



# *GIS Application in Firewall Security Log Visualization*

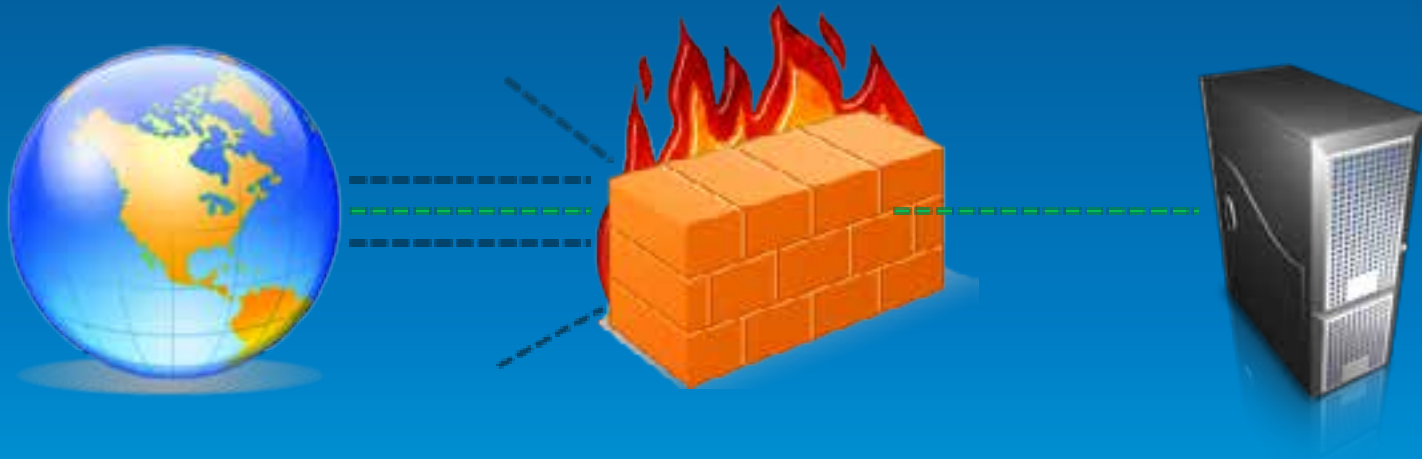
Juliana Lo

# Presentation Outline

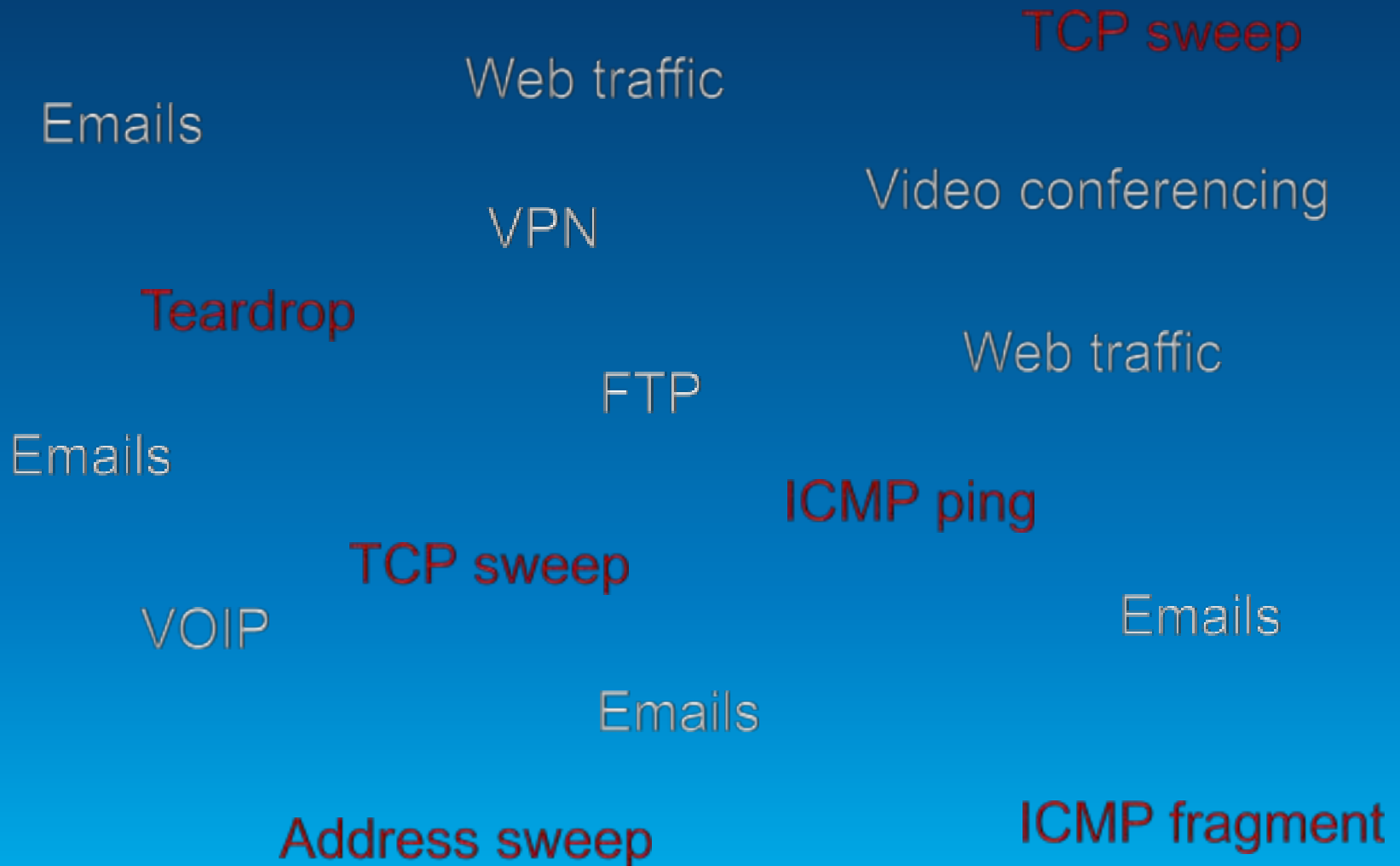
- ✓ What is a firewall
- ✓ Problem definition
- ✓ Project goal, objectives, constraints
- ✓ Framework and system components
- ✓ Solution
- ✓ Conclusions

