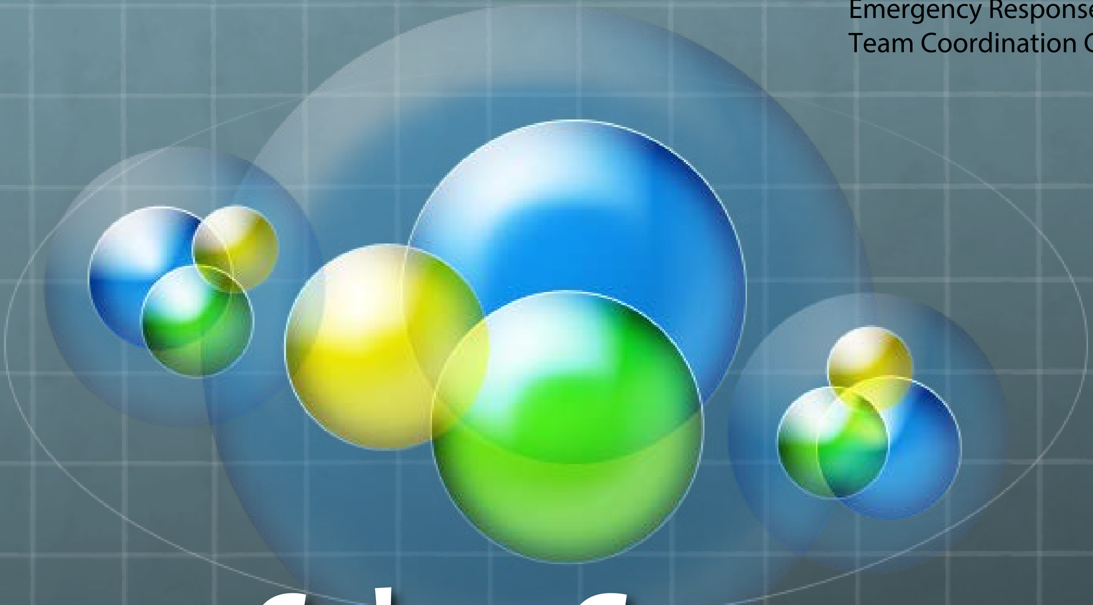


Cyber Green
Improving Cyber Health through Measurement and Mitigation

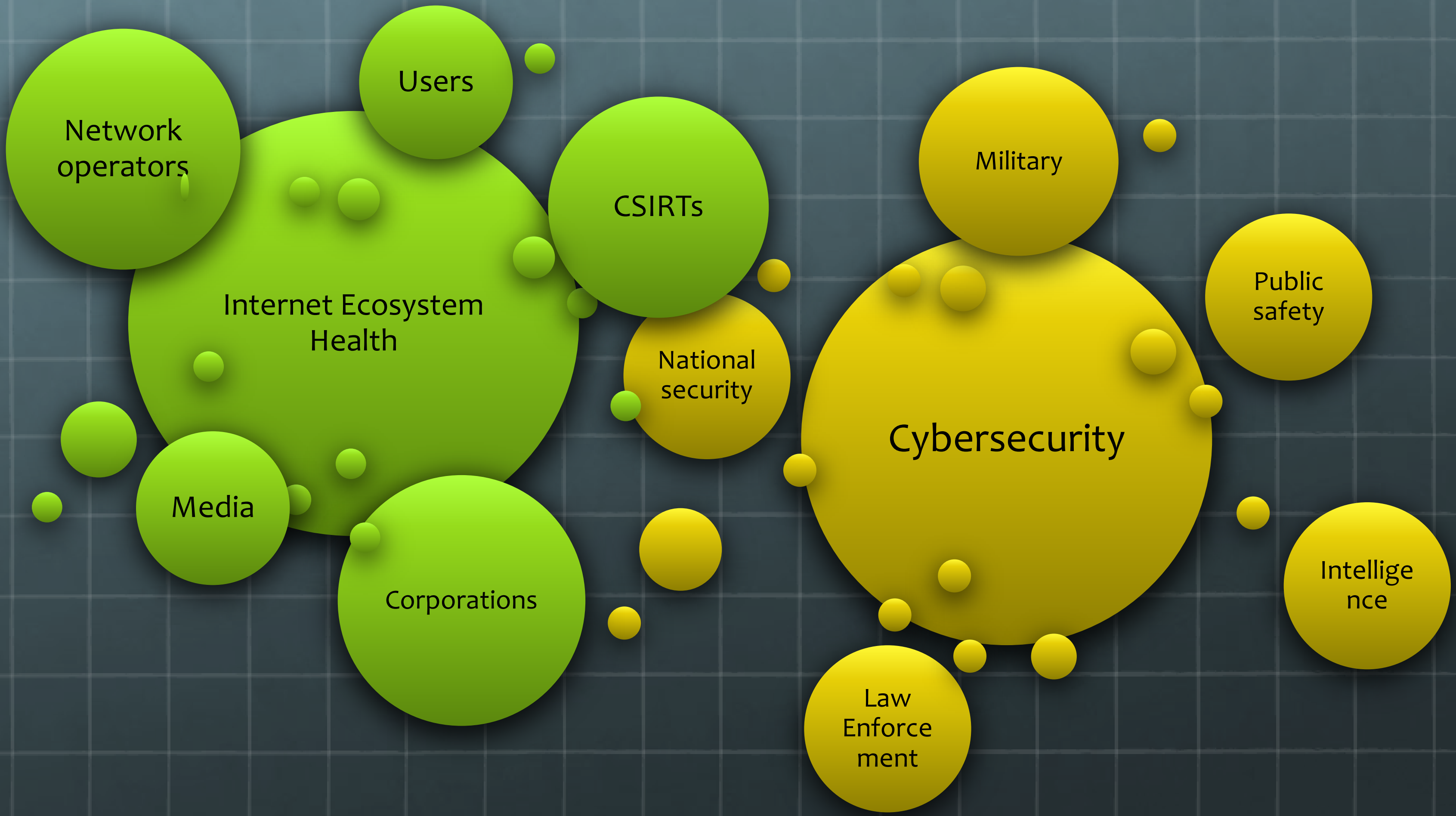
Yurie Ito
Director, JPCERT/CC

Context for the Cyber Green Initiative

- Increasing dominance of cyber underpining communications, business, utilities
- Cyber risks continue to increase across the ecosystem
- Growing focus on attribution-based response undermines the international collaboration among CSIRTs
- Measurement of risks is fundamental to improving the ecosystem to motivate and get actionable information to those who can act
  - This will require increased efficiency of data sharing
- Transparency into the sources and presence of cyber risk is necessary to improve the ecosystem

Cybersecurity landscape

- Lots of attention to attribution
- Need more focus on ecosystem health and improvement



CSIRT service

- Reactive
  - Incident Response
  - Coordination

- Proactive
  - Prevention
    - Indicator sharing
  - Improvement
    - Clean-ups
    - Vulnerability handling/ coordination

Cyber GREEN

Question: Would you build your national critical systems and cybersecurity measures on;

A: an infected global internet ecosystem which is vulnerable, carrying high malicious traffic

B: a clean global internet ecosystem which is resilient with little malicious traffic

Defining Cyber Health

- "Cyber Health" is defined as, **"a condition of cyber systems and networks that are not only free from infection from malware and botnets but also contributes more broadly to the overall trust and usability of the cyberspace for the well-being of all."**

- Cyber health is defined as "a cyber ecosystem that provides trust and usability for all by limiting malware infection, system vulnerability and transiting of malicious traffic."

Yurie Ito, "Managing Global Cyber Health and Security through Risk Reduction." July 18, 2011.

Applying Root-Cause Analysis to Internet Health

Disease	Vector	Root Cause
Malaria	Mosquito	Swamps (mosquito breeding grounds)
DDoS	Amplified network connections	Misconfigured servers
		Lack of access control lists at the application layer
		Source IP spoofing
	Botnet generated traffic	Lack of patches hosts
		Misconfigured servers
		No AV on endpoints

Overarching Goal

- Establishment of an increasingly effective hub for collaboration efforts to address cyber risk and improve the health of the cyber ecosystem.
- Estimation of Internet health, improvement
- Build a system to fuse data sources together for indicator development
- Continuous reporting, distribute to stakeholders

The Cyber Green Mission

Mission:

- **The Cyber Green project will** improve cyber health by enhancing collaboration between key stakeholders in cyberspace

How will Cyber Green Accomplish its Mission:

- Cyber Green established a reliable platform for generating cross-comparable statistics & information sharing mechanisms to enable operational cyber remediation efforts and provide insight into systemic risk conditions in the cyber ecosystem.

