Building Incident Response Communities

The Forum of Incident Response and Security Teams (FIRST)

Cybersecurity: Cooperation and Information Exchange
Skopje, 09.10.2018

About me

Michael Hausding

- Member of SWITCH-CERT (Switzerland)
- Volunteer for FIRST.org
- Board Member of ISOC Switzerland Chapter
- Student of Internet Governance (Diplo Foundation)

Agenda

- What we want
- Introduction to FIRST
- Overview of projects and initiatives
- FIRST in 2020
- Questions and Answers

Incident Response in a nutshell

CSIRTs collaborate informally

They need a high level of trust

Who are we?

- Association of Incident Response and Security Teams
- Founded in 1989

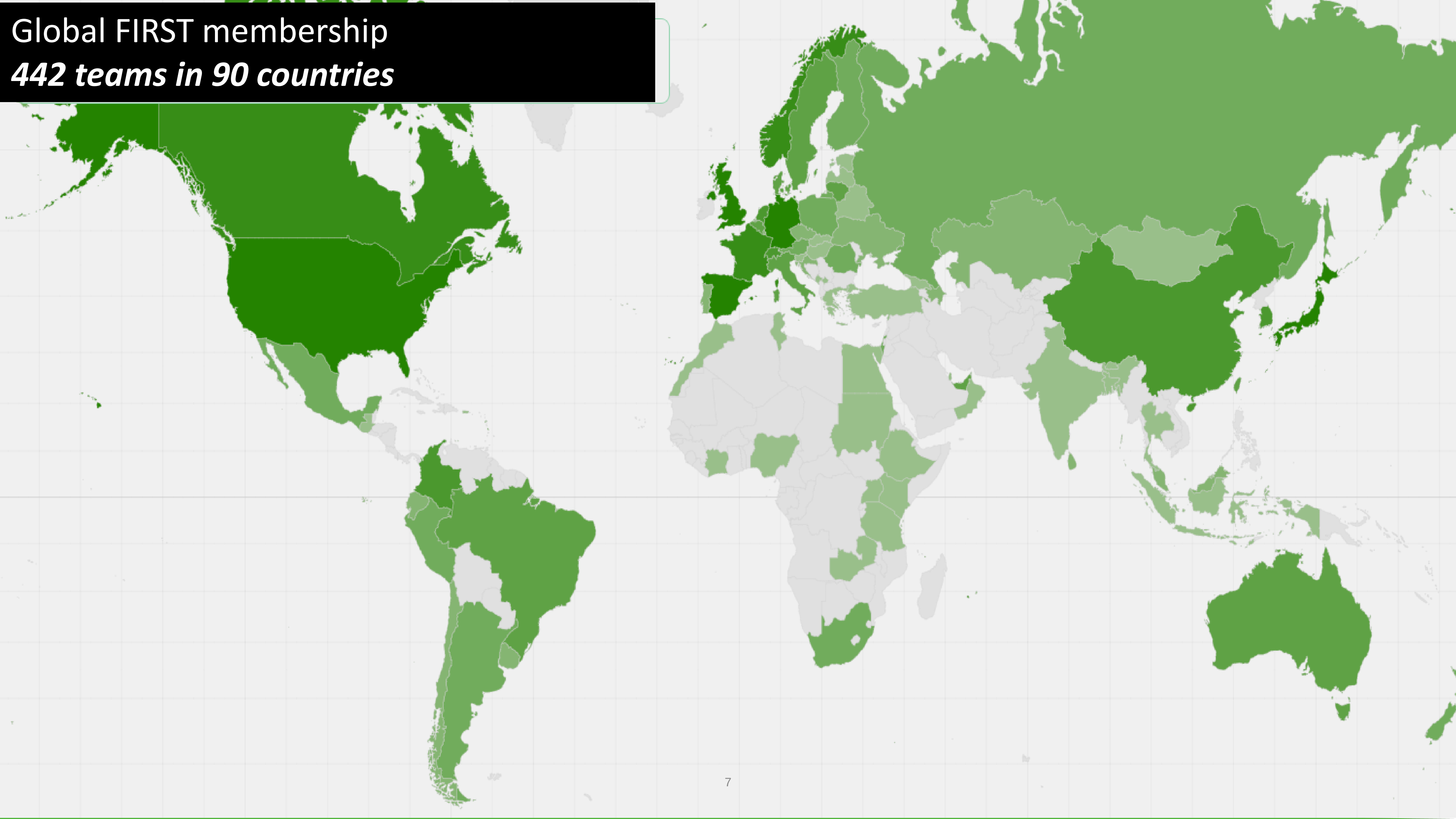
- We enable incident responders
  - To **engage with their peers**
  - To have a **shared understanding** of security problems
  - By developing **technologies and standards**
  - By foster an **environment conductive to their work**

