CyberGreen

*A global community to measure and improve cyberhealth*

# Improving Cyber Ecosystem Health through Metrics, Measurement and Mitigation Support

Yurie Ito
Executive Director, CyberGreen Institute

May 2017, Swiss Re, OECD workshop

# Uniqueness about CG metrics

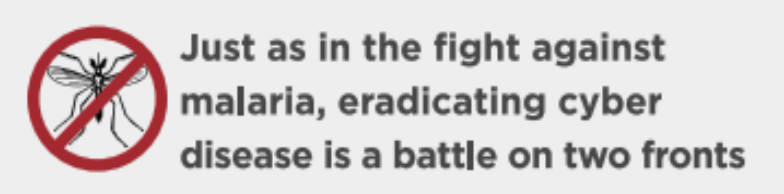
- We measure “Risks to Others”
- Policy / Decision making process support


 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

# Challenges and Opportunities

- Focusing on Symptoms not Cause
  - *Traditional approaches to cybersecurity have crucial limitations based on a reactive approach to addressing threats or incidents. Reactive approaches do not improve underlying conditions and reduce risk at a systemic level.*



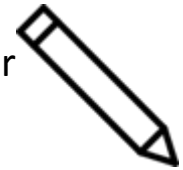

- Establishing Statistical Rigor
  - *Challenges stem from many sources, including issues in collection, the inability to cross compare data, and a failure to apply normalization techniques*

# CyberGreen: What we do

Cyber Health Measurement.
We measure **Risk-to-others.**

Source risk condition data

Provide a clearinghouse for
Risk Mitigation BCPs.



Capacity Building
needs analysis and
impact measurement

Advocacy


 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

CyberGreen

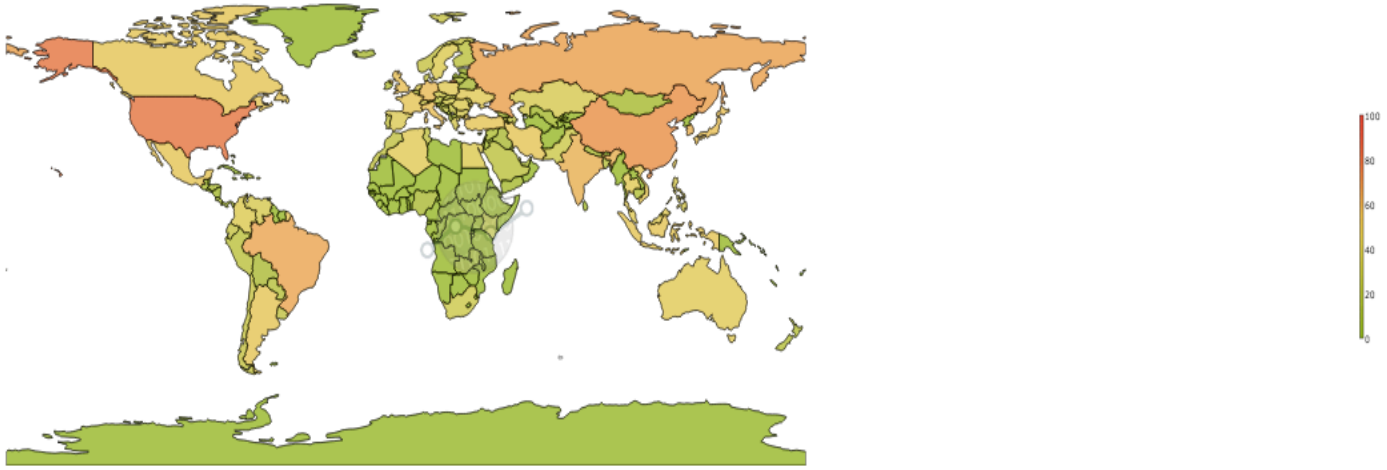
# Introduction to features on the CyberGreen Stats Portal

# Stats.cybergreen.net

## View a Country

Select a country

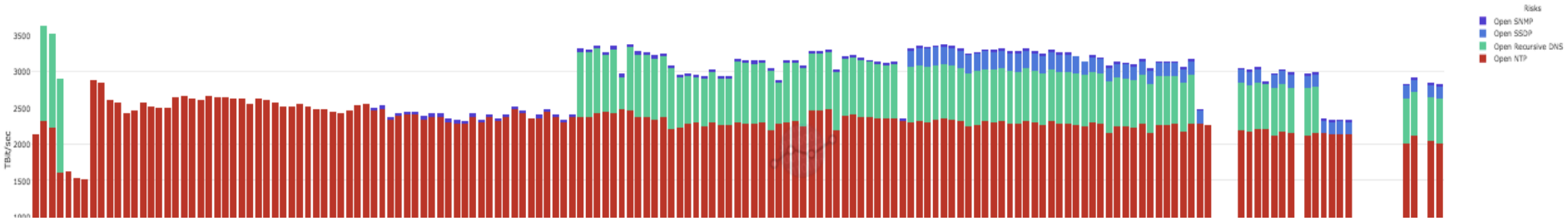
## Level of Risk Posed to Others




Level of risk posed to others on selected risk on a scale from 0-100 (100=worst). For more on data sources, calculations and terms see Glossary and data page