Key Internet Health Risk Indicators

- **Number of known, compromised hosts**
  - Botnet infections
  - Host being used for phishing … etc
- **Number of known, vulnerable hosts**
  - Specific vulnerabilities client side / Server side
  - Open NTP, recursive resolvers, … . etc
- **Number of know, "unsolicited" hosts**
  - Spam, DDoS, attack, scanners … .etc
  - Realized events, wasted capacity

Goal is to drive these values to 0

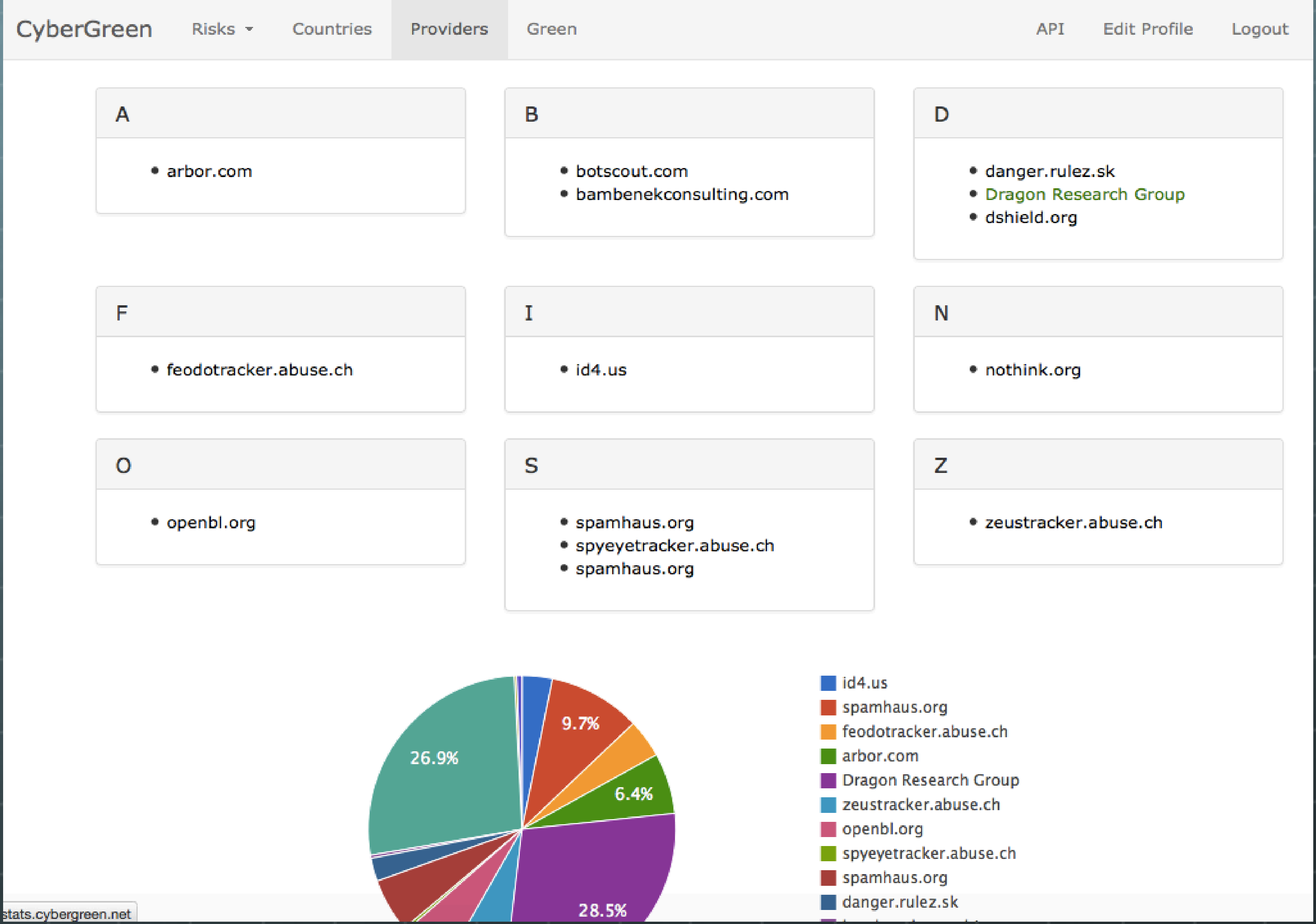
Counting Strategy

- By unique IP seen in a 24 hour window
  - Common across many data sources
  - Understand limitations in this approach
- Look for trend lines

Data Sources

- We will collaborate with partners to gather risk condition data
- We seek reliable, high confidence, global data sources
- Import regularly (daily, etc) measurement into the Cyber Green system
- Accept partner redistribution restrictions
- Free of any fees

Providers



A

- arbor.com

B

- botscout.com
- bambenekconsulting.com

D

- danger.rulez.sk
- Dragon Research Group
- dshield.org

F

- feodotracker.abuse.ch

I

- id4.us

N

- nothink.org

O

- openbl.org

S

- spamhaus.org
- spyeyetracker.abuse.ch
- spamhaus.org

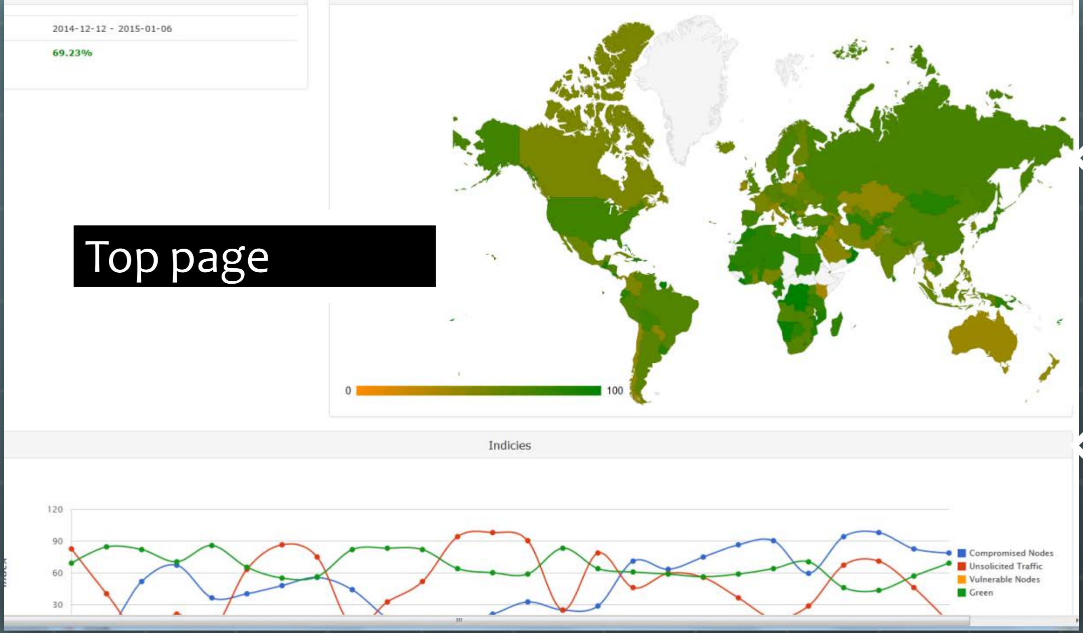
Z

- zeustracker.abuse.ch

Data Normalization

- Permits comparison across time
- Permits comparison across space
- By IP address (IPv4, IPv6) – ARIN, etc
- By population – global sources
- By Internet-connected population – OECD
- By Internet subscriptions – ITU
- By website count – internal data
- By Internet connected device – *unknown*

Cyber Green will make available high-confidence, cross-comparable, and actionable information to stakeholders.