# 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

The screenshot displays the Syslog Watcher application window. The main pane shows a list of received syslog messages with columns for Received, Severity, and Message. The messages are sorted by time, showing various alerts from a NetScreen device. A detailed view of a critical alert is shown in the bottom pane.

Received	Severity	Message
4/26/2015 11:14:50.398 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 138.118.219.105 to zone Untrust, proto TCP [int ethern...
4/26/2015 11:14:51.364 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 138.118.219.105 to zone Untrust, proto TCP [int ethern...
4/26/2015 11:14:52.305 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 138.118.219.105 to zone Untrust, proto TCP [int ethern...
4/26/2015 11:14:56.387 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 138.118.219.105 to zone Untrust, proto TCP [int ethern...
4/26/2015 11:18:46.101 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From [redacted] zone Trust, proto UDP [int ethernett...
4/26/2015 11:18:47.101 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From [redacted] zone Trust, proto UDP [int ethernett...
4/26/2015 11:18:48.101 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From [redacted] zone Trust, proto UDP [int ethernett...
4/26/2015 11:18:49.101 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From [redacted] zone Trust, proto UDP [int ethernett...
4/26/2015 11:31:43.360 AM	Critical	NetScreen device_id=009512010000717 [root]system-critical-00441: ICMP ping id=0! From 105.62.189.242 to [redacted] proto I Coar...
4/26/2015 11:32:06.309 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 133.108.21.56 to zone Untrust, proto TCP [int ethernett...
4/26/2015 11:37:58.324 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From 27.124.127.182 to zone Untrust, proto UDP [int ethernett...
4/26/2015 11:37:59.324 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From 27.124.127.182 to zone Untrust, proto UDP [int ethernett...
4/26/2015 11:38:00.324 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From 27.124.127.182 to zone Untrust, proto UDP [int ethernett...
4/26/2015 11:38:01.324 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From 27.124.127.182 to zone Untrust, proto UDP [int ethernett...
4/26/2015 11:38:02.324 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From 27.124.127.182 to zone Untrust, proto UDP [int ethernett...
4/26/2015 11:41:08.315 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 101.108.114.187 to zone Untrust, proto TCP [int ethernett...
4/26/2015 11:41:11.316 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 101.108.114.187 to zone Untrust, proto TCP [int ethernett...
4/26/2015 11:41:17.317 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00442: TCP sweep! From 101.108.114.187 to zone Untrust, proto TCP [int ethernett...
4/26/2015 11:41:19.318 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From [redacted] zone Trust, proto UDP [int ethernett...
4/26/2015 11:41:20.318 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From [redacted] zone Trust, proto UDP [int ethernett...
4/26/2015 11:42:24.312 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From 199.217.117.78 to zone Untrust, proto UDP [int ethernett...
4/26/2015 11:42:25.311 AM	Alert	NetScreen device_id=009512010000717 [root]system-alert-00443: UDP sweep! From 199.217.117.78 to zone Untrust, proto UDP [int ethernett...

