CSIRT Establishment and Operation

Origin of CERTs

- 1988 Morris Worm Incident (10% of Internet capable computers, damages of $98 Million)
- Carnegie Mellon University formed world's first Computer Emergency Response Team / Coordination Centre (CERT/CC)
- Other countries recognized the need for in-country response capabilities, as use and importance of ICT increased
- Many National CERTs and Computer Security Incident Response Teams (CSIRTs) continue to appear

Reasons for the conception of Sri Lanka CERT

- Anticipated dramatic increase in the use of Information Communication technology for the provisioning of citizen services through e-Sri Lanka initiative, and corresponding increase in computer security incidents
- Inability of a large organization to run an effective, dynamic response capability internally (red tape, group dynamics, skill sets, etc)
- Independent, unbiased actions and assessments
- Formal Authority to coordinate response efforts and advise and educate on Information Security measures

Sri Lanka CERT's Mandate

"Sri Lanka CERT is to be the **national focal point** for cyber security in Sri Lanka.

It is to be recognized as the **single trusted source** of advice on the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from ***cyber attacks***."

About Sri Lanka CERT

- It is Sri Lanka's National CERT.

  There may be other CSIRTs in various sectors or organizations (e.g. Universities, Banks) which operate within the Sri Lanka CERT umbrella.

- APCERT and FIRST membership

About Sri Lanka CERT | CC

- Currently a non-profit organization dedicated to serving the Information Security needs of its constituency
- Small size allows for quicker response, decision making and lower overheads
- Sri Lanka CERT will assist industry sectors, such as banking, telecommunication and manufacturing to set up their own CSIRTs

Activity Classifications

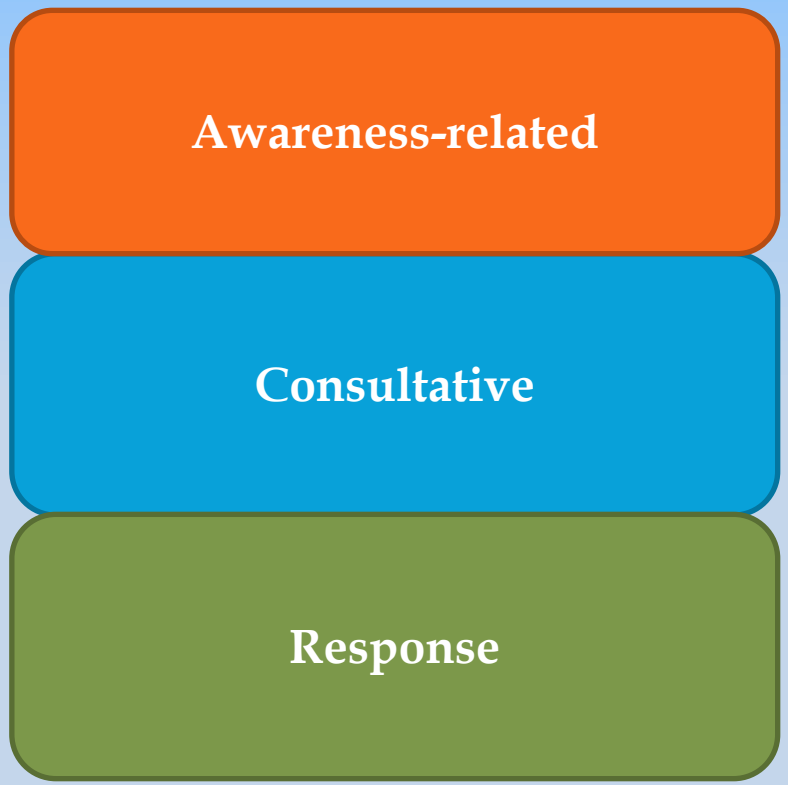
- Sri Lanka CERT's activities are classified as follows:
  - **Response**

    Triggered by events that are capable of having adverse effects on a constituent's Cyber Systems
  - **Awareness-related**

    These services are designed to inform and educate our Constituents on the importance of Information Security and related topics ranging from Information Security Fundamentals and best practices to more immediate issues, such as the latest cyber threats and attacks.
  - **Consultation**

    These services are aimed at providing Constituents with a means of determining the adequacy of their Information Security systems, and (if found necessary) to take necessary steps to strengthen their defenses.

Sri Lanka CERT Activities



- Workshops
- Knowledgebase
- Technology Watch
- Seminars & Conferences
- Alerts
- Sensor deployment
- Security reviews
- Advisory for IS Policy
- CSIRT Formation
- VAPT
- Digital Forensics
- Incident Handling

What is a security incident?

- Any real or suspected adverse event in relation to the security of computer systems or computer networks
- Unauthorized access
- Disruption or denial of service
- Unauthorized use
- Incident handling includes three functions: incident reporting, incident analysis, and incident response.
- ***Why would an organization need a CSIRT?***

What types of CSIRTs exist?