2014-12-12 - 2015-01-06

69.23%

Top page

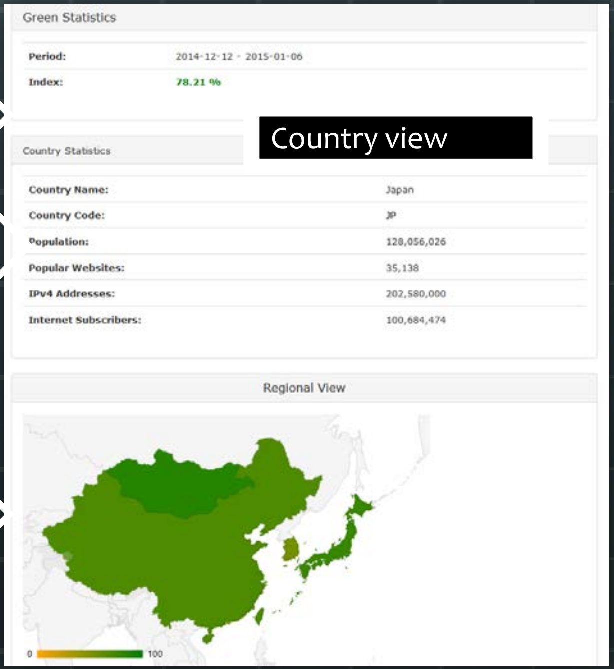
Today's Cyber Health index global view

3 risk indicators volatility:
- Vulnerable nodes
- Infection
- Unsolicited traffic

Health index

Country data (Normalization data)
- Population, GDP, IP addresses….
etc

Raw data and metrics of each risk indicators



Green Statistics

Period:	2014-12-12 - 2015-01-06
Index:	78.21 %

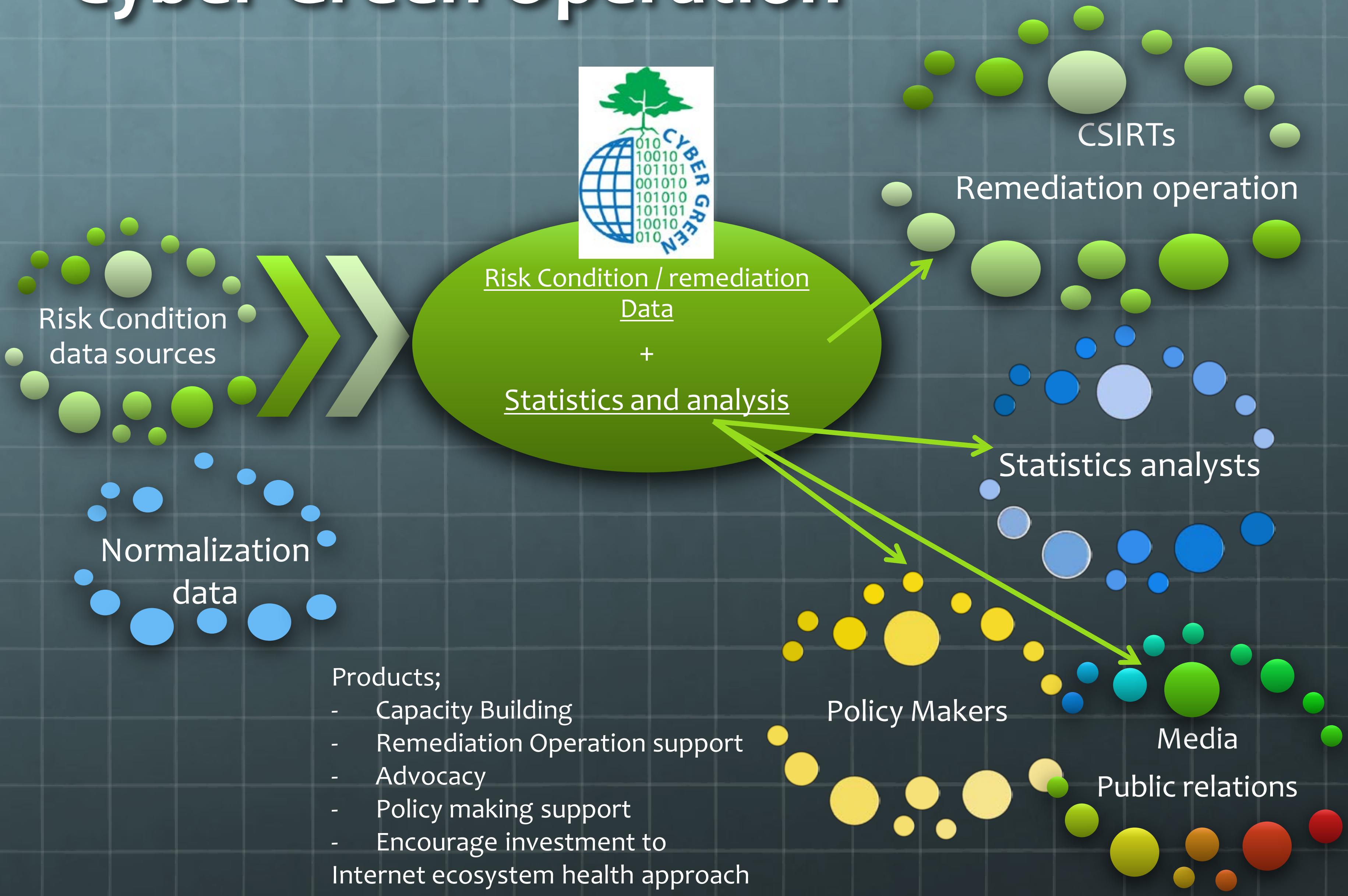
Country view

Country Statistics

Country Name:	Japan
Country Code:	JP
Population:	128,056,026
Popular Websites:	35,138
IPv4 Addresses:	202,580,000
Internet Subscribers:	100,684,474

Regional View

Cyber Green Operation



Risk Condition data sources

Normalization data

Risk Condition / remediation Data

+

Statistics and analysis

CSIRTs

Remediation operation

Statistics analysts

Policy Makers

Media

Public relations

Products;

- Capacity Building
- Remediation Operation support
- Advocacy
- Policy making support
- Encourage investment to

Internet ecosystem health approach

What is the Portal?

- Ruby on Rails application, hosted by Amazon Elastic Beanstalk
  - https://stats.cybergreen.net

- Built as an application using the "CIF" platform
  - http://csritgadgets.org/collective-intelligence-framework/

What is “CIF”

- Collective intelligence Framework
- A cyber threat intelligence management system
- Combines known malicious threat information from many sources
- Enables CSIRTs to use that information for identification, detection and mitigation
- The most common types of threat intelligence warehoused in CIF are IP addresses, domains and urls

CIF Base Applications

- CIF provides a standardized REST + JSON interface into an ElasticSearch backend containing normalized risk condition data
- CIF takes care of the parsing and normalizing, so applications such as CyberGreen can make use of the data

