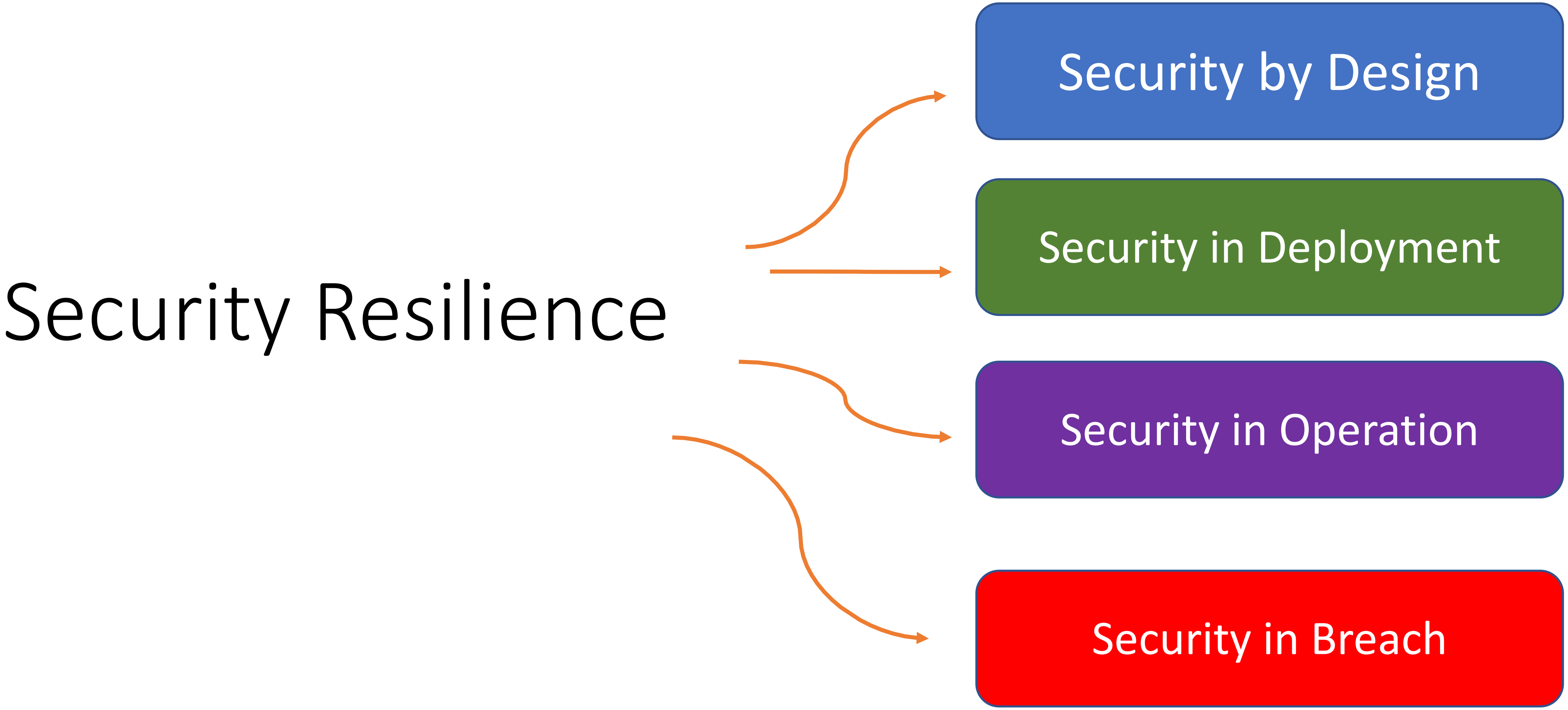
Security Incident Response Capabilities & CSIRTs

Adli Wahid
Security Specialist
adli@apnic.net

Adli Wahid

- Security Specialist @ APNIC
- Board Member @ FIRST.org
- Member of INTERPOL Cyber Crime Expert Group
- Let’s Connect
  - Twitter: @adliwahid
  - Linkedin: Adli Wahid
  - APNIC’s Blog: https://blog.apnic.net



