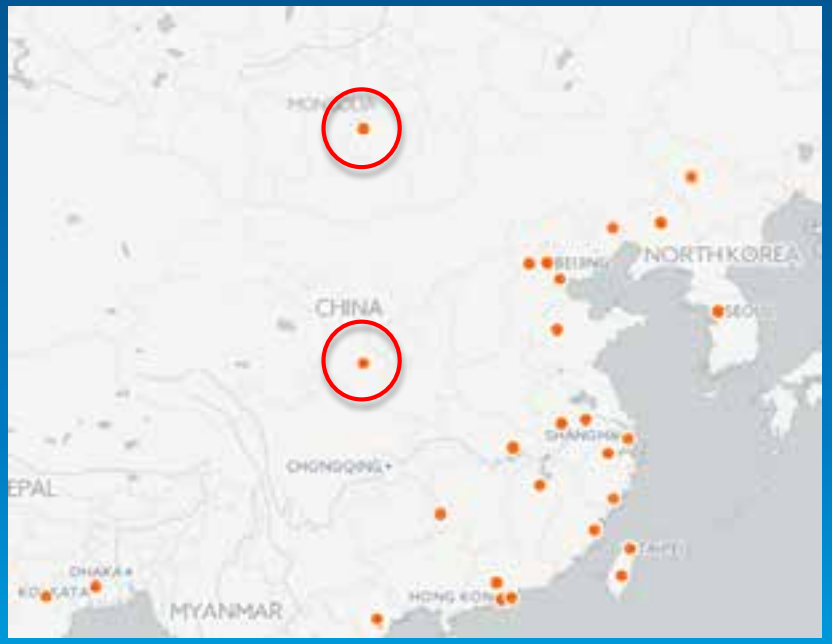
Issues and Improvements

Geolocation result accuracy

Zero accuracy



Country centroid



Issues and Improvements

IP Evasion Issue

- Web proxies, anonymizer software such as Tor

Improvements

- Add more filters
- Handle multiple firewalls

Questions

Juliana Lo
Pacific Disaster Center
Email: jlo@pdc.org