Mission

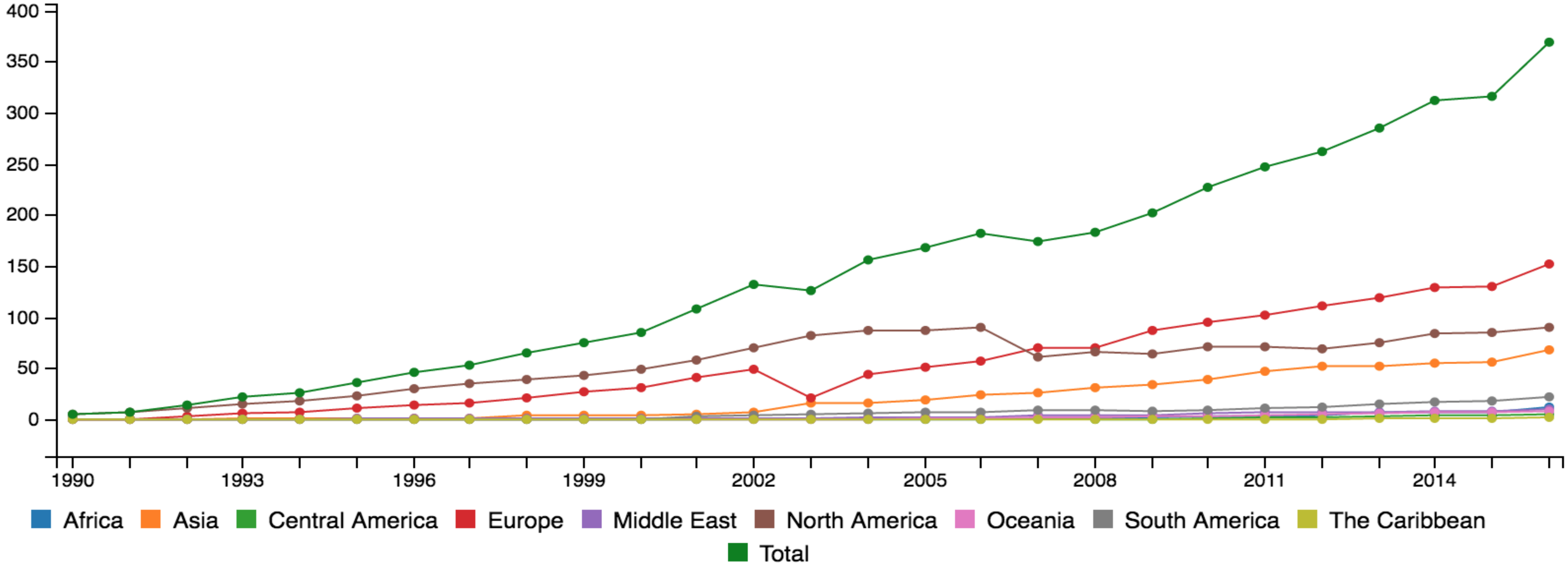
- Every **FIRST member can successfully find a FIRST member** to work with during any incident, whether in another country or industry.
- **FIRST teams know they can rely on FIRST teams**, and know they are capable partners to work with.
- When FIRST members trust each other, they have **a toolset** they can use to share.
- FIRST teams can work in an **environment conductive to their goals**.