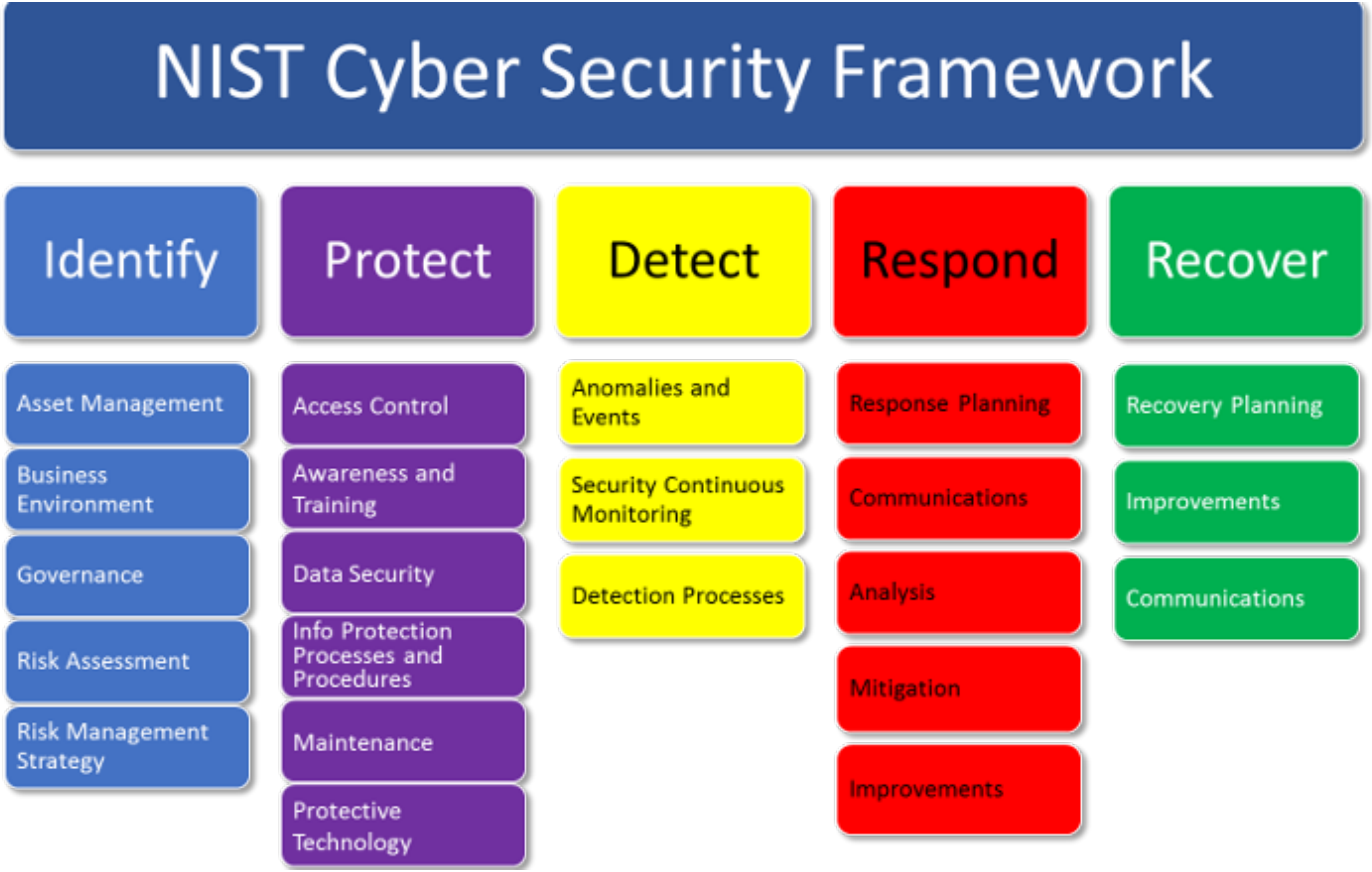
Security Resilience

Security by Design

Security in Deployment

Security in Operation

Security in Breach



NIST Cyber Security Framework

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

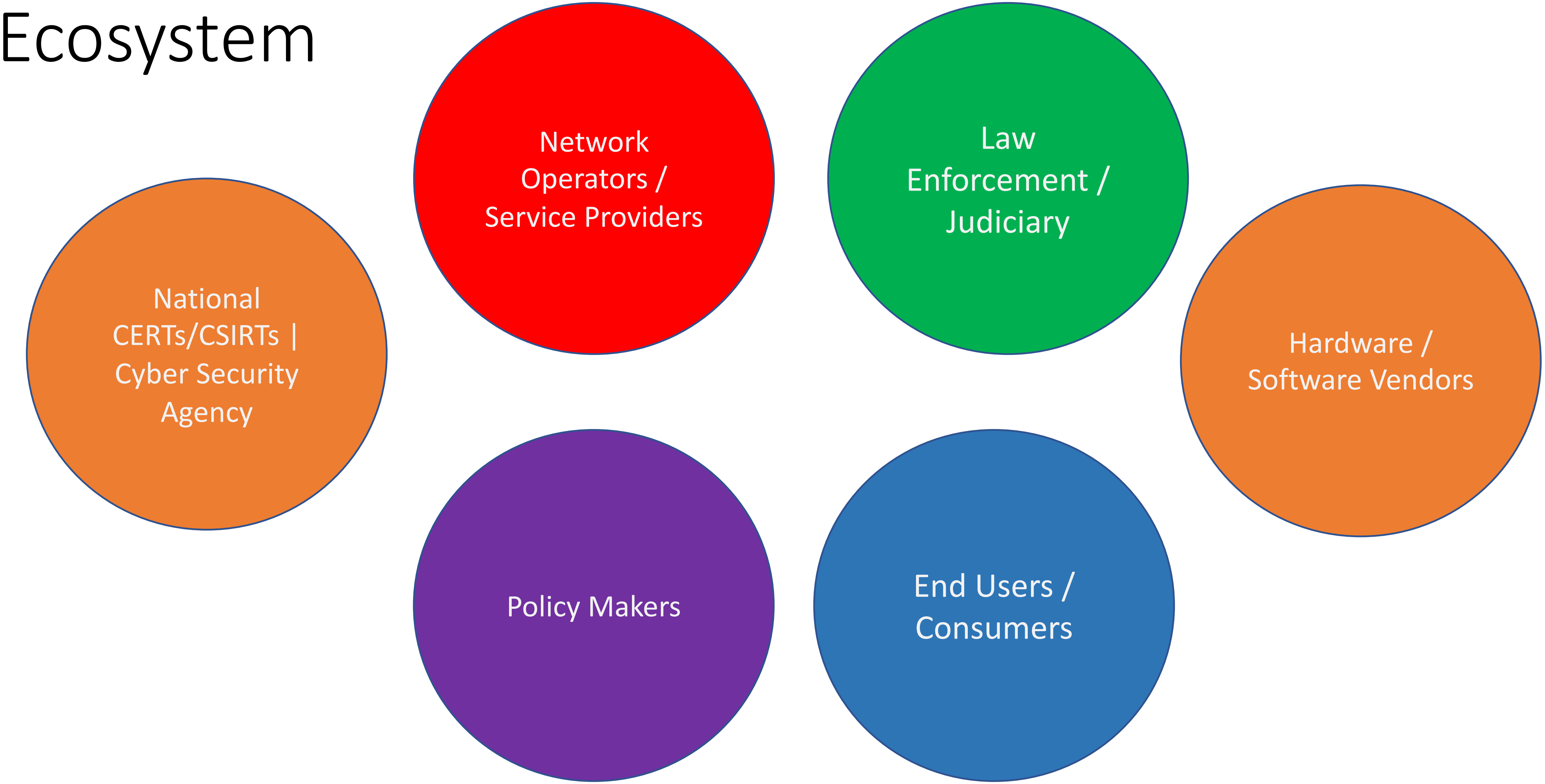
Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

Ecosystem



Network Operators / Service Providers

Law Enforcement / Judiciary

National CERTs/CSIRTs | Cyber Security Agency

Hardware / Software Vendors

Policy Makers

End Users / Consumers

Why?