**Message View**

Critical / Local 0 / Remote [redacted] Thursday, June 11, 2015 11:02:48.114 AM

NetScreen device\_id=009512010000717 [root]system-critical-00441: ICMP ping id=0! From 105.62.189.242 to [redacted] proto I (zone Untrust int ethernett0/2). Occurred 1 times. (2015-06-11 11:15:54)

For help, press F1. Service: Started (4.5.3) Tel: 82.872. Dns: 1.000. Pk: 0. Ssl: 0. LDP: 514. TCP: 1468. IPv4. IPv6. Ver: 4.5.3

# 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 C
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 C
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 C
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 C
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 C
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 C
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 C
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 C
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 C
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',%s',%s,%s

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

# Solution - Data Automation

## Step 5 – Database Table View

The screenshot displays the 'fhtable' interface in 'DATA VIEW' mode. The table contains the following data:

cartodb_id	lne_geom	alert	city	code	country	err	event_time	from_ip	latitude	longitude	occur
51452	118.7778, 32.0617	alert	Nanjing	442	China	TCP sweep	2015-05-22T22:31:06Z	222.186.21.145	32.0617	118.7778	822
51453	118.7778, 32.0617	alert	Nanjing	442	China	TCP sweep	2015-05-22T22:31:07Z	222.186.21.145	32.0617	118.7778	87
51454	130.0000, -27.0000	critical		441	Australia	ICMP ping id=0	2015-05-22T22:35:59Z	202.173.29.312	-27.0	130.0	1
51455	47.5000, 40.5000	critical		441	Azerbaijan	ICMP ping id=0	2015-05-22T22:36:33Z	46.32.171.26	40.5	47.5	1
51456	0.0000, 0.0000	alert		443		UDP sweep	2015-05-22T22:38:09Z	104.255.71.251	0.0	0.0	727
51457	-118.4143, 34.0995	critical	Beverly Hills	441	United States	ICMP ping id=0	2015-05-22T22:44:13Z	216.178.46.224	34.0995	-118.4143	1
51458	-118.4143, 34.0995	critical	Beverly Hills	441	United States	ICMP ping id=0	2015-05-22T23:00:22Z	216.178.46.224	34.0995	-118.4143	1
51459	-118.4143, 34.0995	critical	Beverly Hills	441	United States	ICMP ping id=0	2015-05-22T23:00:48Z	216.178.46.224	34.0995	-118.4143	1
51460	8.0000, 47.0000	critical		441	Europe	ICMP ping id=0	2015-05-22T23:12:56Z	185.31.19.193	47.0	8.0	1
51461	8.0000, 47.0000	critical		441	Europe	ICMP ping id=0	2015-05-22T23:13:00Z	185.31.19.193	47.0	8.0	1
51462	8.0000, 47.0000	critical		441	Europe	ICMP ping id=0	2015-05-22T23:13:00Z	185.31.19.193	47.0	8.0	1
51463	8.0000, 47.0000	critical		441	Europe	ICMP ping id=0	2015-05-22T23:13:04Z	185.31.19.193	47.0	8.0	1