DDOS

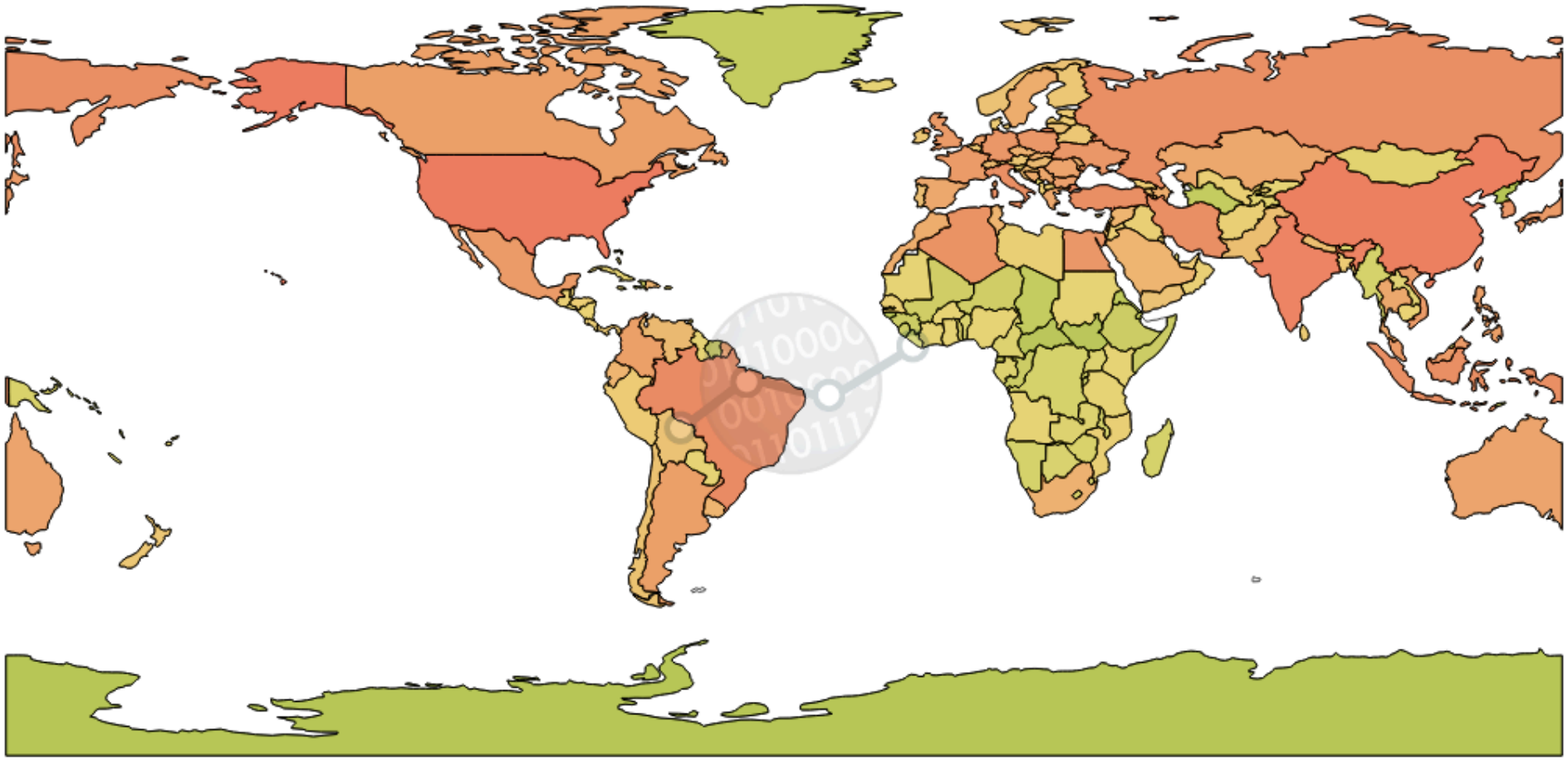
## Global DDOS Potential




 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

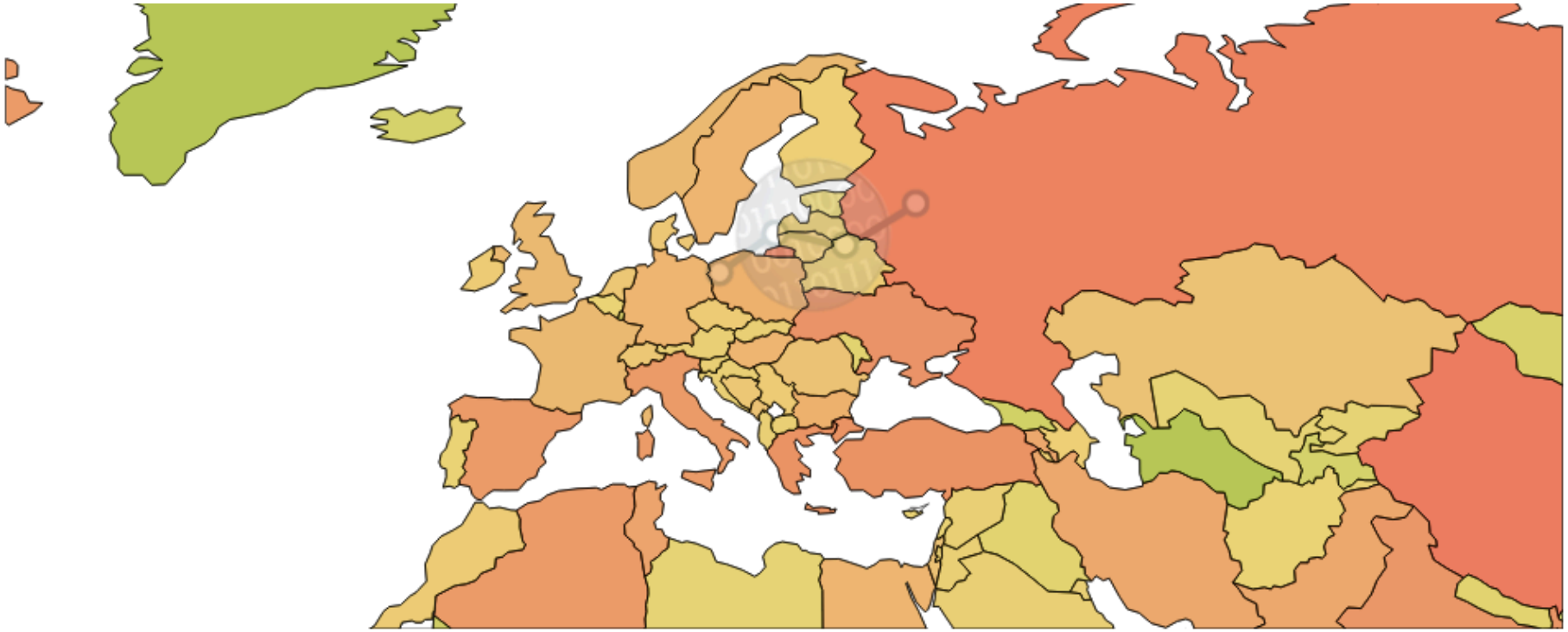
# Global look –
# Open recursive NTP servers