1. Get notified
2. Reduce Impact of Security Incident
3. Understand the (root) cause
4. Do Something About It

Get Notified

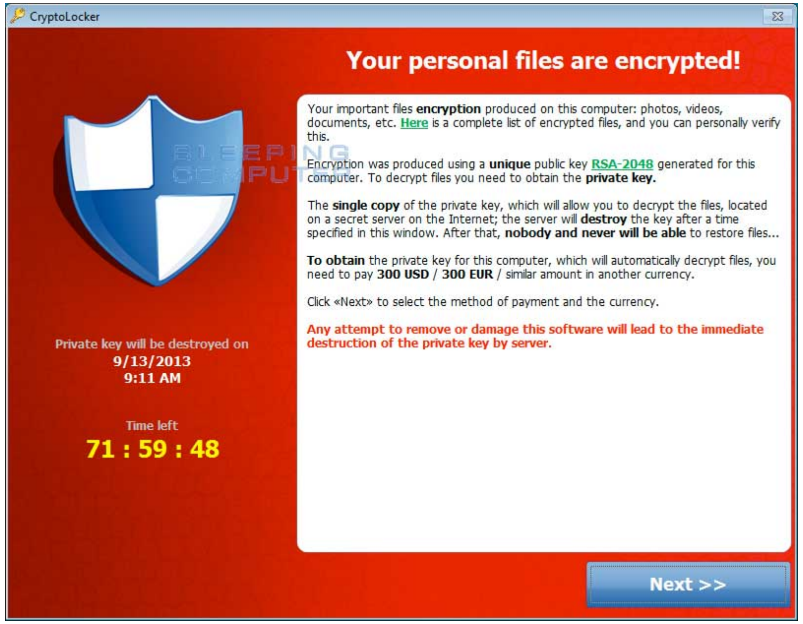
- How can other CERTs/CSIRT contact you?
  - Incidents
  - Source of Security Incidents
  - Suspicious activities
  - Threat Information
- Whois db and other means
  - APNIC's Whois Accuracy initiative
- Will you do something about it?
  - Awareness
  - Capabilities
  - Policies & Procedures
- All of the above: Preparedness

```
irt:           IRT-APNIC-IS-AP
address:       South Brisbane, Australia
e-mail:        helpdesk@apnic.net
abuse-mailbox: helpdesk@apnic.net
admin-c:       AIC1-AP
tech-c:        AIC1-AP
auth:          # Filtered
remarks:       APNIC Infrastructure Services
mnt-by:        MAINT-APNIC-IS-AP
changed:       hm-changed@apnic.net 20110704
source:        APNIC
```

https://blog.apnic.net/2016/09/27/lea-stakeholders-enter-whois-discussion/

Reduce Potential Impact

- Timeliness
- Security Incidents have affect constituent’s
    - Operation
    - Business
    - Image / Brand
    - Safety
- Understand the (root) cause
    - Advise / Alert the constituents
- Reduce cost required to fix



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

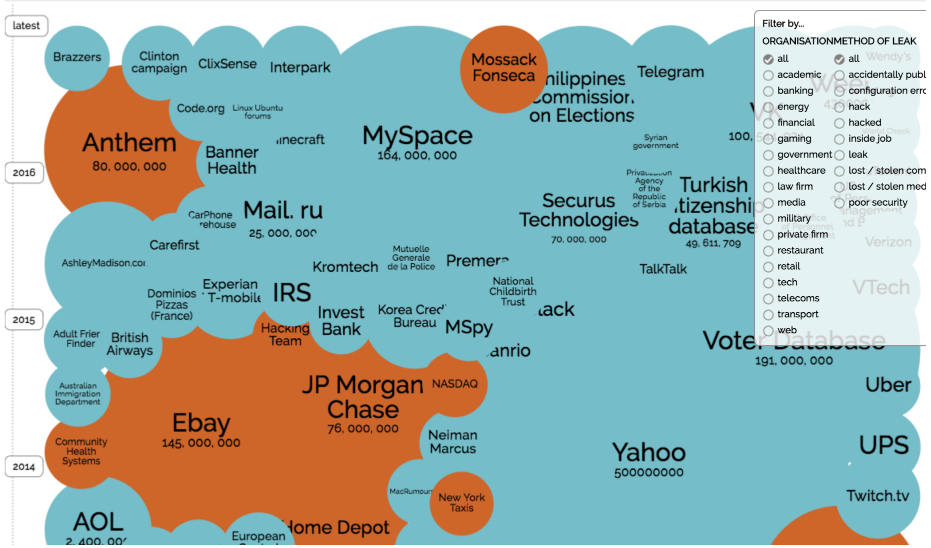
Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/13/2013
9:11 AM