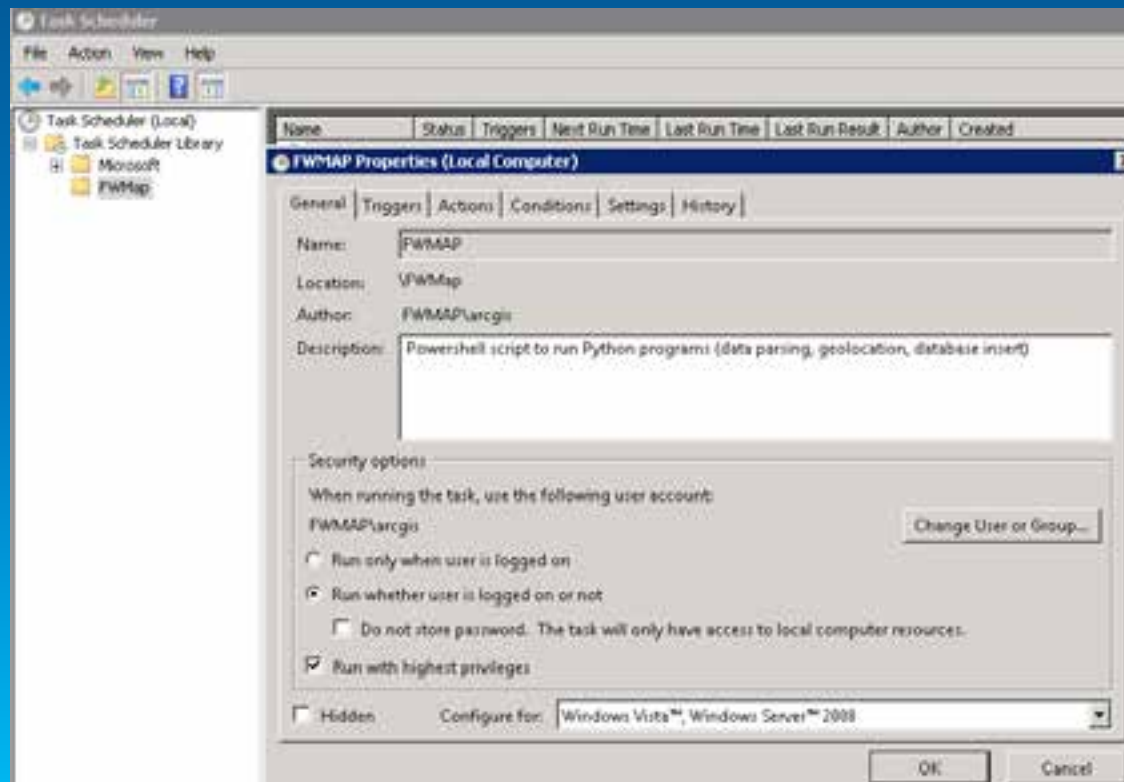


# Solution - Data Automation

## Step 6 – Automated Updates

Use Windows'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

Map Window

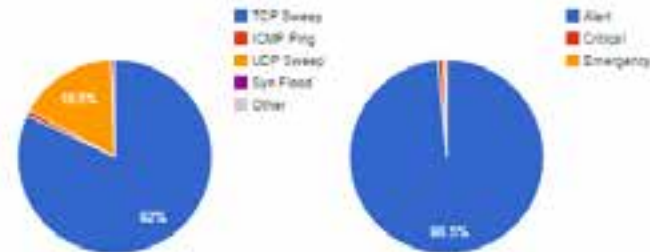
Layers/Symbols Selectors



Dashboard

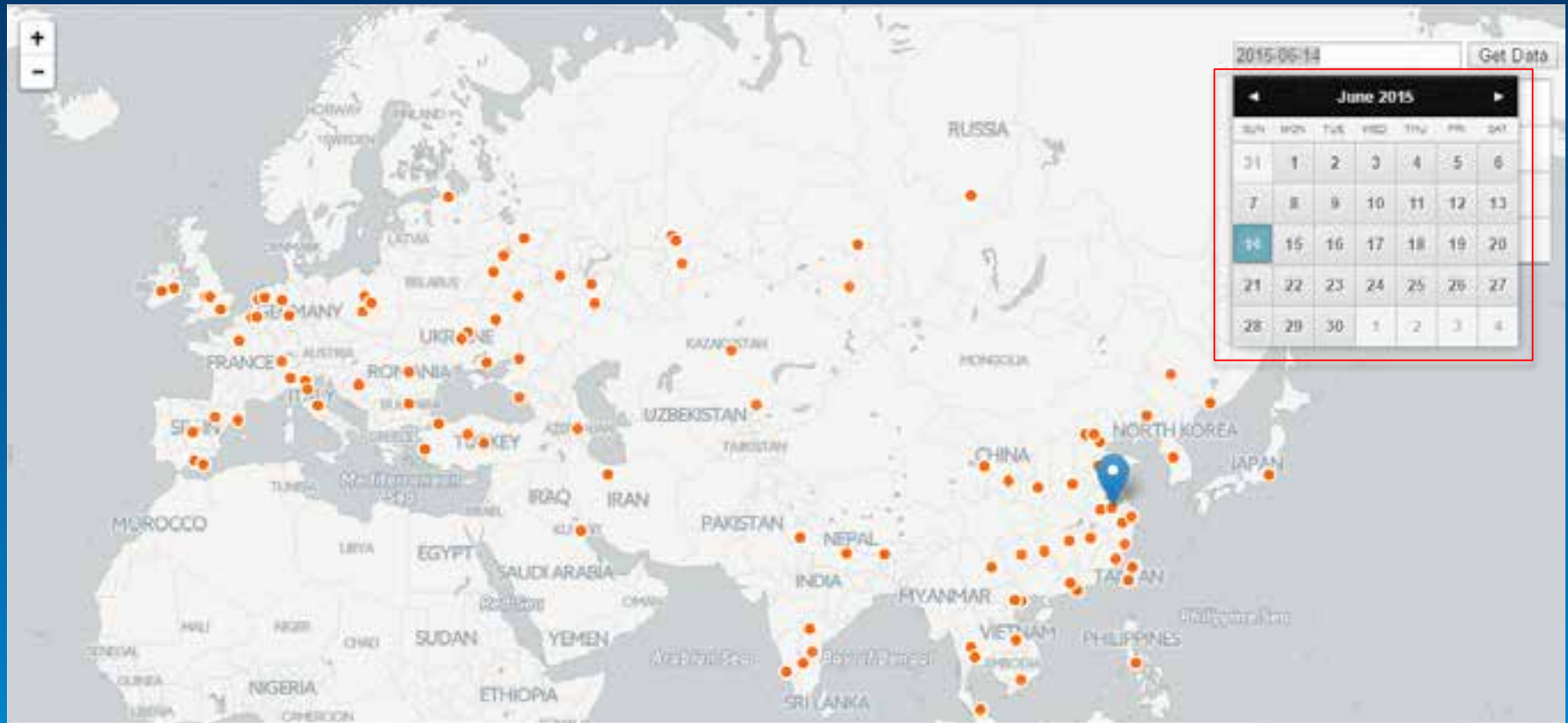
IP Addr	Level	Error	Location	Time	Occur
222.186.21.108	alert	TCP sweep	Nanjing,China	2015-07-02T20:02:32Z	929
222.186.3.171	alert	TCP sweep	Nanjing,China	2015-07-02T18:17:35Z	936
222.187.226.206	alert	TCP sweep	Nanjing,China	2015-07-02T15:31:39Z	380
222.186.21.168	alert	TCP sweep	Nanjing,China	2015-07-02T15:00:18Z	65
