



The Forum of Incident Response and Security Teams (FIRST)

Agenda

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

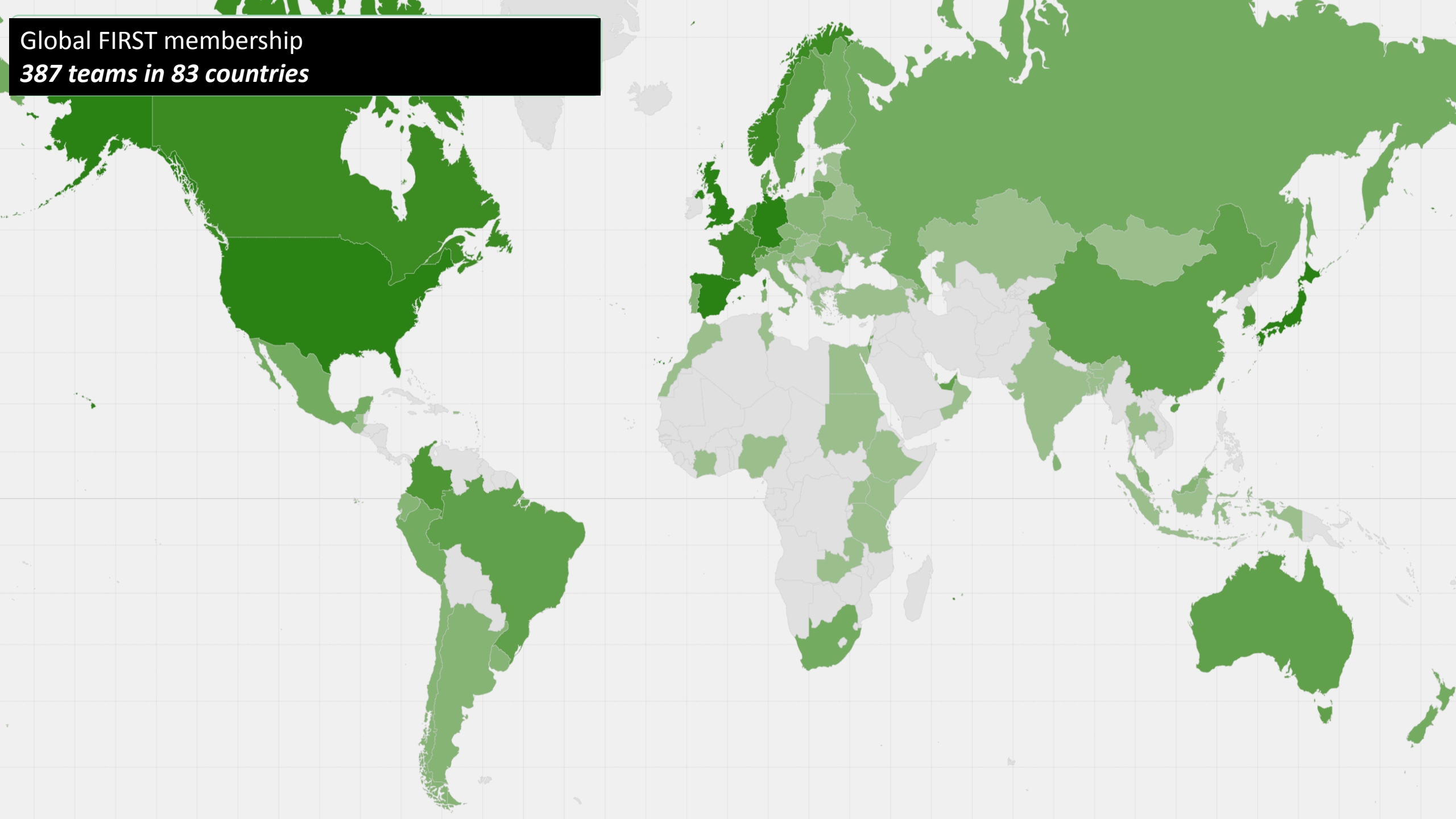


Who are we?