Global FIRST membership

442 teams in 90 countries

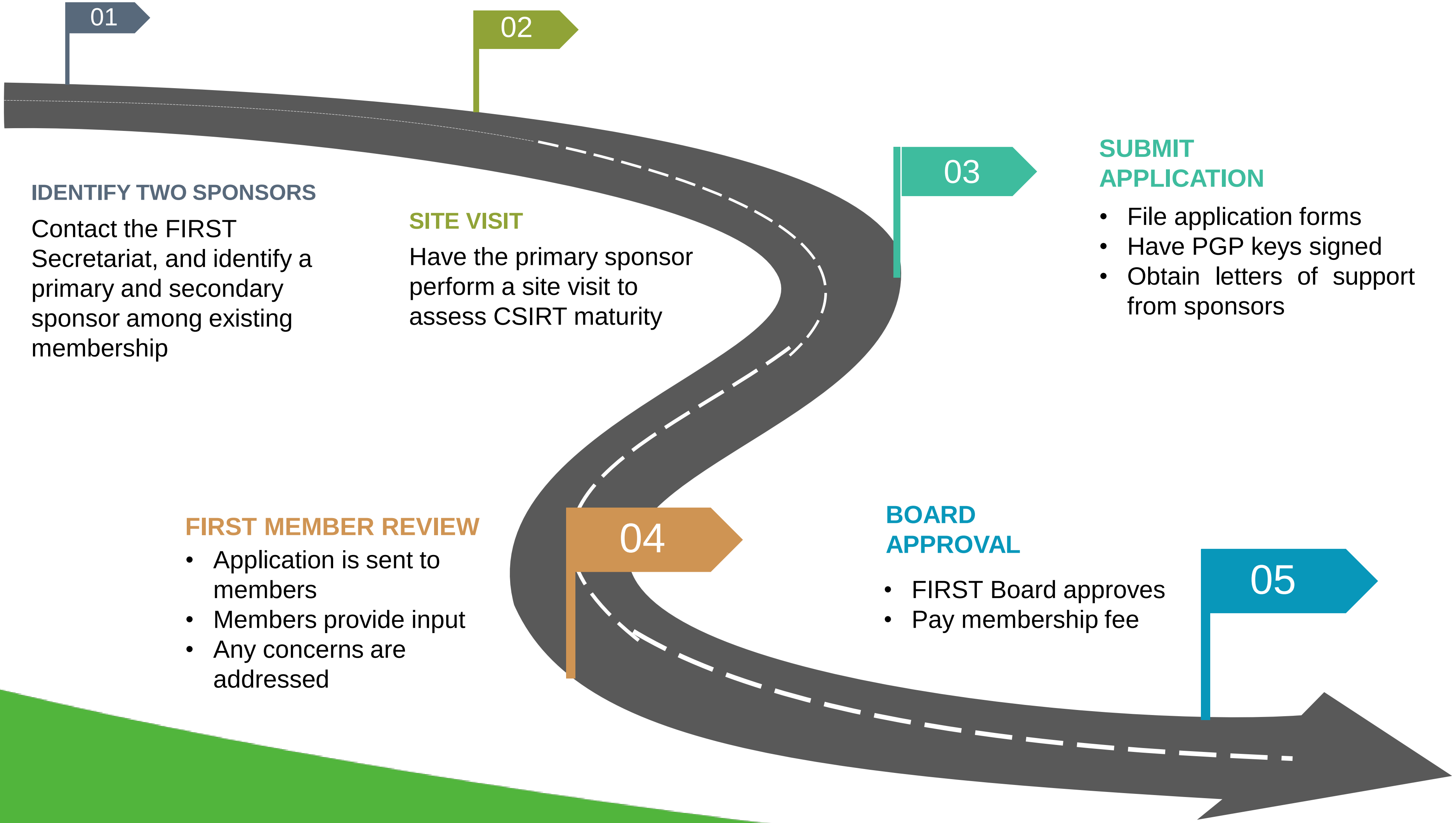


Membership



400
350
300
250
200
150
100
50
0
1990
1993
1996
1999
2002
2005
2008
2011
2014
Africa
Asia
Central America
Europe
Middle East
North America
Oceania
South America
The Caribbean
Total

Membership application process



IDENTIFY TWO SPONSORS

Contact the FIRST Secretariat, and identify a primary and secondary sponsor among existing membership

SITE VISIT

Have the primary sponsor perform a site visit to assess CSIRT maturity

SUBMIT APPLICATION

- File application forms
- Have PGP keys signed
- Obtain letters of support from sponsors