 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

# Regional view: Europe - Open recursive SSDP servers



Level of risk posed to others on selected risk on a scale from 0-100 (100=worst). For more on data sources, calculations and terms see Glossary and data page

Open SSDP

 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

# SWITZERLAND

Level and trends of risk posed to others by this country. Breakdown of risk source by Autonomous System (AS). For more on data collection, methodology and meaning of terms see Glossary and data page

## Country Comparison

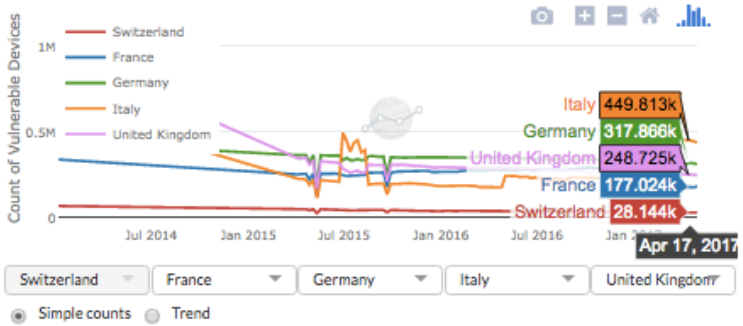
These graphs show the risk over time and allows you to compare this country with others.

## AS Source

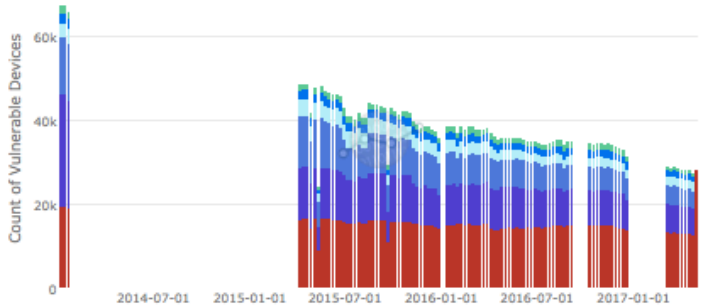
These graphs show which Autonomous Systems (AS) are the biggest contributors to this risk.

View any Autonomous System in this country

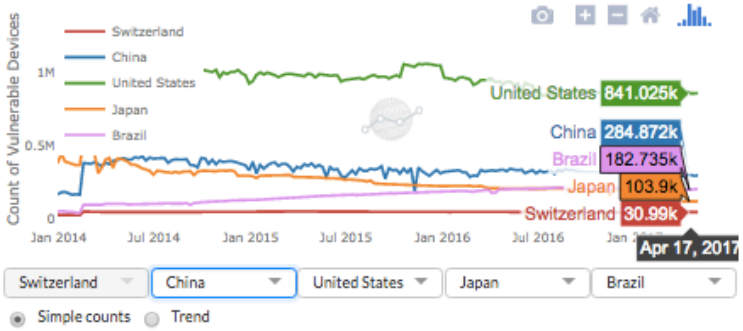
### OPEN RECURSIVE DNS | SWITZERLAND #53