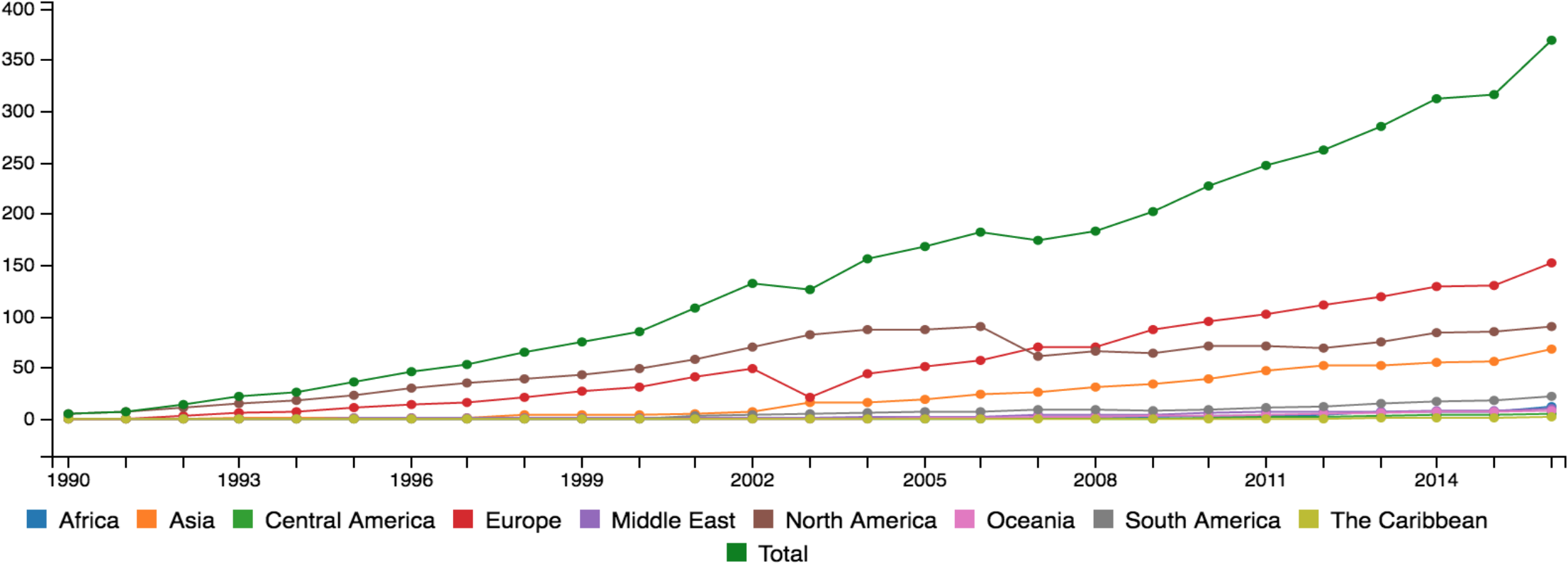
- Association of Incident Response and Security Teams
- Founded in 1989
- We enable incident responders
 - To **engage with their peers**
 - To have a **shared understanding** of security problems
 - By developing **technologies and standards**