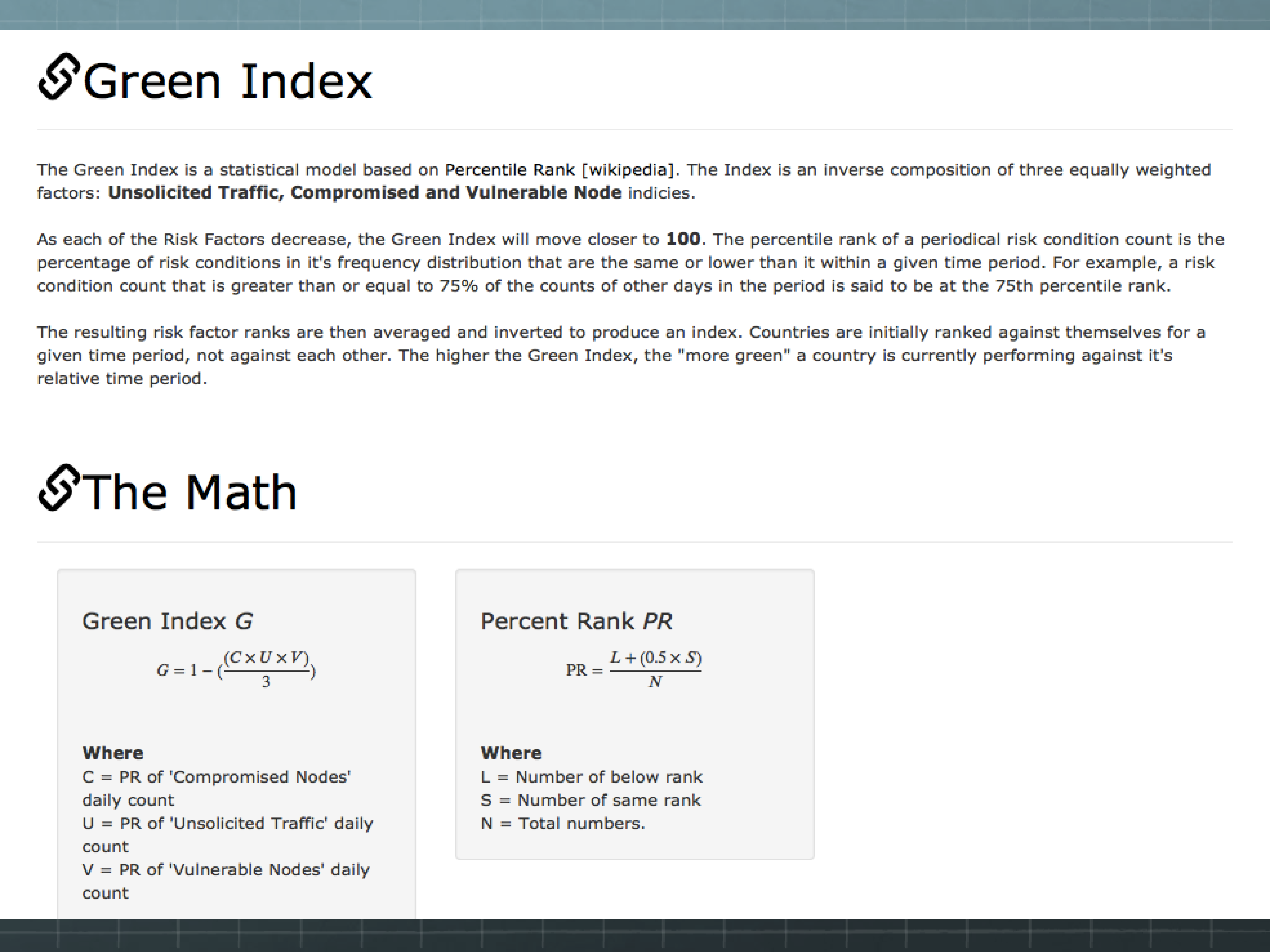
Cyber Green Portal

- Ruby on Rails engine
- Independent of CIF
- Pulls its data from the CIF API, normalizes it into its own data warehouse
- Provides API layer (with python SDK) for applications to build upon its data

Green Index

- A normalization “per day” view of a country’s;

  - Number of known, vulnerable hosts
  - Number of know, compromised hosts
  - Number of known unsolicited traffic hosts



Green Index

The Green Index is a statistical model based on Percentile Rank [wikipedia]. The Index is an inverse composition of three equally weighted factors: **Unsolicited Traffic, Compromised and Vulnerable Node** indicies.

As each of the Risk Factors decrease, the Green Index will move closer to **100**. The percentile rank of a periodical risk condition count is the percentage of risk conditions in it's frequency distribution that are the same or lower than it within a given time period. For example, a risk condition count that is greater than or equal to 75% of the counts of other days in the period is said to be at the 75th percentile rank.

The resulting risk factor ranks are then averaged and inverted to produce an index. Countries are initially ranked against themselves for a given time period, not against each other. The higher the Green Index, the "more green" a country is currently performing against it's relative time period.

The Math

Green Index *G*

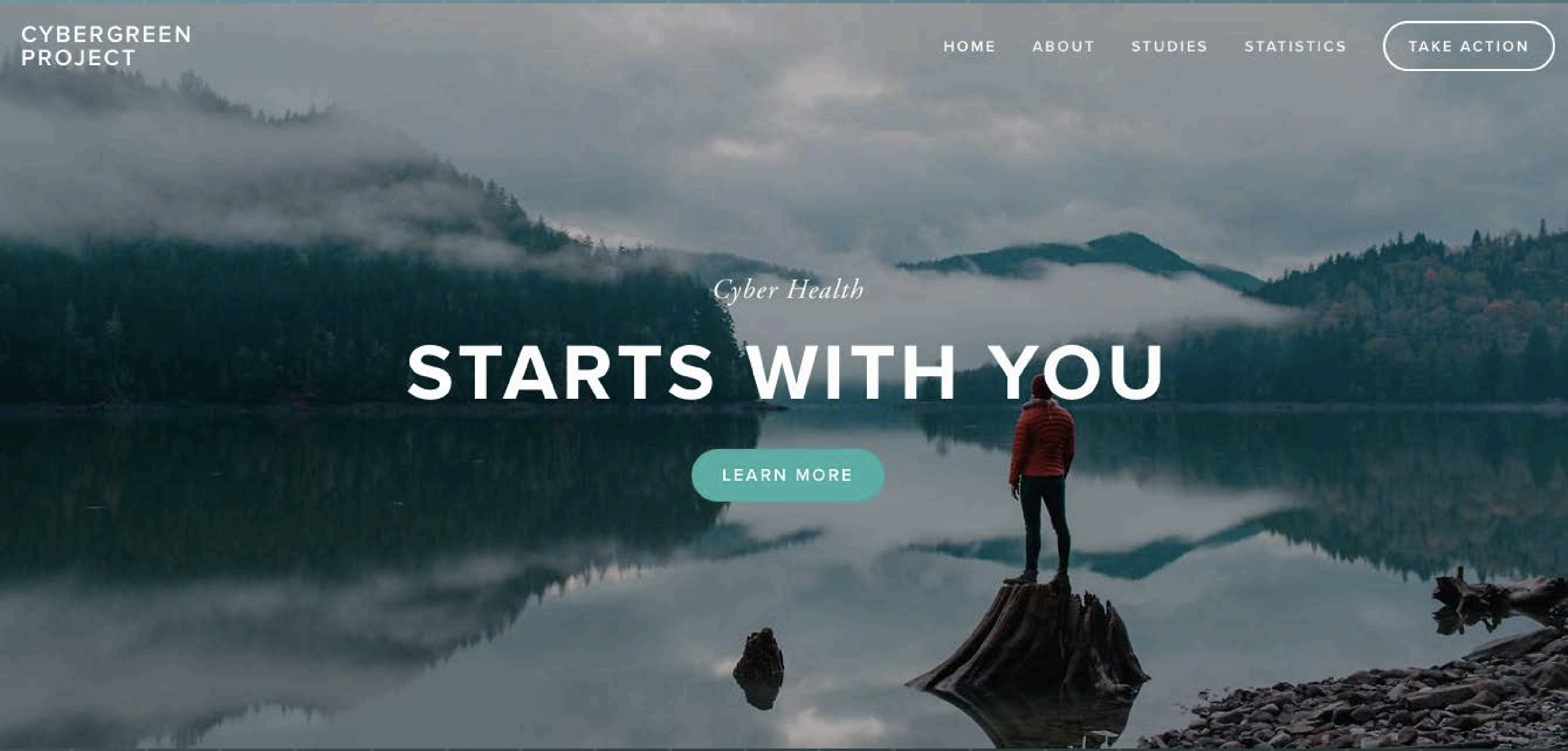
$$G = 1 - (\frac{(C \times U \times V)}{3})$$

Where
C = PR of 'Compromised Nodes' daily count
U = PR of 'Unsolicited Traffic' daily count
V = PR of 'Vulnerable Nodes' daily count