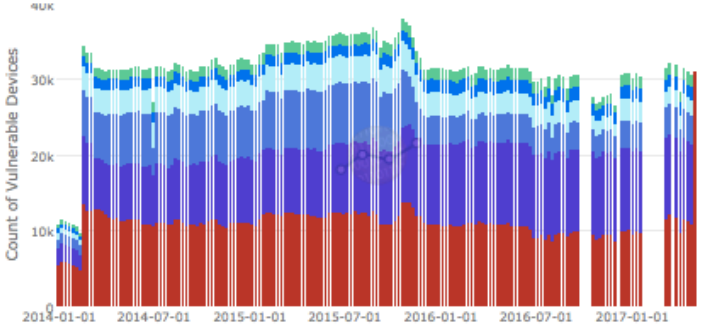

### OPEN RECURSIVE DNS | AS SOURCE



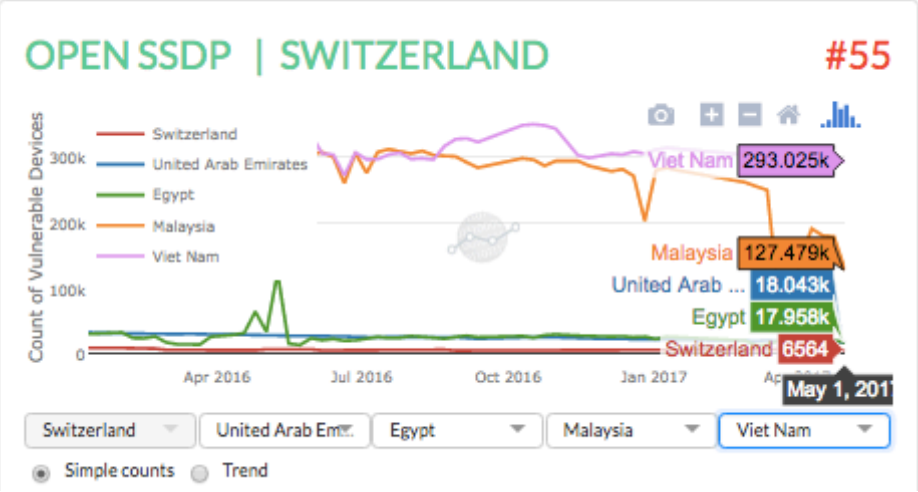

### OPEN NTP | SWITZERLAND #21

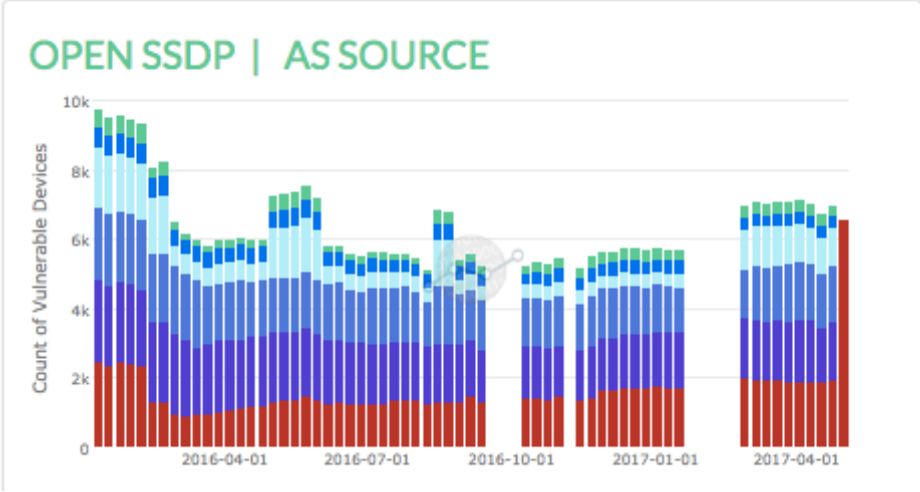


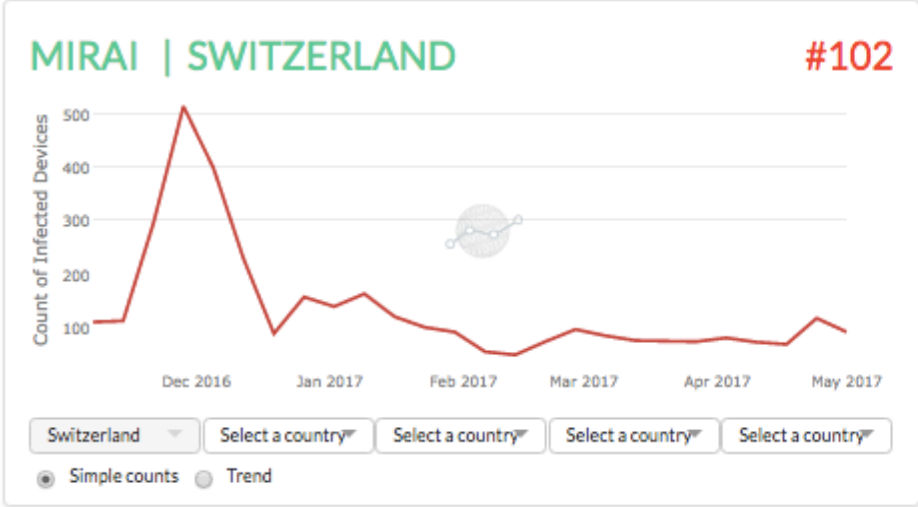

### OPEN NTP | AS SOURCE

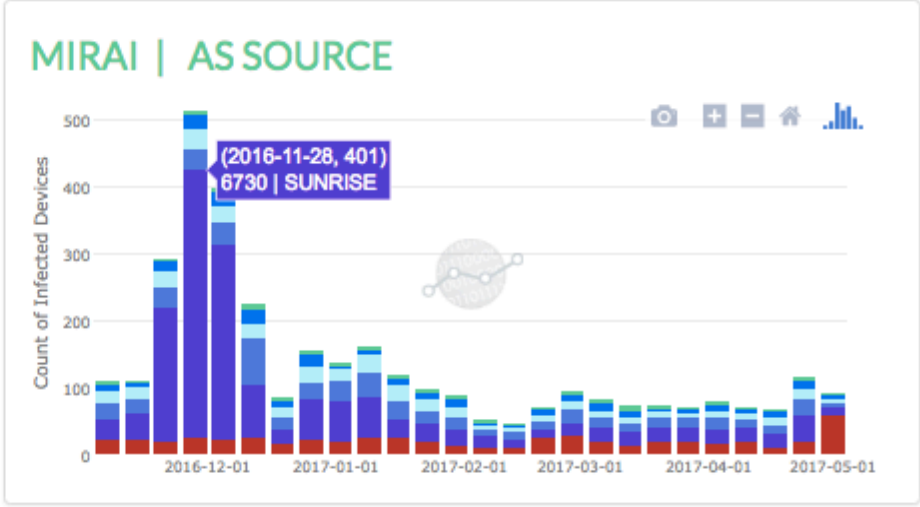



 Copyright © 2016, CyberGreen 


OPEN SSDP | SWITZERLAND
#55
Count of Vulnerable Devices
Switzerland
United Arab Emirates
Egypt
Malaysia
Viet Nam
300k
200k
100k
0
Viet Nam 293.025k
Malaysia 127.479k
United Arab ... 18.043k
Egypt 17.958k
Switzerland 6564
Apr 2016
Jul 2016
Oct 2016
Jan 2017
May 1, 201
Switzerland
United Arab Em
Egypt
Malaysia
Viet Nam
Simple counts
Trend