- CSIRTs come in all shapes and sizes and serve diverse constituencies.
- Some CSIRTs support an entire country, for example, the Sri Lanka Computer Emergency Readiness Team Coordination Center (Sri Lanka CERT/CC);
- others may provide assistance to a particular region, such as APCERT does for the Asia-Pacific area; Most of the CERTs in the Asia Pacific region are members of APCERT;
- still others may provide support to a particular university or commercial organization. FINCSIRT for Financial sector

APCERT

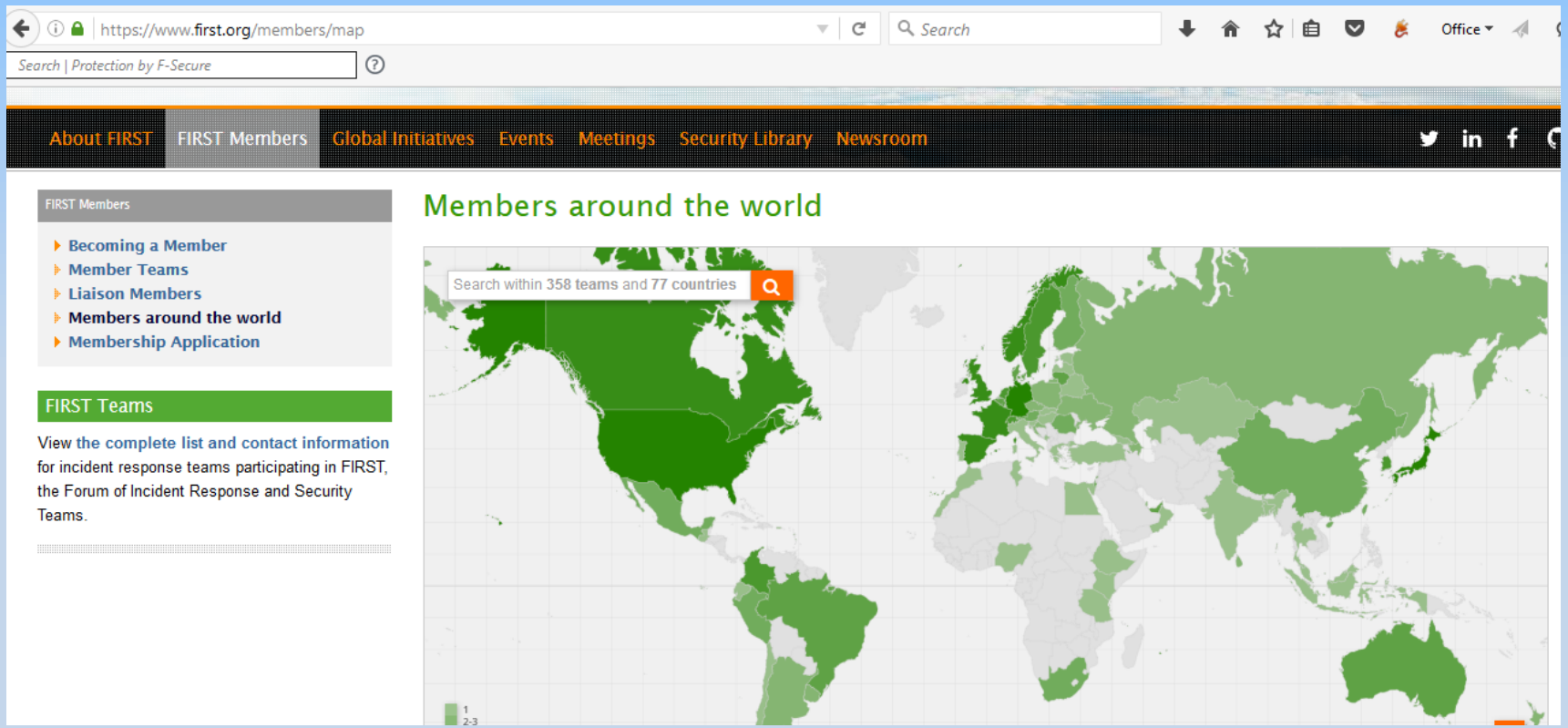
https://www.apcert.org/about/structure/members.html

Search | Protection by F-Secure

Operational Members (28 Teams / 20 Economies)

Team	Official Team Name	Economy	POC
AusCERT	Australian Computer Emergency Response Team	Australia	
bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh	X
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam	X
CCERT	CERNET Computer Emergency Response Team	People's Republic of China	
CERT Australia	CERT Australia	Australia	X
CERT-In	Indian Computer Emergency Response Team	India	X
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China	X
EC-CERT	Taiwan E-Commerce Computer Emergency Response Team	Chinese Taipei	
GovCERT.HK	Government Computer Emergency Response Team Hong Kong	Hong Kong, China	
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China	X

FIRST


https://www.first.org/members/map
Search
Search | Protection by F-Secure
Office
About FIRST
FIRST Members
Global Initiatives
Events
Meetings
Security Library
Newsroom
FIRST Members
Becoming a Member
Member Teams
Liaison Members
Members around the world
Membership Application
FIRST Teams
View the complete list and contact information for incident response teams participating in FIRST, the Forum of Incident Response and Security Teams.
Members around the world
Search within 358 teams and 77 countries