Percent Rank *PR*

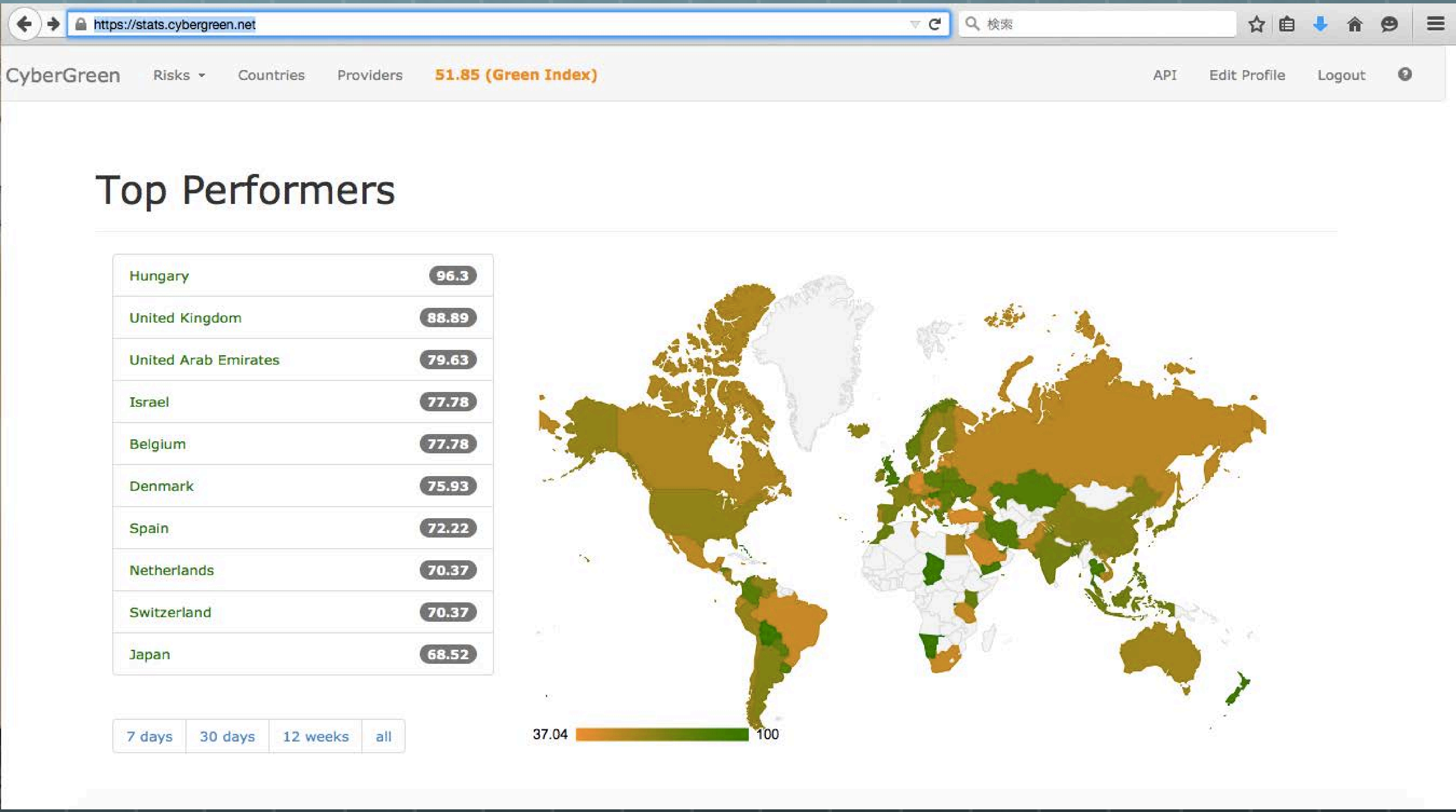
$$\mathrm{PR} = \frac{L + (0.5 \times S)}{N}$$

Where
L = Number of below rank
S = Number of same rank
N = Total numbers.



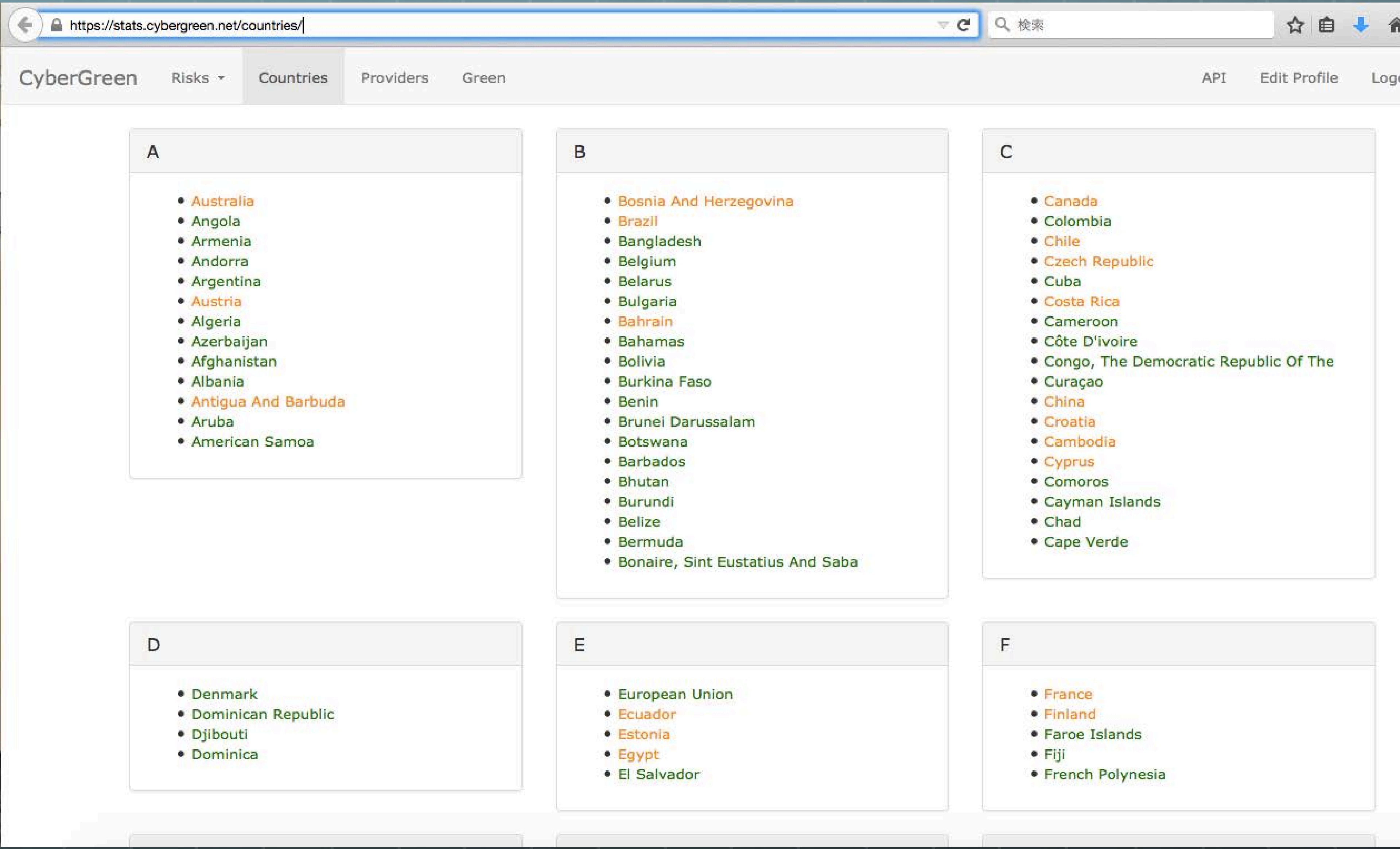
Cyber Health

STARTS WITH YOU



Top Performers

Hungary	96.3
United Kingdom	88.89
United Arab Emirates	79.63
Israel	77.78
Belgium	77.78
Denmark	75.93
Spain	72.22
Netherlands	70.37
Switzerland	70.37
Japan	68.52



A

- Australia
- Angola
- Armenia
- Andorra
- Argentina
- Austria
- Algeria
- Azerbaijan
- Afghanistan
- Albania
- Antigua And Barbuda
- Aruba
- American Samoa

B

- Bosnia And Herzegovina
- Brazil
- Bangladesh
- Belgium
- Belarus
- Bulgaria
- Bahrain
- Bahamas
- Bolivia
- Burkina Faso
- Benin
- Brunei Darussalam
- Botswana
- Barbados
- Bhutan
- Burundi
- Belize
- Bermuda
- Bonaire, Sint Eustatius And Saba

C

- Canada
- Colombia
- Chile
- Czech Republic
- Cuba
- Costa Rica
- Cameroon
- Côte D'ivoire
- Congo, The Democratic Republic Of The
- Curaçao
- China
- Croatia
- Cambodia
- Cyprus
- Comoros
- Cayman Islands
- Chad
- Cape Verde