FIRST MEMBER REVIEW

- Application is sent to members
- Members provide input
- Any concerns are addressed

BOARD APPROVAL

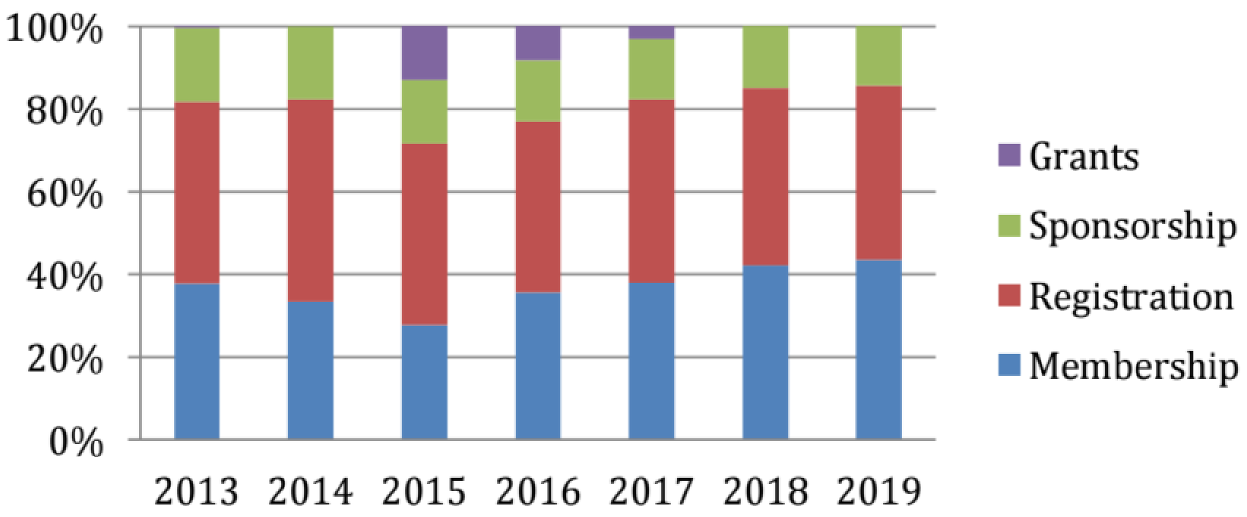
- FIRST Board approves
- Pay membership fee

Fellowship Program

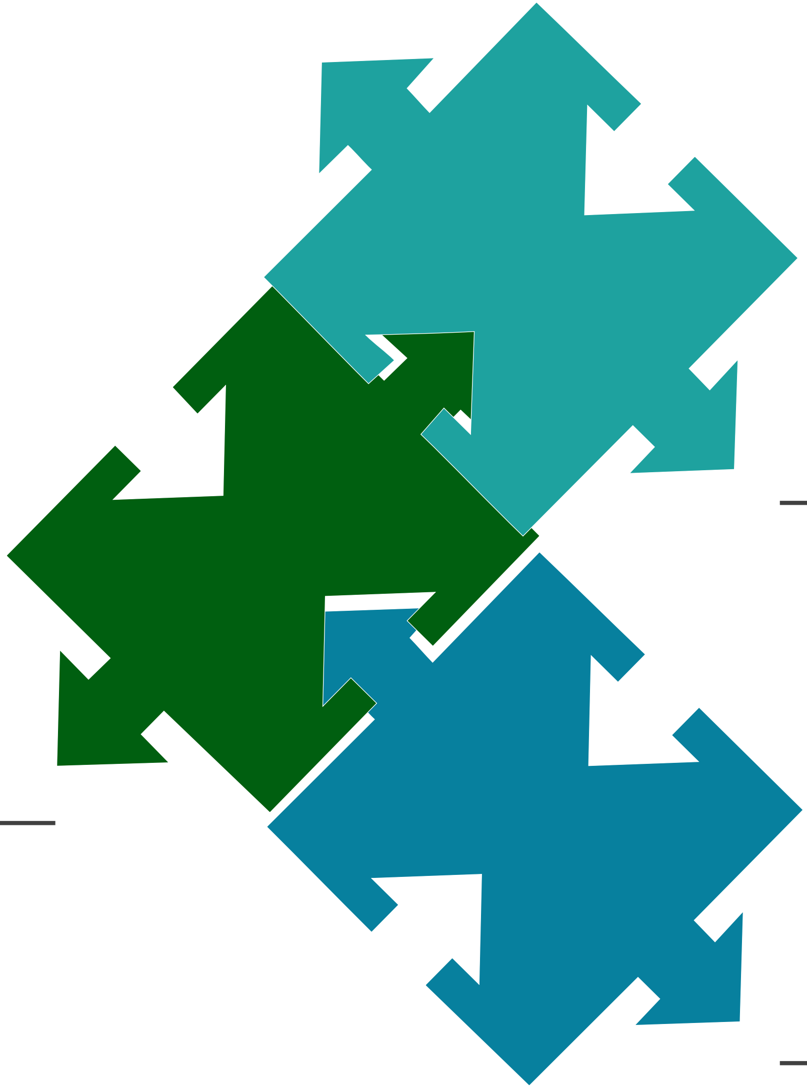
- FIRST **funds participation** for up to four new teams each year
- Open to CSIRTs with some **level of national responsibility**

