Strengthening the CERTs/CSIRTs Community

Adli Wahid
Security Specialist
APNIC

adli@apnic.net

Background

- Security Specialist @ APNIC
- Board Member of Forum of Incident Response and Security Teams (FIRST.org)
  - Outreach & Fellowship
- Engagements with CERTs/CSIRT, Law Enforcement Agencies, Inter-governmen forums & agencies

Agenda

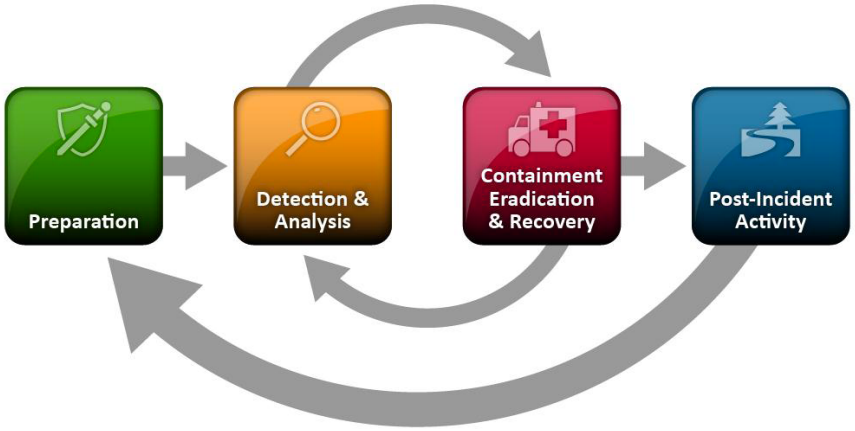
- Security Incident Response
- The Global CERT/CSIRT Community
  - FIRST Events & Initiatives
  - Other engagements
- CERTs/CSIRTs in the AP Region

Secure in Breach?

- Security is a process
  - Designing, Hardening, Monitoring, Auditing / Pen-Testing
  - Planning, Best Practices, Standards , Strategies
  - People – Skills
- Breach Fatigue!
  - Vulnerabilities in protocols & software
  - Lapse in practice & misconfiguration
  - Lack of Awareness!
- Minimizing Impact & recovery is critical
  - So is not appearing in the next day news headline
- IRT object in whois db?

Prepare & Mitigate

- Preparing to deal with incidents
  - Resources, Plans, Processes, Drills
- Minimize impact of the securitv incidents
  - Information Sharing, Tools
- Resolution / Fix
  - Collaboration, Takedowns,
- Sharing Lessons Learned!