D

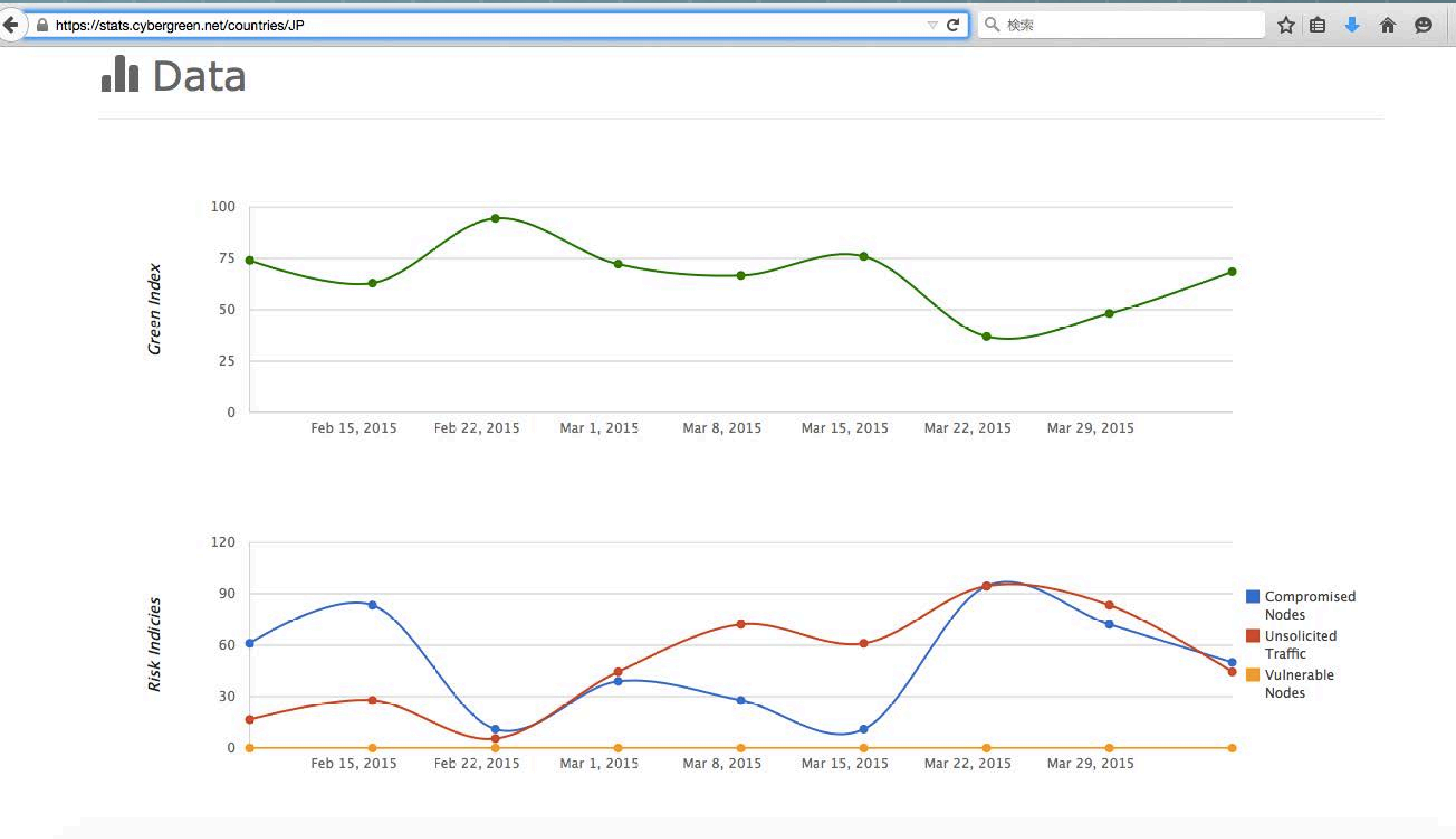
- Denmark
- Dominican Republic
- Djibouti
- Dominica

E

- European Union
- Ecuador
- Estonia
- Egypt
- El Salvador

F

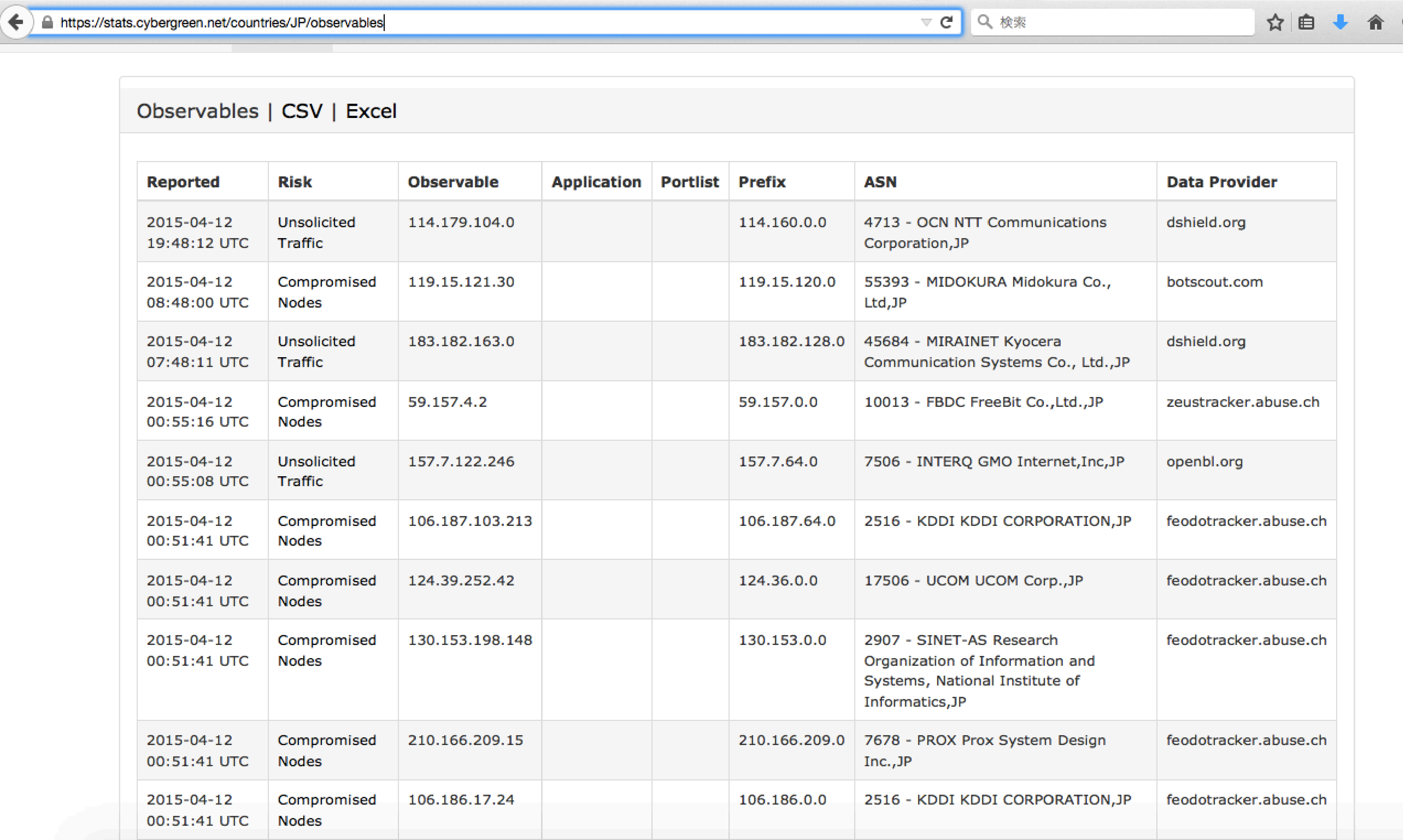
- France
- Finland
- Faroe Islands
- Fiji
- French Polynesia