FIRST as an organization

- Lead by a 10-person **Board of Directors**, elected by Members
- No headquarters, but **secretariat** in Chicago
- **501c3 non-profit** incorporated in the United States
- Funded primarily through membership and conference fees



Events



30th ANNUAL FIRST CONFERENCE
KUALA LUMPUR
June 24-29, 2018

Conference

- Flagship event
- Once per year, travels between regions
- ~500-800 attendees

2017
FIRST-ITU
Regional Symposium
for Africa and
Arab Regions
Dar es Salaam, Tanzania
November 13-17, 2017

Symposia

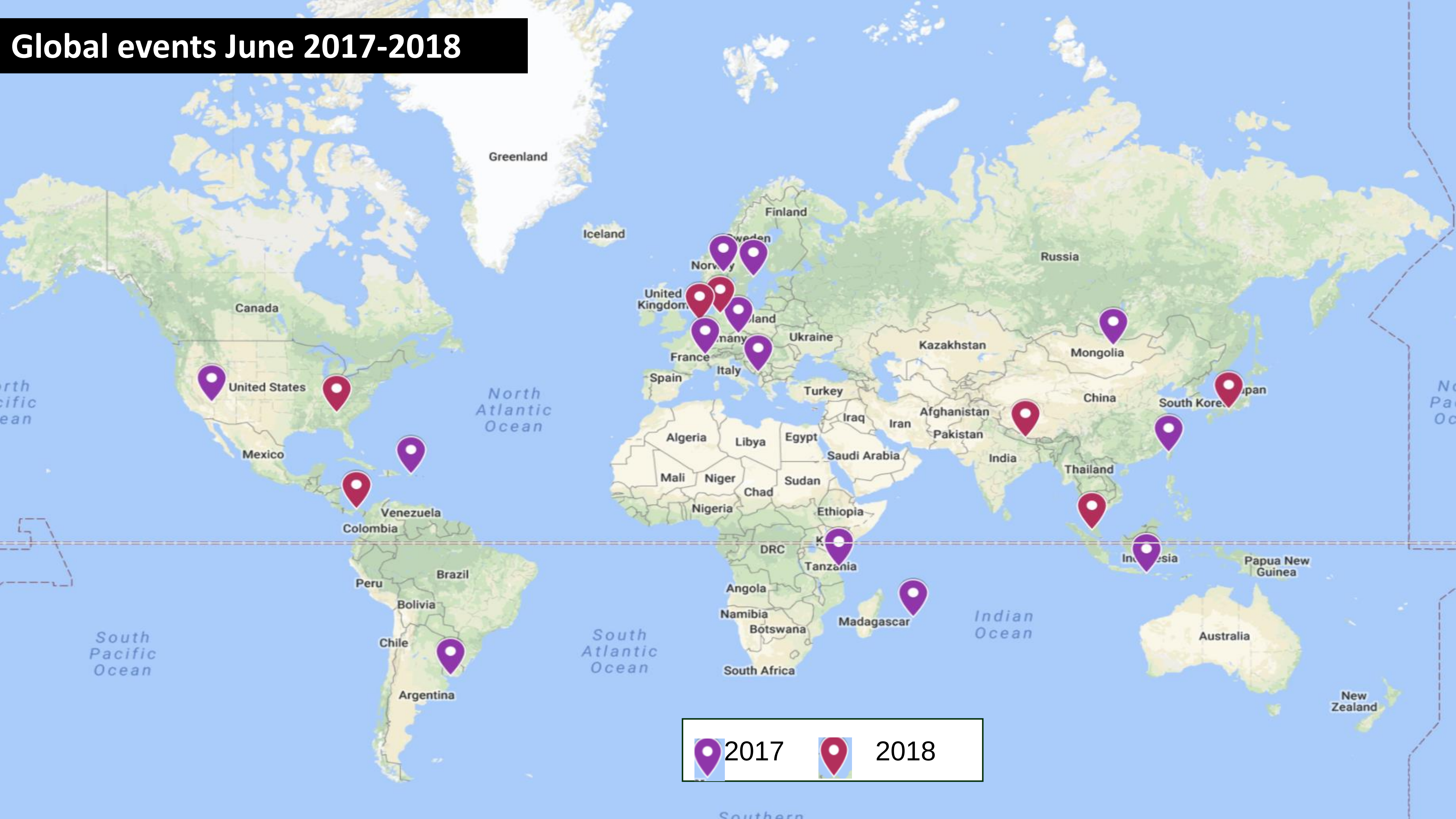
- Four per year
- In each major region (Africa, Europe, Latin America, Asia)
- Hosted by FIRST and often a partner