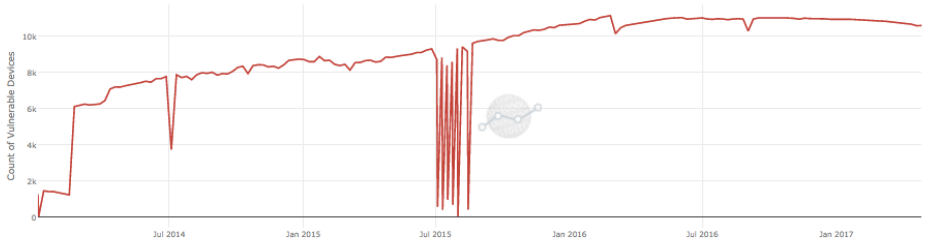

OPEN SSDP | AS SOURCE
Count of Vulnerable Devices
10k
8k
6k
4k
2k
0
2016-04-01
2016-07-01
2016-10-01
2017-01-01
2017-04-01


MIRAI | SWITZERLAND
#102
Count of Infected Devices
500
400
300
200
100
Dec 2016
Jan 2017
Feb 2017
Mar 2017
Apr 2017
May 2017
Switzerland
Select a country
Select a country
Select a country
Select a country
Simple counts
Trend


MIRAI | AS SOURCE
Count of Infected Devices
500
400
300
200
100
0
(2016-11-28, 401)
6730 | SUNRISE
2016-12-01
2017-01-01
2017-02-01
2017-03-01
2017-04-01
2017-05-01

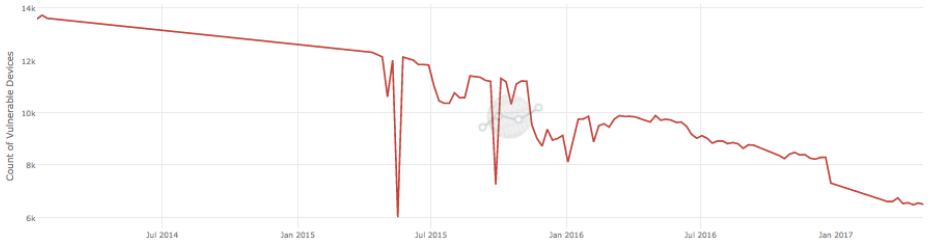
# AS Switzerland - 3303 | SWISSCOM Swisscom (Switzerland) Ltd

## OPEN NTP



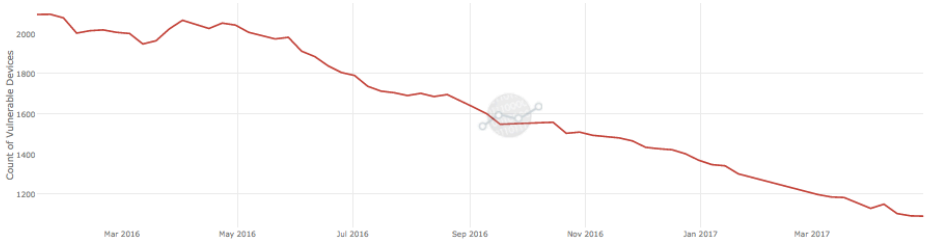

3303 | SWISSCOM Swisscom (Switzerla... | Select an ASN | Select an ASN | Select an ASN | Select an ASN

## OPEN RECURSIVE DNS




3303 | SWISSCOM Swisscom (Switzerla... | Select an ASN | Select an ASN | Select an ASN | Select an ASN

## OPEN SSDP




3303 | SWISSCOM Swisscom (Switzerla... | Select an ASN | Select an ASN | Select an ASN | Select an ASN

## OPEN SNMP

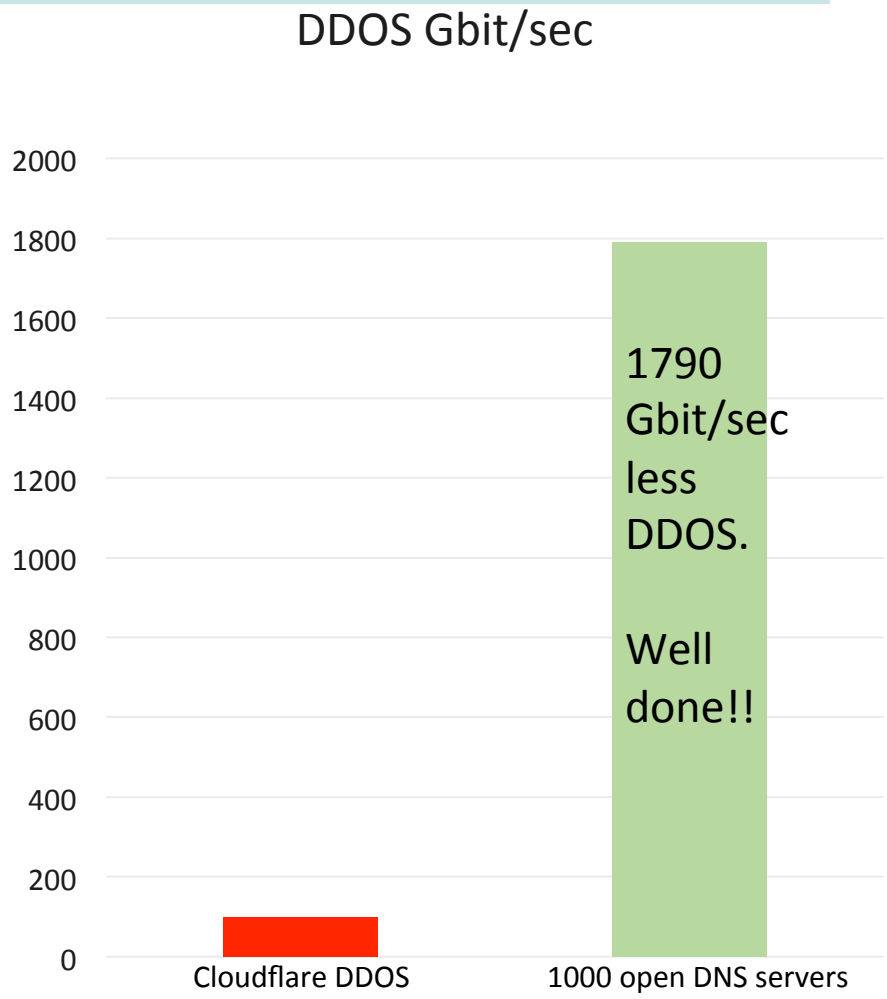

3303 | SWISSCOM Swisscom (Switzerla... | Select an ASN | Select an ASN | Select an ASN | Select an ASN