Time left
71 : 59 : 48

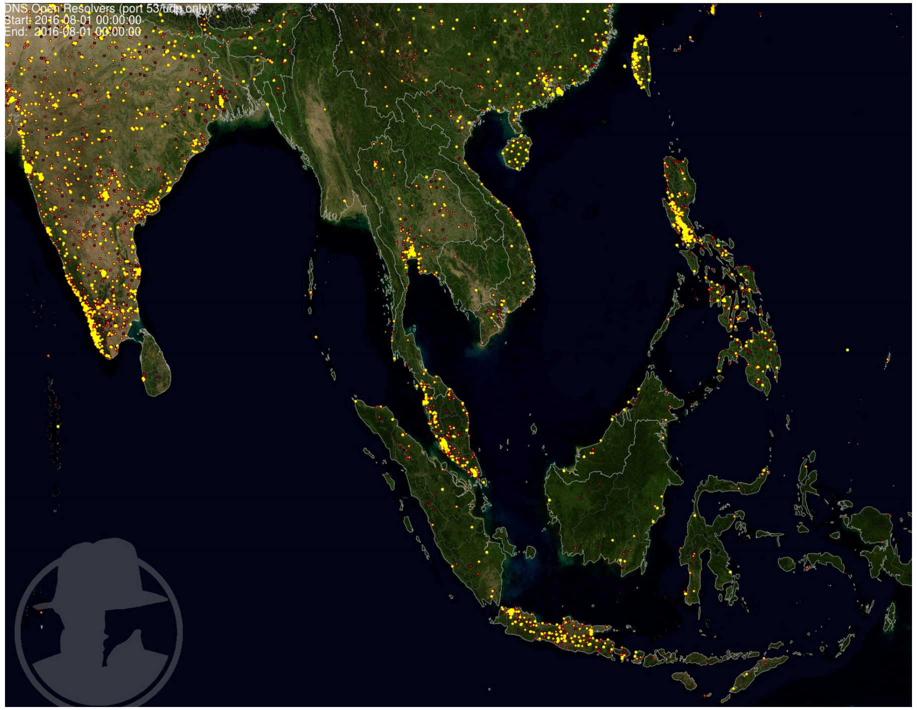
Cryptolocker



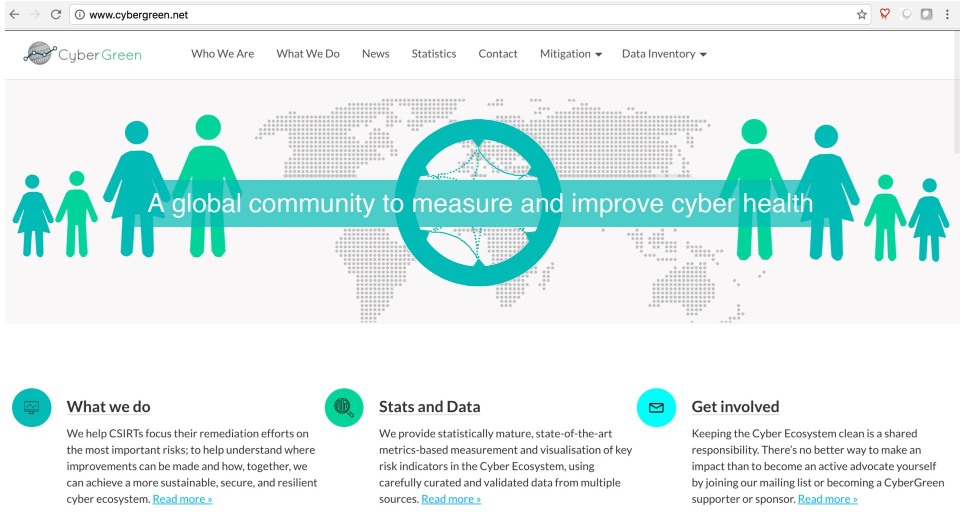
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Do Something About It

- Remediation
  - ○ Analysis
  - ○ Collaboration
  - ○ Escalation
- DDoS Example
  - ○ Fixing / removing vulnerable hosts
  - ○ Fixing / removing vulnerable services
  - ○ BCP 38 / Source Address Validation
  - ○ Continuous Monitoring
- Join industry-wide initiatives


DNS Open Resolvers (port 53/udp only)
Start: 2016-08-01 00:00:00
End: 2016-08-01 00:00:00