2017
UNDP/FIRST
Technical
Colloquium
Podgorica, ME
Nov 07-09, 2017

Technical Colloquium

- Organized by individual members
- National or regional event
- Typically 10-15 events per year

Global events June 2017-2018



Training and Education

- FIRST maintains a **CSIRT and PSIRT Services Framework**
  - Details all services typically offered by CSIRT
  - Offers a roadmap and guide for CSIRT as they expand capability
- FIRST **develops training materials** for individual services
  - CSIRT Fundamentals, Incident Coordination, Information Sources
  - All materials are Creative Commons licensed and available for free
- FIRST **delivers training** with partners and at events
  - Roster of trainer-practitioners

Special Interest Groups

- Convene members around topics of common interest
- Often have a formal charter, timeline and deliverables

- Types of SIGs:
  - **Working groups:** Big Data, Ethics, Red Team
  - **Standards groups:** CVSS, IEP, TLP, Passive DNS exchange
  - **Discussion groups:** Vendors, Metrics, Industrial Control Systems
  - **Bird of a Feather session:** legal issues, specific temporary topics

Standards

CVSS

Common Vulnerability Scoring System

- Scoring system for software vulnerabilities
- Allows integration of environmental factors
- Interactive training

Traffic Light Protocol

- Allows data senders to encode how information may be distributed
- Focused on human sharing, simple to use

TLP

IEP

Information Exchange Protocol

- More fine grained specification of **Handling**, **Action**, **Sharing** and **Licensing** policies
- Focused on machine sharing (JSON)

Passive DNS

- Enable easier sharing of passive DNS information
- Standard contributed to the IETF

Passive DNS

Technical resources

Membership database

A FIRST member database with contact information for incident responders at other members. **Including PGP keys.**

FIRST Incident Response Team API

Poll information on other members using a **public API**.

Malware Information Sharing Platform

Share machine-parseable incident descriptions with members using the **MISP platform**.

Mailing lists and IRC

Immediate communications channels with other FIRST members.

Internet Governance and Policy

- Be a **trusted security expert** to the policy community
- FIRST regularly participates in policy forums, such as the Internet Governance Forum, Global Conference on Cyberspace to educate policy makers on incident response
- Lead experts to the **IGF Best Practices Forum on Cybersecurity**
- Help **develop technology expertise** and capability

Partners

- Partners share our vision of a strong incident response community

OIC-CERT
Computer Emergency Response Team

ITU

ORGANIZATION OF AMERICAN STATES
OAS
More rights
for more people

GÉANT

GFCE
Global Forum on Cyber Expertise

lacnic

ICT for peace foundation

APNIC

FIRST Annual Meeting 2019

Questions?

first-sec@first.org
https://www.first.org