## MIRAI


3303 | SWISSCOM Swisscom (Switzerla... | Select an ASN | Select an ASN | Select an ASN | Select an ASN

# Health benefit to the Internet

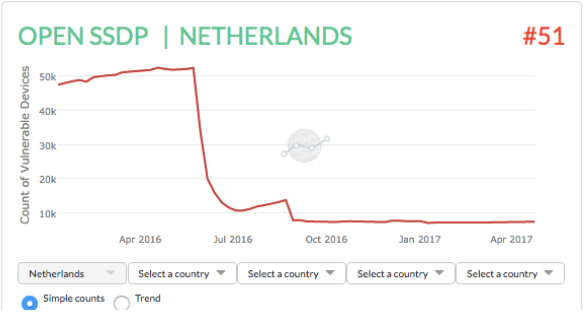
- Open DNS has an amplification factor of 179.
- Every reduction in 1000 open DNS vulnerable servers, reduces the global DDOS potential by 1790 Gbit/sec
- The DDOS which took down cloudflare was a mere 100 Gbit/sec

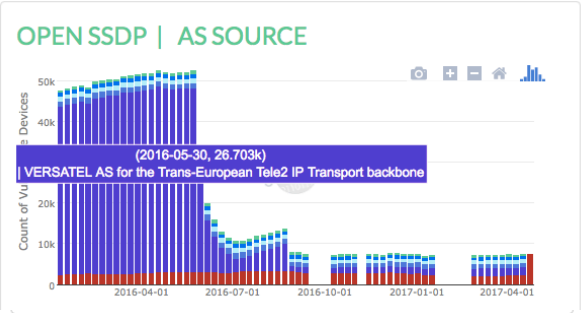



 Copyright © CyberGreen 2016 All Rights Reserved.

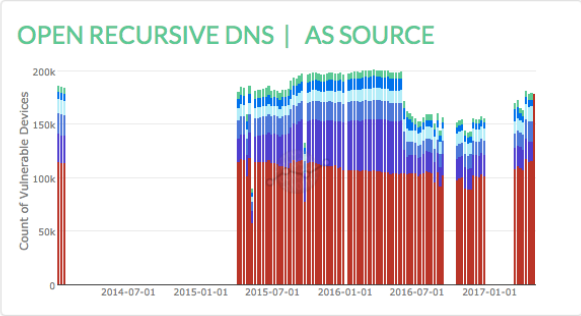
CyberGreen

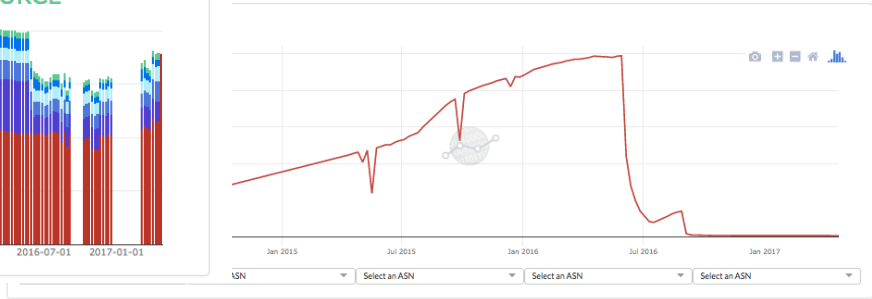
# Clearing House for Global Mitigation BCPs









 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

# Download aggregated data through API

## Download & API

We provide full access to all the data available here in the portal. The two main methods to access it are:

- Bulk: download complete CSV files (~12m rows)
  - Coming soon: individual slices of the data pre-computed!
- API: via an API that allows you to slice and dice the data and integrate easily with your own applications
  - Format: CSV and JSON
  - Interested in an SLA? Please contact us contact us

### Bulk Data

The Bulk Data is stored in bits store here:

http://bits.cybergreen.net/dev/stats/latest/

Download the full aggregated data:

http://bits.cybergreen.net/dev/stats/latest/count.csv

The structure of the file is:

```
date,risk,country,asn,count,count_amplified
```

### API

There are three different groups of API endpoints for getting data:

- Count API: the main data in the portal available via two main API endpoints:
  - count: full access to the count data at the lowest level of granularity
  - count_by_country: data aggregated to the country level
- Reference Data API: access to the reference data we use e.g. countries, risks and AS
- Rankings API - Responds with list of countries with corresponding ranks for given risk and time period

### Limitations

We are limiting number of results requested from API. We are doing this in order to avoid possible timeoute errors, as requested data in some cases may easily exceed several milion rows. To get the full data you have two aptions:

- Download the full aggregated data (see above) and slice and dice on your own.
- Change `page` attribute of query string and get next 50000 results. API will respond with empty list of `results` if `page` exceeds total number of pages.

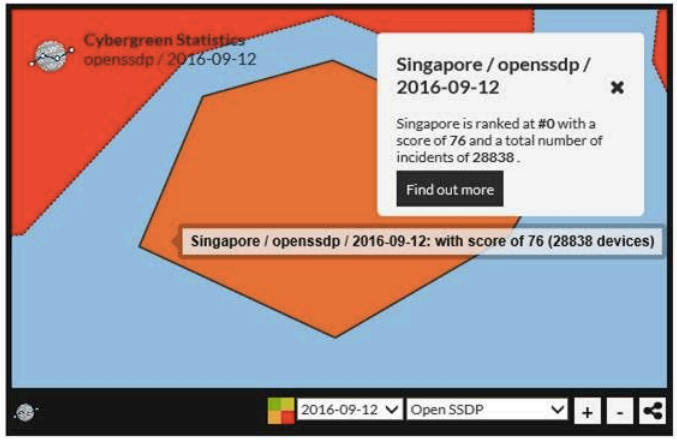
You can find full documentation of the API below and try out the API using the interactive interface.