https://stats.cybergreen.net/countries/JP
検索

Data

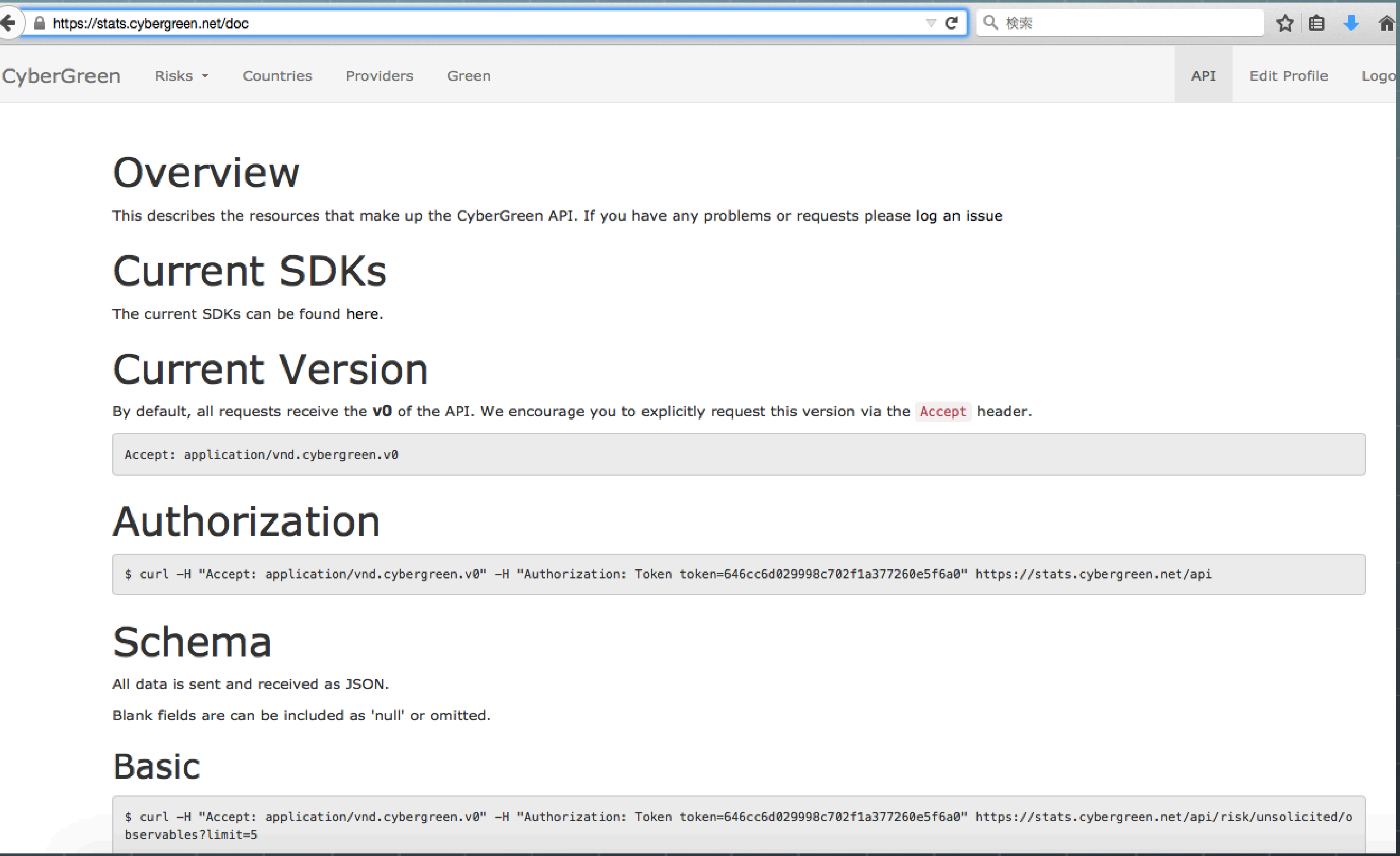
Green Index
100
75
50
25
0
Feb 15, 2015
Feb 22, 2015
Mar 1, 2015
Mar 8, 2015
Mar 15, 2015
Mar 22, 2015
Mar 29, 2015
Risk Indicies
120
90
60
30
0
Feb 15, 2015
Feb 22, 2015
Mar 1, 2015
Mar 8, 2015
Mar 15, 2015
Mar 22, 2015
Mar 29, 2015
🟦 Compromised Nodes
🟥 Unsolicited Traffic
🟧 Vulnerable Nodes



https://stats.cybergreen.net/countries/JP/observables

Observables | CSV | Excel

Reported	Risk	Observable	Application	Portlist	Prefix	ASN	Data Provider
2015-04-12 19:48:12 UTC	Unsolicited Traffic	114.179.104.0			114.160.0.0	4713 - OCN NTT Communications Corporation,JP	dshield.org
2015-04-12 08:48:00 UTC	Compromised Nodes	119.15.121.30			119.15.120.0	55393 - MIDOKURA Midokura Co., Ltd,JP	botscout.com
2015-04-12 07:48:11 UTC	Unsolicited Traffic	183.182.163.0			183.182.128.0	45684 - MIRAINET Kyocera Communication Systems Co., Ltd.,JP	dshield.org
2015-04-12 00:55:16 UTC	Compromised Nodes	59.157.4.2			59.157.0.0	10013 - FBDC FreeBit Co.,Ltd.,JP	zeustracker.abuse.ch
2015-04-12 00:55:08 UTC	Unsolicited Traffic	157.7.122.246			157.7.64.0	7506 - INTERQ GMO Internet,Inc,JP	openbl.org
2015-04-12 00:51:41 UTC	Compromised Nodes	106.187.103.213			106.187.64.0	2516 - KDDI KDDI CORPORATION,JP	feodotracker.abuse.ch
2015-04-12 00:51:41 UTC	Compromised Nodes	124.39.252.42			124.36.0.0	17506 - UCOM UCOM Corp.,JP	feodotracker.abuse.ch
2015-04-12 00:51:41 UTC	Compromised Nodes	130.153.198.148			130.153.0.0	2907 - SINET-AS Research Organization of Information and Systems, National Institute of Informatics,JP	feodotracker.abuse.ch
2015-04-12 00:51:41 UTC	Compromised Nodes	210.166.209.15			210.166.209.0	7678 - PROX Prox System Design Inc.,JP	feodotracker.abuse.ch
2015-04-12 00:51:41 UTC	Compromised Nodes	106.186.17.24			106.186.0.0	2516 - KDDI KDDI CORPORATION,JP	feodotracker.abuse.ch



Overview

This describes the resources that make up the CyberGreen API. If you have any problems or requests please log an issue

Current SDKs

The current SDKs can be found here.

Current Version

By default, all requests receive the **v0** of the API. We encourage you to explicitly request this version via the `Accept` header.

```
Accept: application/vnd.cybergreen.v0
```

Authorization

```
$ curl -H "Accept: application/vnd.cybergreen.v0" -H "Authorization: Token token=646cc6d029998c702f1a377260e5f6a0" https://stats.cybergreen.net/api
```