222.186.21.168	alert	TCP sweep	Nanjing,China	2015-07-02T15:00:17Z	845
222.186.21.168	alert	TCP sweep	Nanjing,China	2015-07-02T15:00:14Z	789
222.186.21.168	alert	TCP sweep	Nanjing,China	2015-07-02T15:00:14Z	124
222.187.227.130	alert	TCP sweep	Nanjing,China	2015-07-02T14:58:55Z	361

Reporting period: Between hours 12-24 Total no of hits (all locations): 46203



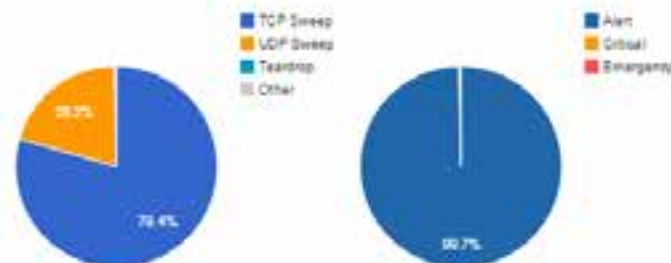
Top IP		Top Locations	
IP Address	City	Hits	
222.186.21.168	Nanjing	1823	🔍
222.186.30.170	Nanjing	1577	🔍
121.163.45.126		1275	🔍
195.60.131.62		1180	🔍
167.114.210.233	Mcallen	964	🔍
43.225.57.215		964	🔍
113.108.21.18	Guangzhou	964	🔍