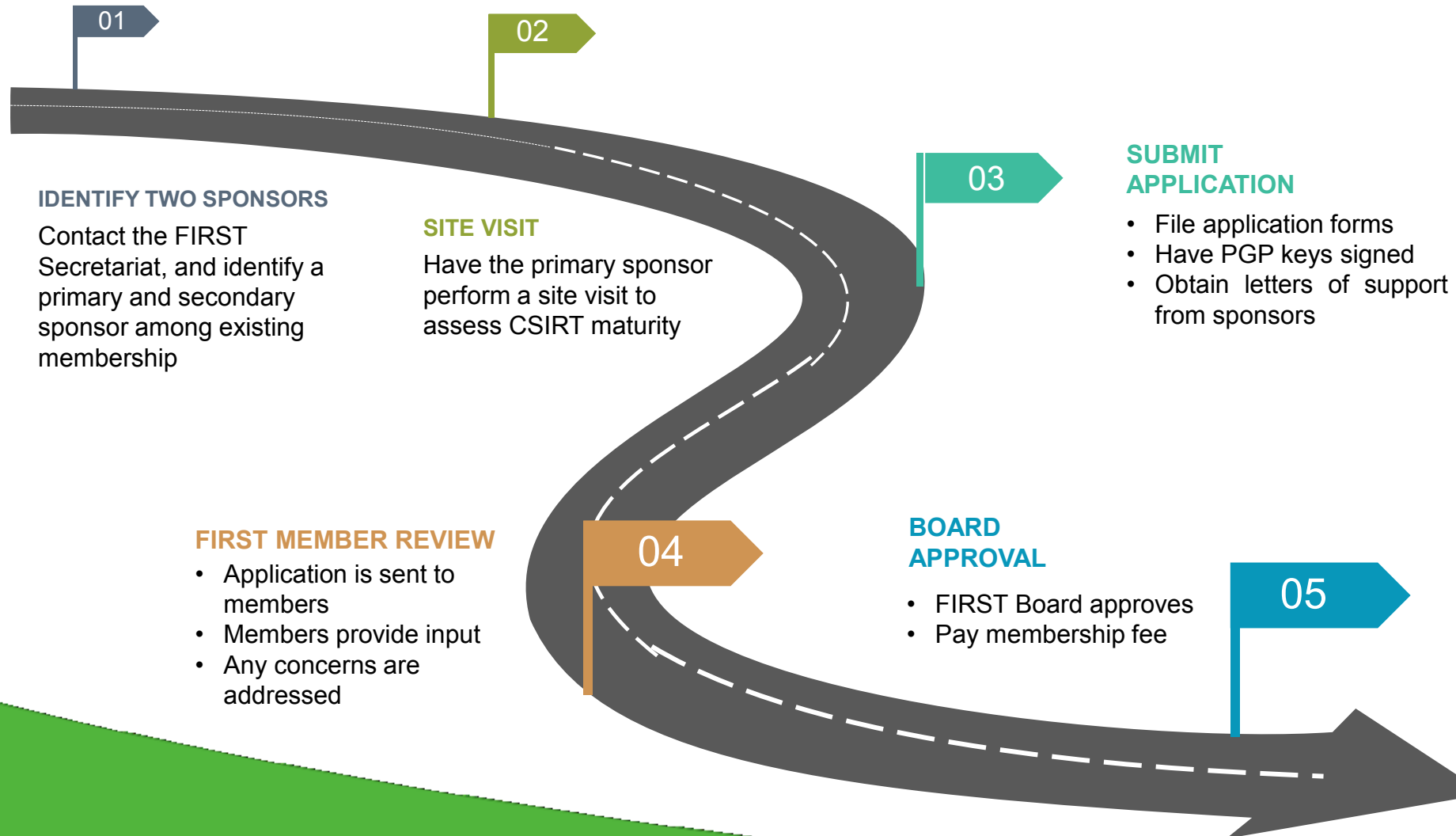
Global FIRST membership
387 teams in 83 countries



Membership



Membership application process



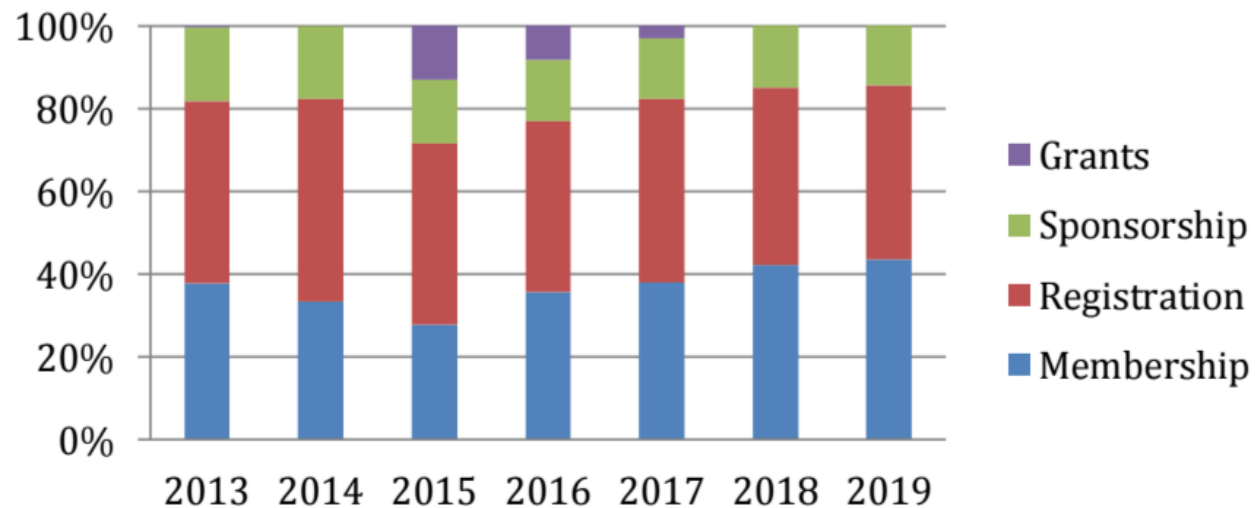
Fellowship Program

- 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



Symposia

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



Conference

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



Technical Colloquium

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



Global events 2016-2017



FIRST activity across the world:  Training classes  TC's and Symposia  Annual conference 2017,

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



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

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

TLP

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





FIRST Annual Meeting 2018

Questions?

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