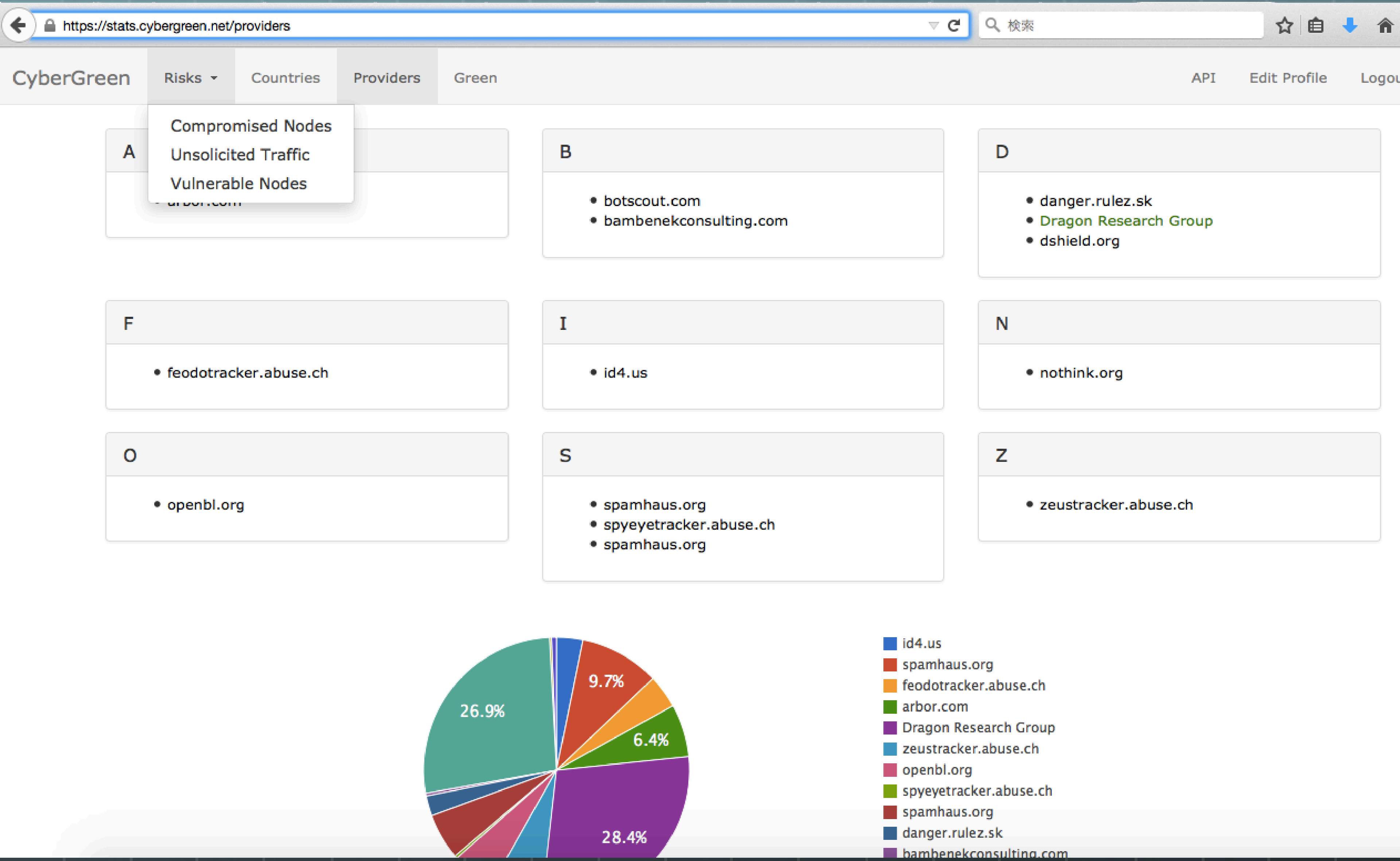
Schema

All data is sent and received as JSON.

Blank fields are can be included as 'null' or omitted.

Basic

```
$ curl -H "Accept: application/vnd.cybergreen.v0" -H "Authorization: Token token=646cc6d029998c702f1a377260e5f6a0" https://stats.cybergreen.net/api/risk/unsolicited/o
bservables?limit=5
```



A

- arbor.com

B

- botscout.com
- bambenekconsulting.com

D

- danger.rulez.sk
- Dragon Research Group
- dshield.org

F

- feodotracker.abuse.ch

I

- id4.us

N

- nothink.org

O

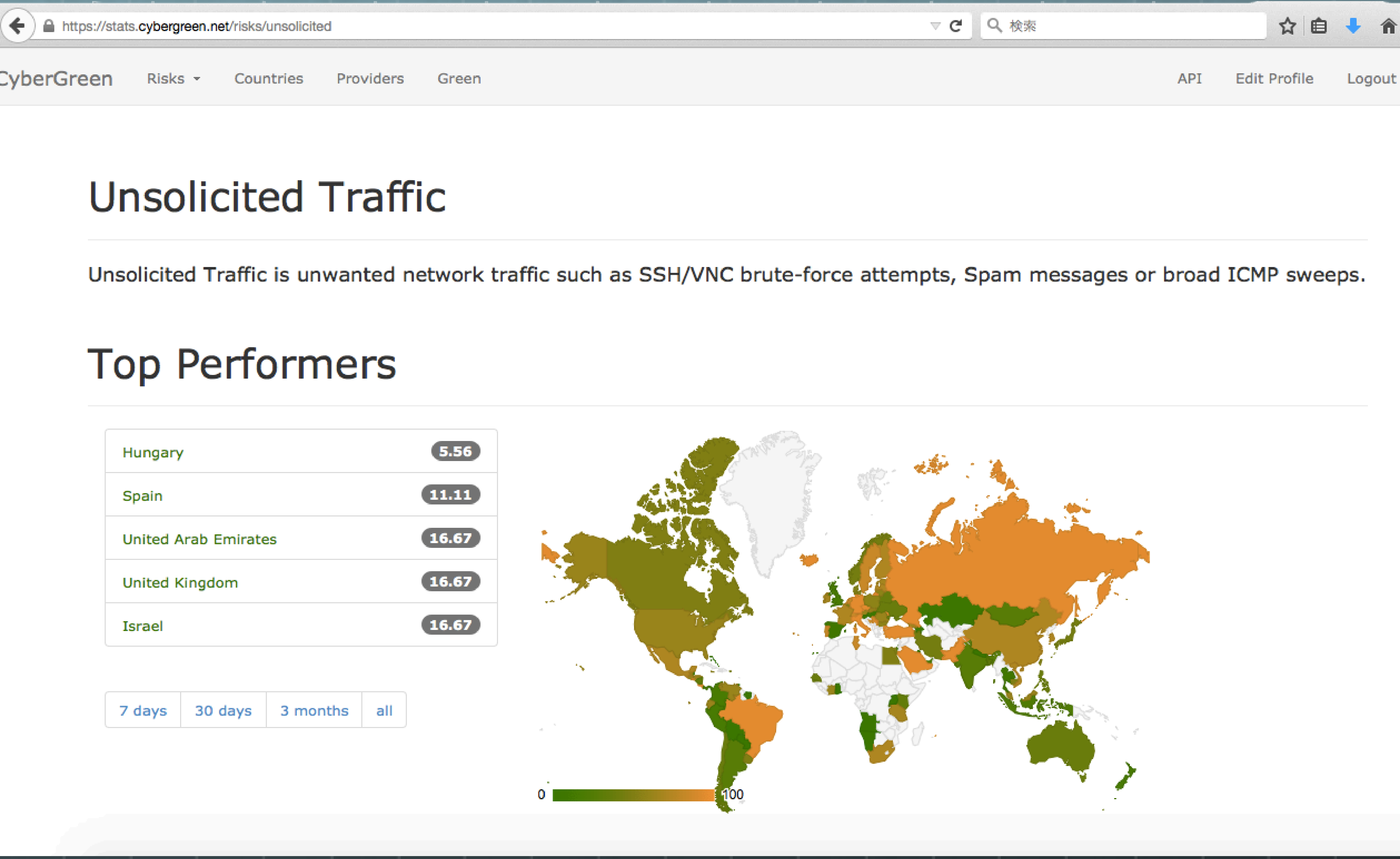
- openbl.org

S

- spamhaus.org
- spyeyetracker.abuse.ch
- spamhaus.org

Z

- zeustracker.abuse.ch



Unsolicited Traffic

Unsolicited Traffic is unwanted network traffic such as SSH/VNC brute-force attempts, Spam messages or broad ICMP sweeps.

Top Performers

Hungary	5.56
Spain	11.11
United Arab Emirates	16.67
United Kingdom	16.67
Israel	16.67

Internet health Analysis

- Correlate with other statistics
  - By ICT budget – in progress from OECD
  - By pirated software rates – from BSA
  - By CERT bulletins released – from CERT provided data
  - By number of CISSP?
  - ....suggestions?
- Small Case study
- Quarterly Report

Metrics Road Map

- Improve the original Green Index
  - Incorporate momentum changes
  - Incorporate “internet subscriber” normalization (comparing “apples to apples ”)
  - Incorporate rolling trend information

- Planning to form the Metrics experts Working Group

Portal - Road map

- Enable CSIRTs and researchers to:
  - Self publish their own analysis
  - Build application on the platform
  - Share data with their peers
- Bootstrap emerging CSIRTs with the tools they need to remediate
- Build an open – source community around out tools and statistics

Key stakeholders

- The CERT community
- Organizations, both commercial and non-profit, that are sources of data relate to cyber risk
- Research organizations and individuals specifically focusing on measurement of cyber health and risk factors

Planning to form a Cyber Green Advisory Board & supporting technical analysis committee

Join the global Cyber Green Initiative!

- The Cyber Green platform provides access to:
  - Data focused on your environment
  - Remediation best practices to address risk factors
  - Statistical reporting on cyber health

For emerging CSIRTs --

We provide training to use portal and tools

Improve your capacity to improve cyber health!

Towards the Safe, Clean and Reliable Internet Ecosystem

JPCERT/CC
Global Coordination Division
global-cc@jpcert.or.jp