# Results – Select a date



IP Addr	Level	Error	Location	Time	Hits
61.147.103.96	alert	TCP sweep	Nanjing,China	2015-06-14T00:01:38Z	956
61.147.103.96	alert	TCP sweep	Nanjing,China	2015-06-14T00:01:39Z	3
61.160.213.216	alert	TCP sweep	Nanjing,China	2015-06-14T00:08:32Z	306
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-14T01:36:03Z	342
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-14T01:36:07Z	426
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-14T01:36:13Z	414
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-14T01:36:29Z	588

Reporting Date: 2015-06-14 Total no of hits (all locations): 125526



IP Address	City	Hits
61.147.103.96	Nanjing	8125
222.186.21.202	Nanjing	4660
46.7.174.192	Taijiaht	2678
187.23.8.47	Franca	2651
5.99.172.18		2637
60.12.99.164	Hangzhou	2622

# Results – Clickable Features

Click on a feature in the map to show details

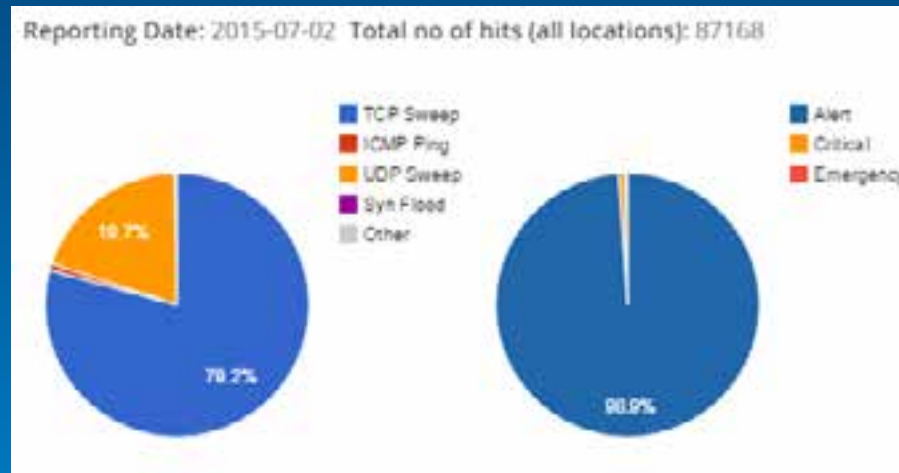
IP Addr	Level	Error	Location	Time	Occur
222.186.31.178	alert	TCP sweep	Nanjing,China	2015-06-27T20:32:19Z	85
222.186.31.178	alert	TCP sweep	Nanjing,China	2015-06-27T20:32:19Z	787
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-27T20:26:08Z	556
222.186.21.202	alert	TCP sweep	Nanjing,China	2015-06-27T20:25:33Z	542
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	2015-06-27T15:39:38Z	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