CERTs/CSIRTs

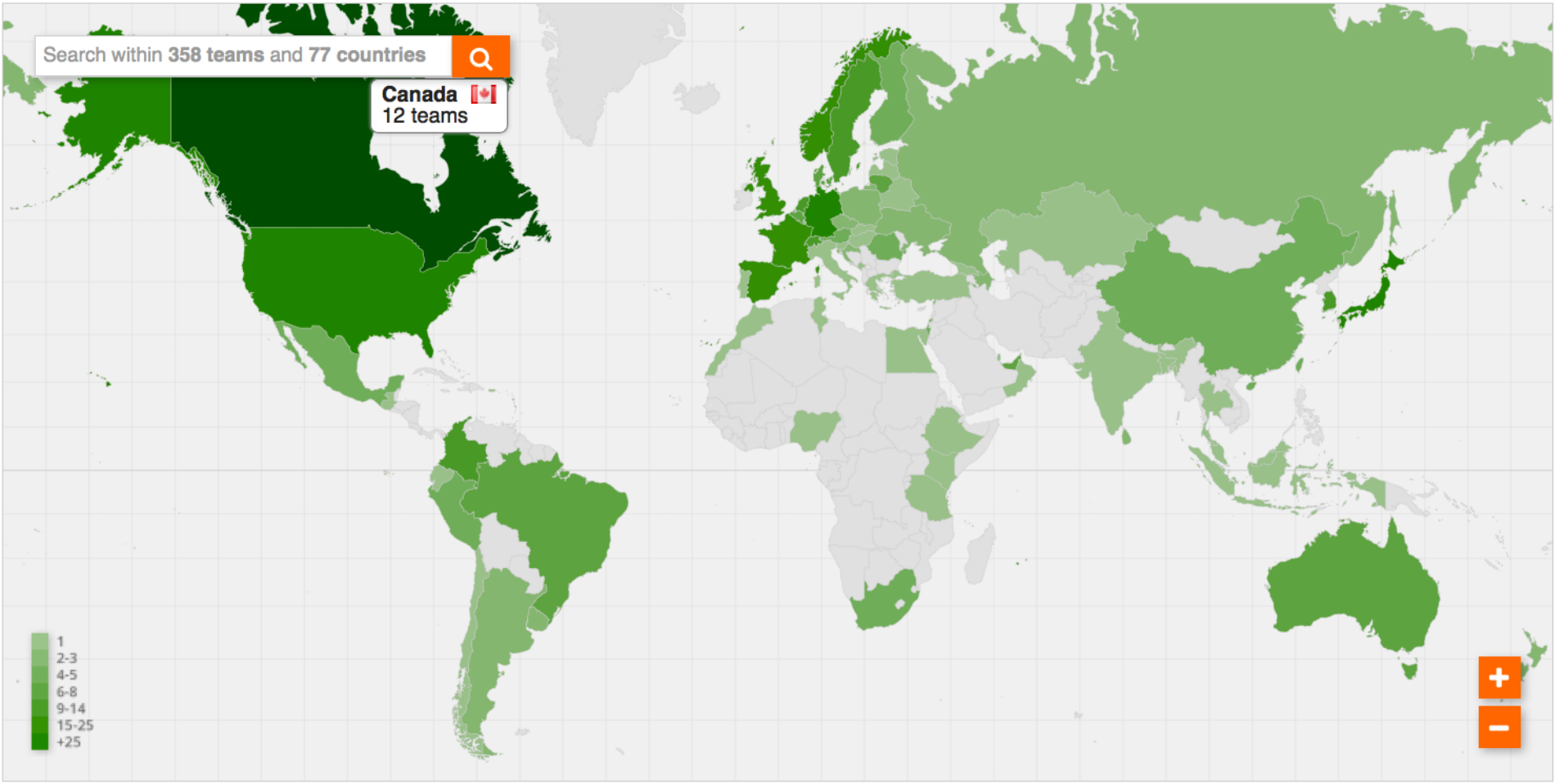
- Computer Emergency Response Teams / Computer Security Incident Response Teams

- Dedicated team|unit|resources for handling & managing security incidents
- A few types
  - National CERTs/CSIRTs
  - Organization / Enterprise CERTS/CSIRTs
  - Product CERTs (PSIRTs)
- Active community of CERTs/CSIRTs helping one another globally
  - Based on Trust

FIRST – Association of CERTs/CSIRTs

- Forum of Incident Response and Security Teams
- Not-for-Profit registered in the US
- Established in 1990
- 358 teams from 77 countries
  - Global in nature
  - Different Industry / Sectors

Global CERTs/CSIRTs Community



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

[credits]

FIRST Activities

http://www.first.org

- Education
  - Services Framework / CSIRT Maturity
  - Training for CERTs/CSIRTs
- Outreach
  - Engagement with members & other stakeholders
  - Network Operators, Government Agencies, Law Enforcement, Standard Bodies, RIR
- Fellowship – bringing new teams from developing economies into the community
- Events
  - Annual Conference
  - **Technical Colloquium**
  - Regional Symposia
- Special Interest Groups
  - Malware, Information Sharing, CVSS, Vulnerability Coordination,
  - Vendor SIG, Industrial Control Systems
- Projects
  - Global Incident Response Teams Database
    - https://api.first.org