 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

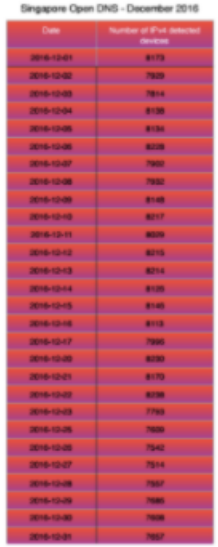
# Singapore case :
# CG Metrics to drive multi-stakeholders risk reduction
# National level campaign

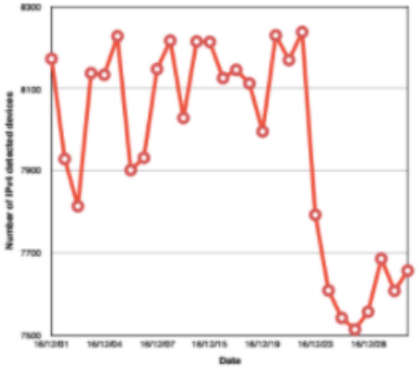
Opening Speech by Dr Yaacob Ibrahim, Minister For Communications And Information And Minister-In-Charge Of Cybersecurity, At The Asean Ministerial Conference On Cybersecurity




**[SingCERT] Cyber Risk Conditions from Vulnerable Internet Service Protocols**

**<u>Joint Advisory by SingCERT and CyberGreen</u>**




Top policy commitment at ASEAN ICT Ministers Meeting in October, 2016 "CyberGreen is one global initiative that will aid us in securing our common cyberspace. The CyberGreen project aims to give countries awareness of the state of cyber health and potential vulnerabilities within our borders…."

 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

# Correlation Analysis, collaborations

## Research Focus

Our team sought to answer two questions:

1. What socioeconomic factors, if any, impact cyberhealth and what are the features of the correlations between them?
2. Does cyberhealth evaluated through a socioeconomic analysis differ from traditional measures specifically those that evaluate cyber re maturity?

## Policy Recommendations

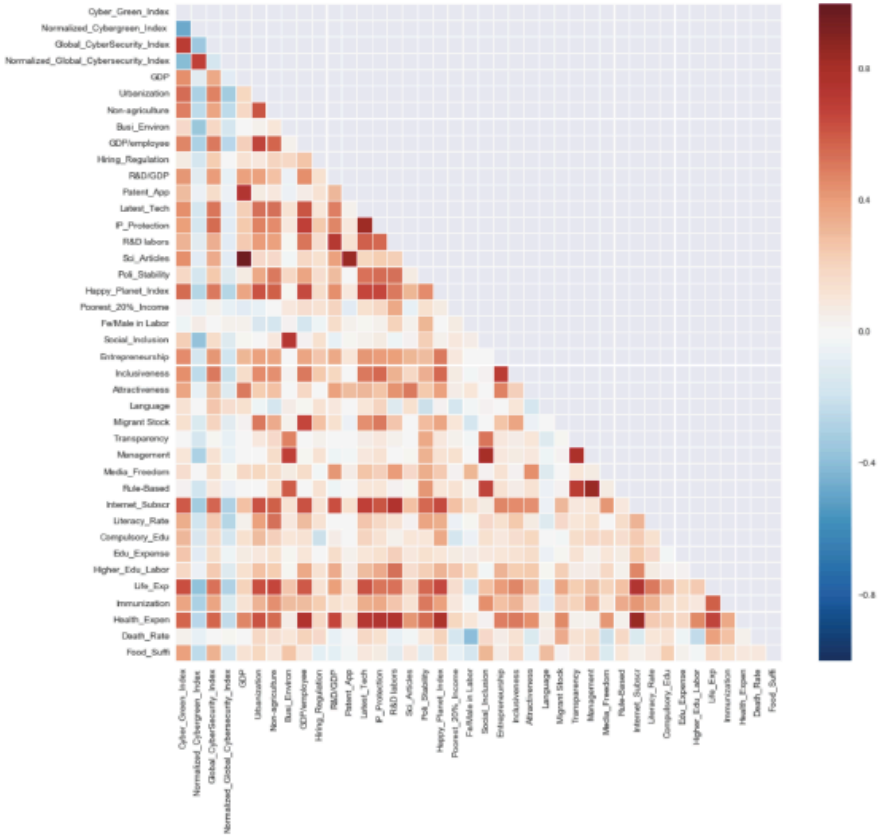
1. To improve the *overall* cyberhealth in countries of all income levels, nations should invest in improving various socioeconomic areas, such as health expenditure (per capita) and research and development
2. Specifically for *lower* and *lower-middle* income countries, these nations should prioritize investing in good governance practices, in addition to the socioeconomic investment areas
3. *Upper* and *upper-middle* income countries should continue to explore other areas which could improve cyberhealth as improvements to cyberhealth through socioeconomic advancements yield marginal results.
4. Countries should commit to developing more tools to measure cyberhealth

 Copyright © CyberGreen 2016 All Rights Reserve

# Methodology: Model I

## Principal Component Analysis

| | CyberGreen Index | Composite Socio-economic Index | Global Cybersecurity Inde |
|---|---|---|---|
| CyberGreen Index | 1 | -- | -- |
| Composite Socio-economic Index | $r_{SC}$ | 1 | -- |
| Global Cybersecurity Index | $r_{GC}$ | $r_{GS}$ | 1 |