ShadowServer Foundation



What we do

We help CSIRTs focus their remediation efforts on the most important risks; to help understand where improvements can be made and how, together, we can achieve a more sustainable, secure, and resilient cyber ecosystem. Read more »

Stats and Data

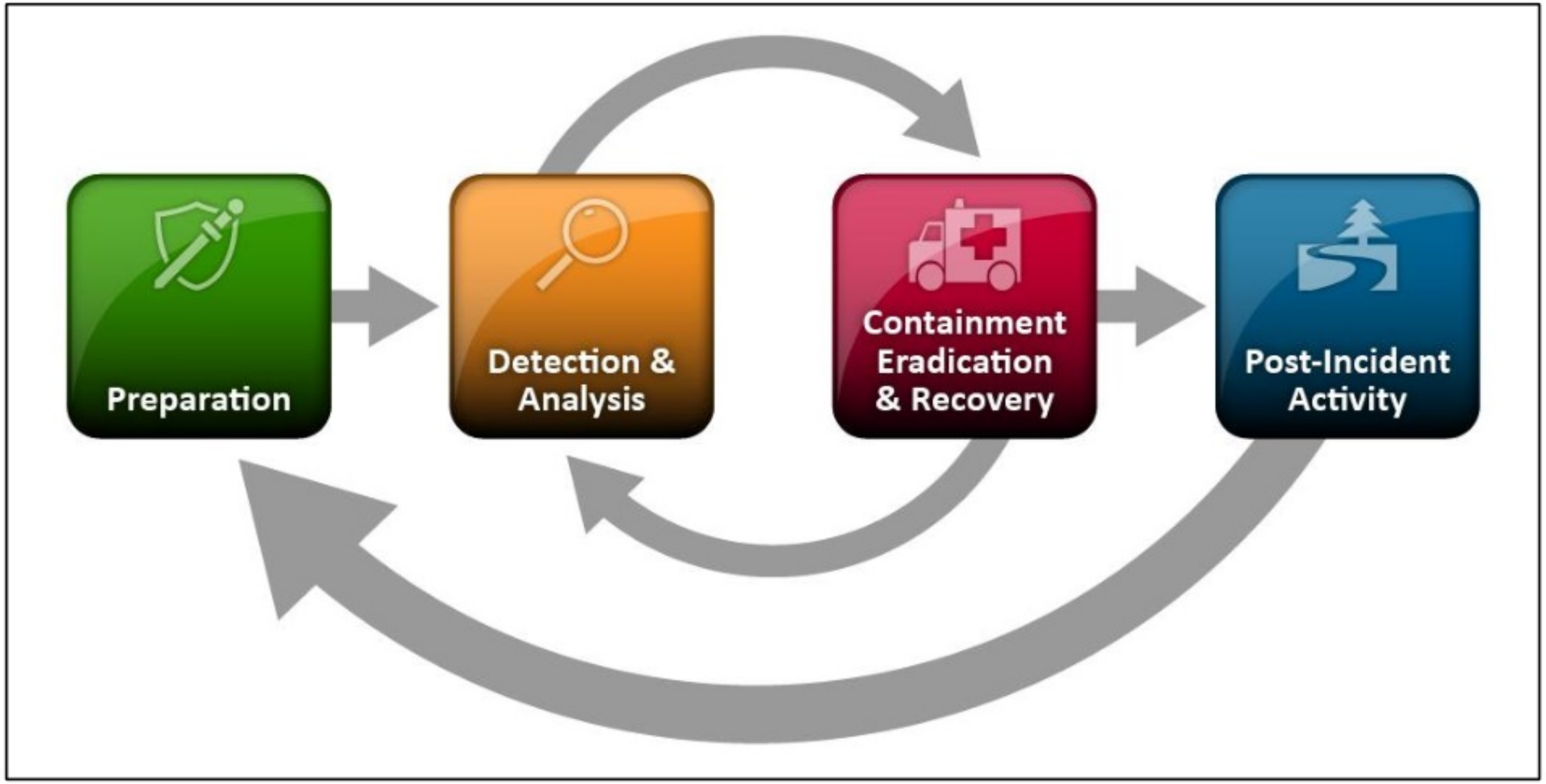
We provide statistically mature, state-of-the-art metrics-based measurement and visualisation of key risk indicators in the Cyber Ecosystem, using carefully curated and validated data from multiple sources. Read more »