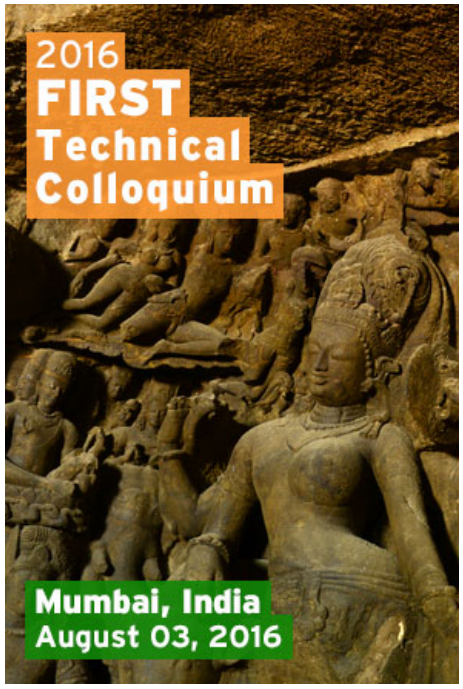
MISP Threat Sharing

$curl -i https://api.first.org/data/v1/teams?country=in&scope=country&field=team


```
{    "status": "OK",
     "status_code": 200,
    "version": "1.0",    "total": 1,
   "last-modified":
   "Fri, 24 Sep 2010 04:34:28 +0000",
   "data": [
        {          "id": "cert-in",
                   "team": "CERT-In",
                   "country": "IN",
                  "region": "Asia"
 }    ]}%
```


Check out: https://api.first.org & https://api.first.org/global-irt for more information

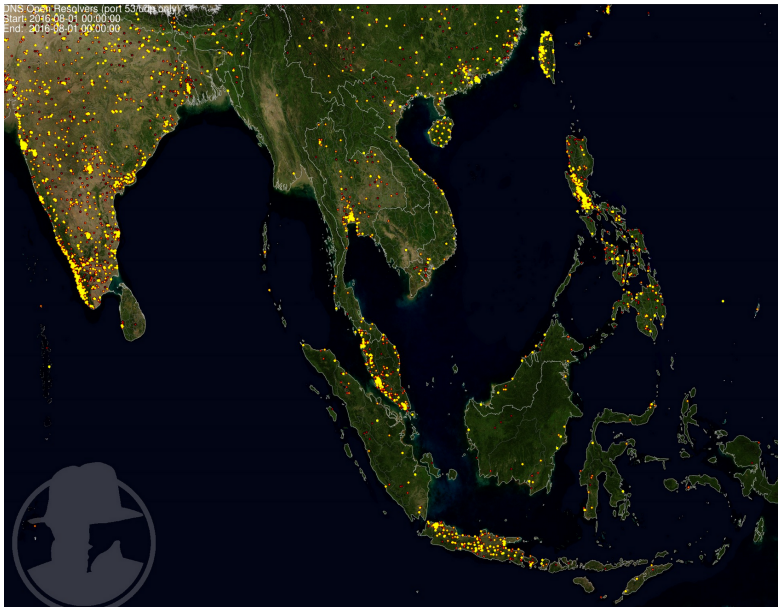
Increasing Awareness & Capabilities



- Many events are organized by members – majority are in Europe & North America
- Started to partner relevant organization to bring more activities to communities in South America, Africa, Asia & Oceania
- Recently TCs & Training at APRICOT/APNIC, LACNIC, AFRINIC events.
  - This week we are in SANOG!
- Encourage collaboration and information sharing between communities & stakeholders

Common Themes

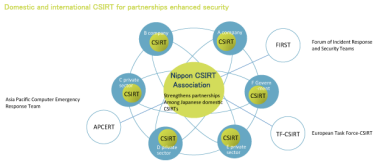
- Lessons Learned from Security Incidents
- Threat Landscape, Cyber Hygene
- Best Current Practices
- Tools for managing incidents, analysis, forensics
- Threat Intelligence & Information Sharing
- Incident Handling Drills, etc
- Check out past events
  - https://www.first.org/events/colloquia
  - https://conference.first.org



Open DNS resolvers
Source:http://www.shadowserver.org

Opportunities in the AP region

- CERT/CSIRT are mostly national teams
  - What about in enterprises?
  - Nippon CSIRT (JP)
    - http://www.nca.gr.jp/en/



- Lack of access to knowledge & expertise
  - More activities
  - More efforts
  - More awareness
  - Wearing Multiple Hats

- Looking forward to working with the SANOG community!
  - BCP38 / SAV

www.apcert.org

CSIRT Tutorial Afghanistan

Tonga CERT meeting

Thank You

Adli Wahid

adli@apnic.net
Twitter: @adliwahid

https://blog.apnic.net

http://www.first.org