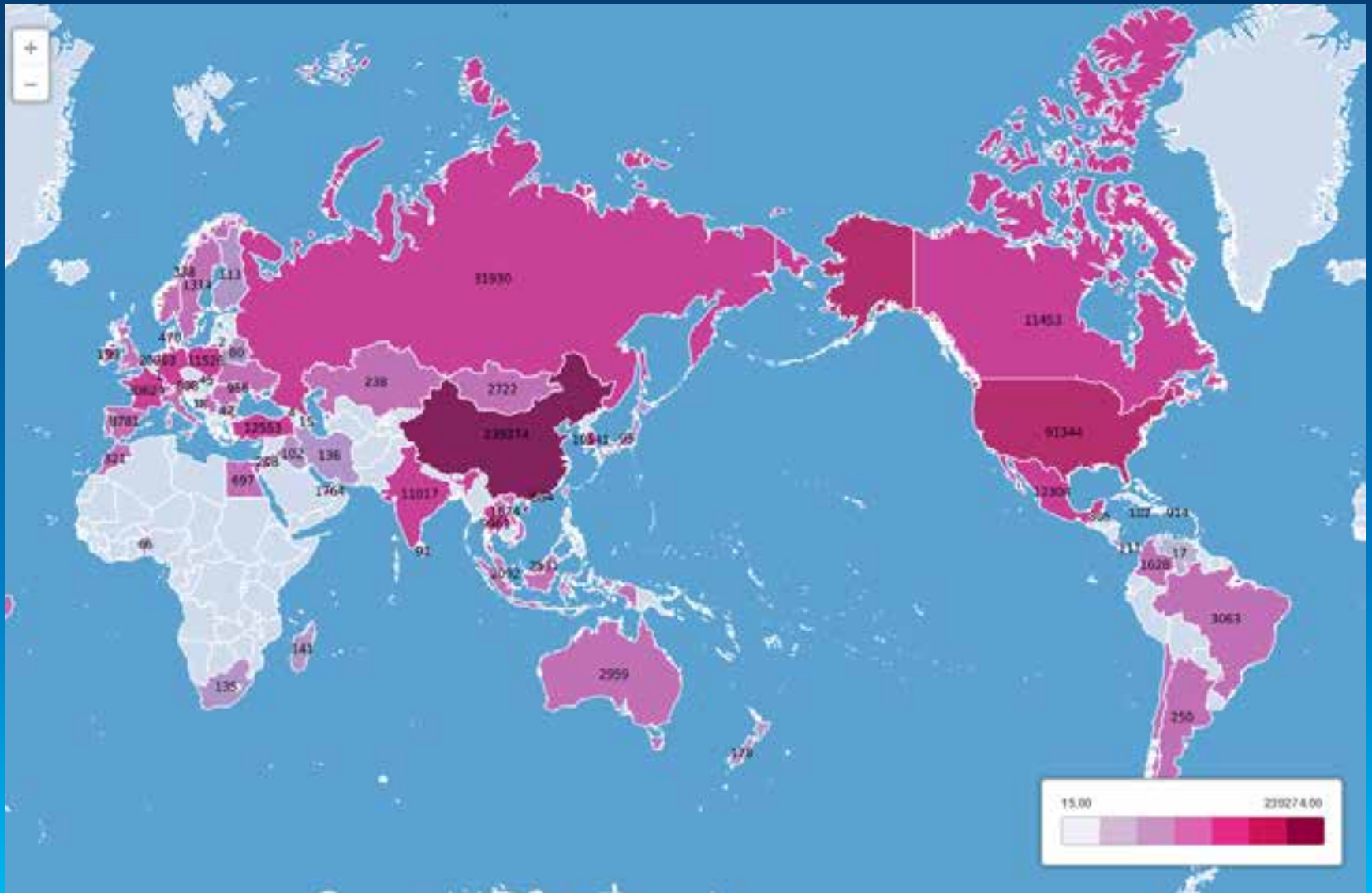


# Results – Animated temporal map

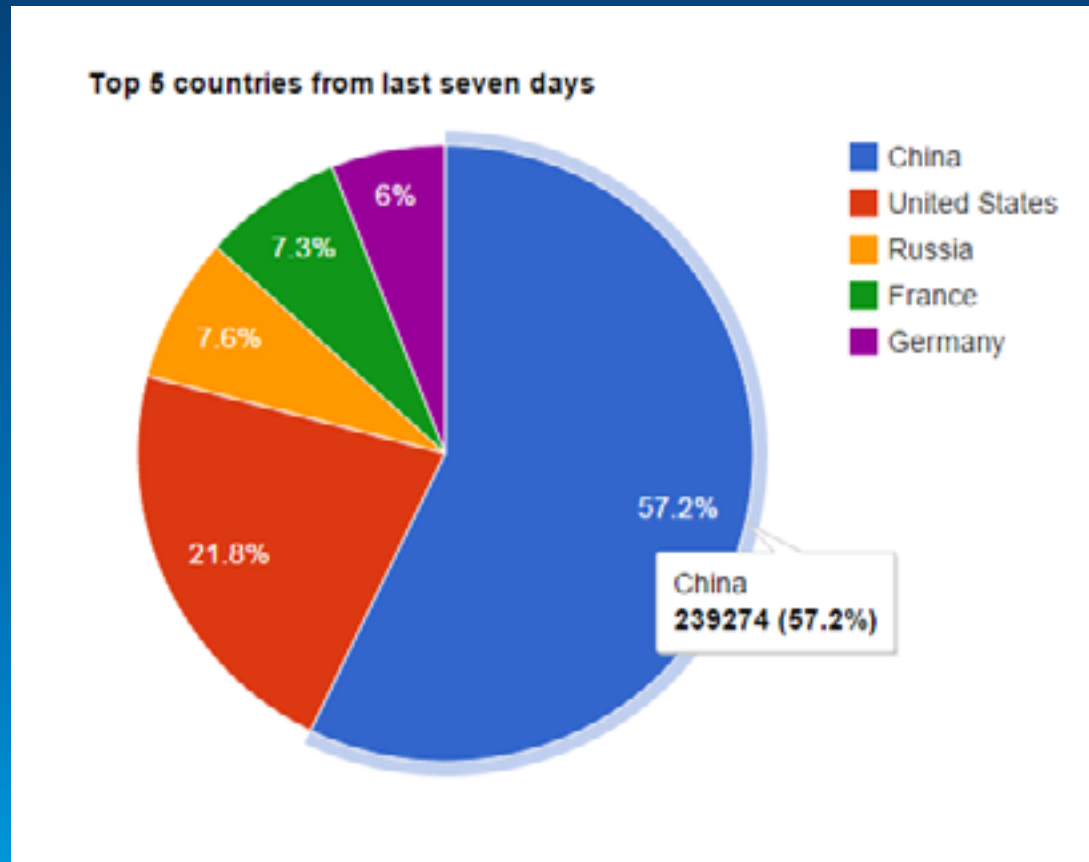




# Results – Country breakdowns, last 7 days



# Results – Top 5 hits from last 7 days



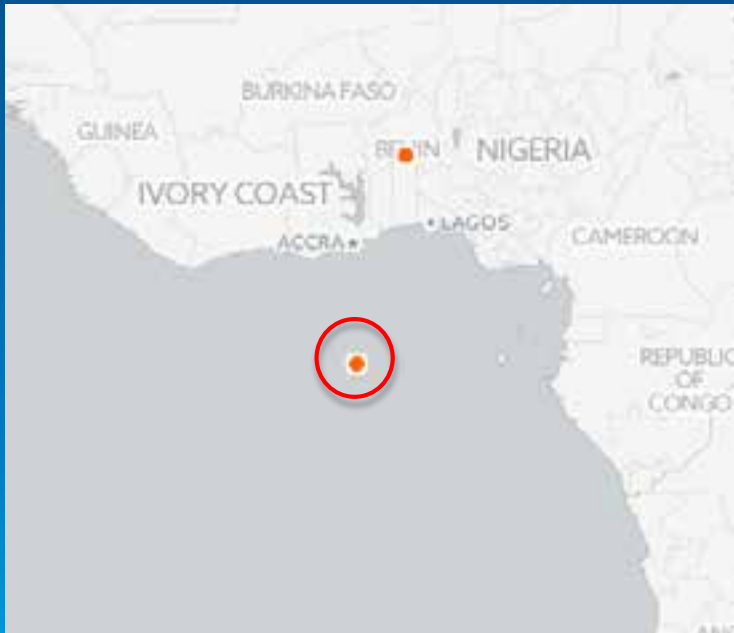