Get involved

Keeping the Cyber Ecosystem clean is a shared responsibility. There's no better way to make an impact than to become an active advocate yourself by joining our mailing list or becoming a CyberGreen supporter or sponsor. Read more »

https://www.cybergreen.net

Mapping Threat to Incident Response



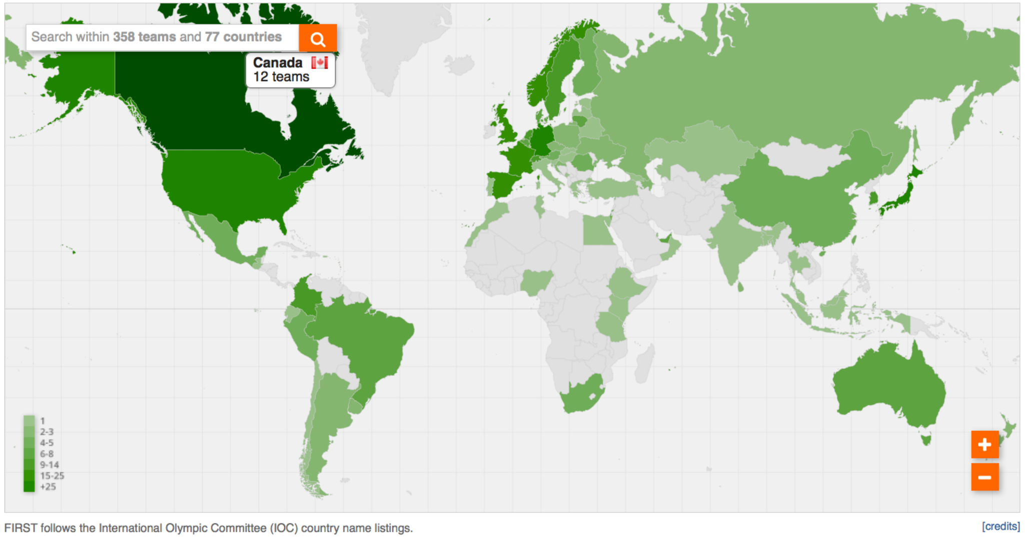
NIST SP 800-61 rev 2 (2012

Community of CSIRTs

- Trusted group
- Information Sharing
- Beyond that
  - ○ Lessons Learned
  - ○ Joint Projects (Standards, Tools, Frameworks)
  - ○ Joint Activities (Events, Drills)
  - ○ Resources (Training, Trainers)
  - ○ Mentoring

○ Examples:
  - ○ FIRST.org , APCERT, NZITF

FIRST.org Fellows



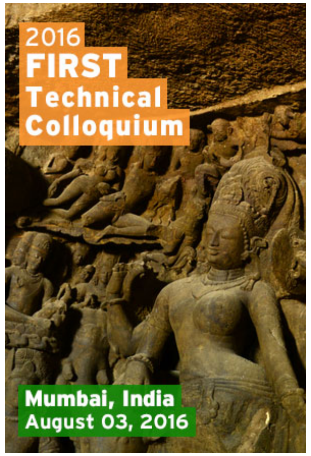
FIRST follows the International Olympic Committee (IOC) country name listings.

[credits]

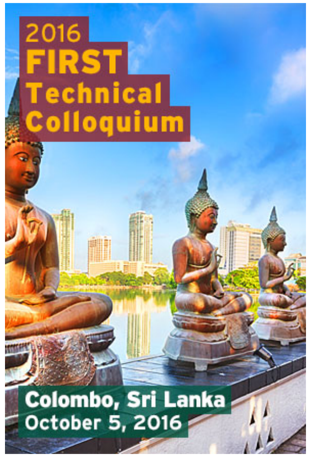
https://www.first.org

CERT/CSIRT Activities in AP Region

- Partnerships
  - Collaboration with FIRST.org
  - MoU with Asia Pacific Computer Emergency Response Teams (APCERT)
  - Share resources, promote initiatives
- Activities
  - FIRST Technical Colloquia (Security Track) at APRICOT & APNIC Supported Events
  - Cyber Security Workshops
  - Training / E-Learning
- 2017
  - FIRST-TC @ APRICOT
  - More activities being planned



Tonga CERT Discussion



Security Workshop in Bhutan

Thank You

Adli Wahid
adli@apnic.net