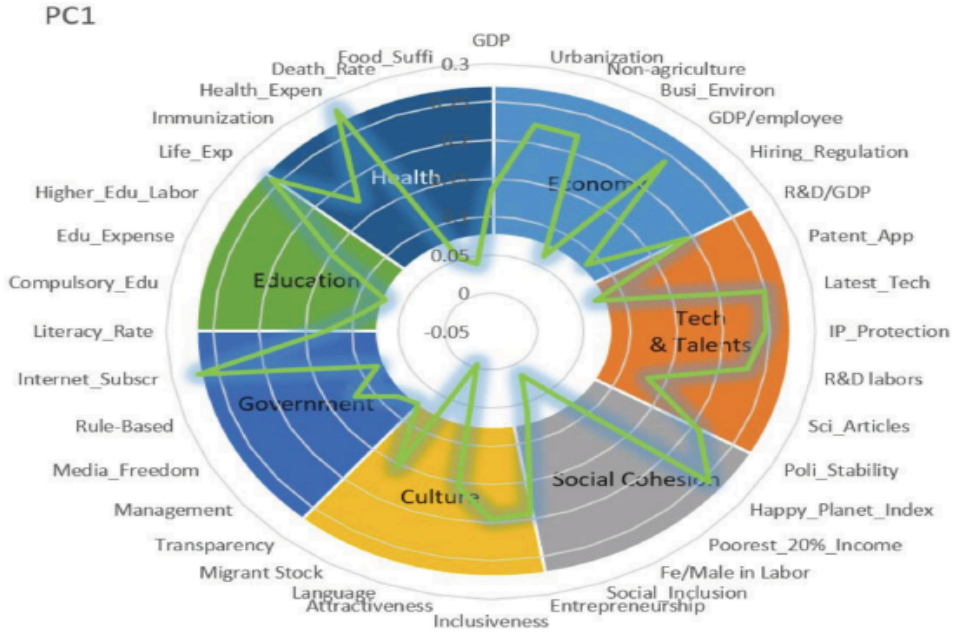



# Methodology: Model II

## Regression on the relevant components from our Model I

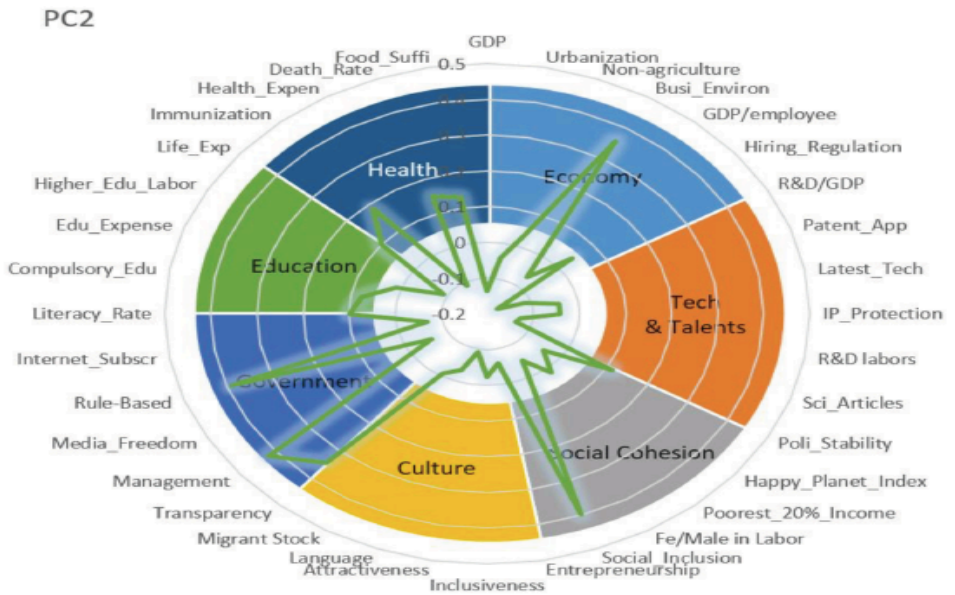
| Socioeconomic Indicators for Component I *"Comprehensive Socioeconomic Competitiveness"* | Socioeconomic Indicators for Component II *"Governance"* |
|---|---|
| Health expenditure per capita, PPP | Public sector management |
| Fixed broadband subscriptions (per 100 people) | CPIA policies for social inclusion/equity |
| Life expectancy at birth, total (years) | CPIA property rights and rule-based governance |
| The Happy Planet Index | Business regulatory environment rating |
| Availability of latest technologies | Transparency, accountability, and corruption |
| Intellectual property protection | |
| GDP per person employed | |
| Researchers and technicians in R&D | |
| Urban population (% of total) | |
| Non-agriculture, value added | |
| Political Stability and Absence of Violence/Terrorism | |

CyberGreen




## Radar Plot of All 36 Socioeconomic Indicators by Sector for Principal Component 1

**Distance from center measures the strength of that indicator in explaining Principal Component 1**




## Radar Plot of All 36 Socioeconomic Indicators by Sector for Principal Component 2

**Distance from center measures the strength of that indicator in explaining Principal Component 2**

# Metrics v.3 : device level health metrics

- Improve Asset Owner Metrics, Create New Vendor Metrics (v.2+)
- Analyze who has greater ability for mitigation impact
- V.2 is asset owner focused
- V.3: how can we add “vendor risk to others”
- IoT devices health metrics

**CyberGreen is looking for the Sponsor for this research and development of Metrics v.3**

**Please contact us how to Support.**

contact@cybergreen.net / yito@cybergreen.net

 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen

# Questions

- Is CG metrics useful to you?
- What do we like to inform policy makers? or your management from incident response community?
  - What other risk indicators should/can we measure?
- Anybody conducted mitigation campaign past 12 months?
- Anybody planning to conduct mitigation campaign next 12 months?
- Anybody wants to data donation? Financial contribution?

 Copyright © CyberGreen 2016 All Rights Reserved.

CyberGreen


Help us foster the CyberGreen approach.

Participate in the Mitigation Campaign.

Contact:

yito@cybergreen.net