# Conclusions

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

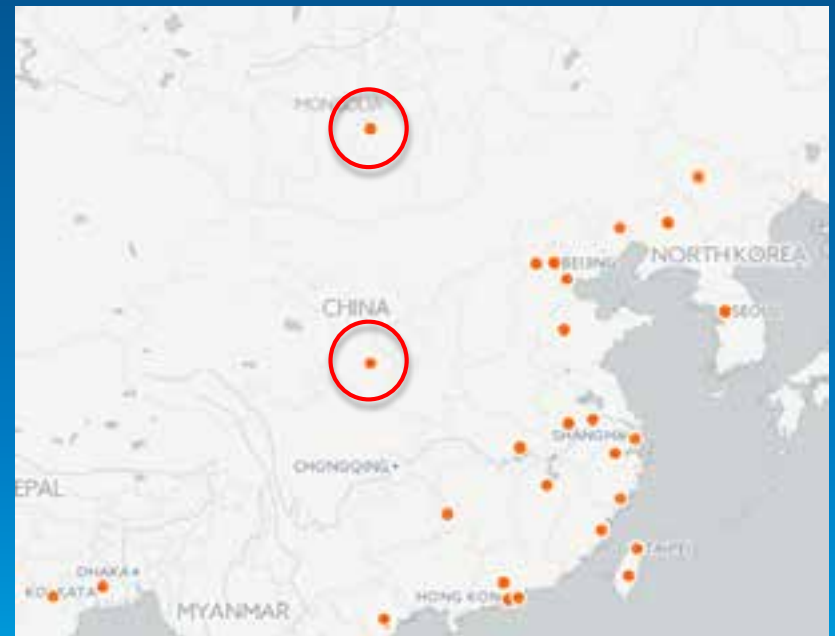
# Issues and Improvements

## 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](mailto:jlo@pdc.org)