Education Program

About FIRST

Founded in 1990, the Forum of Incident Response and Security Teams (FIRST) consists of internet emergency response teams from more than 360 corporations, government bodies, universities and other institutions across 78 countries in the Americas, Asia, Europe, Africa, and Oceania. FIRST is the largest global association of incident response teams, and builds capability by organizing events, organizing training and supporting its members in developing standards. FIRST is incorporated as a 501c3 non-profit in North Carolina, USA.

FIRST and Education

Ensuring CSIRT teams are well trained is a prerequisite for FIRST to be successful in its mission. Security incidents rarely occur in isolation, and in order to effectively respond, incident responders need to be able to find viable partners in the network where the attack originates, or through which it transits.

Incident Response has taken a prominent place as countries implement cyber security risk frameworks incorporating response mechanisms. Although there are an increasing number of incident response teams, nations and critical infrastructures as well as enterprises in all areas of the world need both to join the communities of trust and to attain maturity in their operations.

FIRST Education is aimed at ensuring well trained, responsive partners exist wherever needed to mitigate an information security threat. FIRST has historically organized third party training at its events. Professionalizing this effort, in 2013, FIRST signed a Memorandum of Understanding with TERENA, authors of the TRANSITS CSIRT training, enabling FIRST to coordinate TRANSITS training outside of Europe.

In 2014, FIRST announced the initiation of the FIRST Education Program. As part of this initiative, FIRST is convening community members to assist in steering the development of a comprehensive CSIRT training framework. FIRST will develop a services training curriculum based on this framework. The program was initiated with internal seed funding from FIRST of $500,000 and funding by interested partners.

FIRST Education will aim to develop capability, capacity and maturity.

- ***Capability –*** *Can you do it?* A capability defines a measurable activity that may be performed as part of an organization's roles and responsibilities. For the purpose

of the CSIRT services framework the capabilities can either be defined as the broader services or as the requisite tasks, sub-tasks or functions.

- ***Capacity –*** *How much can you do?* Capacity defines the number of simultaneous occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

- ***Maturity –*** *How well can you do it?* Maturity defines how effectively an organization executes a particular capability within the mission and authorities of the organization.

While FIRST will continue to partner and deliver third party training as needed, the CSIRT Education Program aims to **address gaps** and **ensures training is available to teams for their own internal training**, to **help them train their business partners**, and for **capacity building** in both underrepresented regions and industries.

Development will take place across four phases:

- Development of a high level framework;
- Training development;
- Training delivery;
- Regular framework and training review.

Development of a high level framework

From 2014 through 2016, FIRST convened a set of summits, during which the outline of the program was developed. These summits included participants from 15 countries across six continents, and involved the national CSIRT community, and information security educators. Starting 2015, FIRST also convened education summits that involved more private sector participation.

This series of summits is intended to lead to a final version of a CSIRT Services Framework, which will specify the services offered by CSIRT to its constituents. An initial draft was published for public comment on April 30th, 2015. Based on this framework, more detailed tasks and sub-tasks will be specified by FIRST and its community participants. These tasks were used as initial input for FIRST to develop training courses.

The framework is being developed according to these tenets:

- FIRST will create an **inclusive community of incident responders and education professionals** to have comprehensive debates about the direction of the effort. FIRST will gradually enlarge the steering group to involve participants from the national CSIRT community, as well as industry and academia;

- FIRST will endeavor to be representative of all regions and industries during framework development, and **ensure the final product is useable regardless of industry, culture and geographical location**;
- FIRST will **seek third party funding and partnerships** to ensure scalability.

Training development

FIRST has developed and maintained a set of basic training courses, which include:

- **FIRST CSIRT Basic Course:** These six modules teach new teams the basics of CSIRT work. Founded on the FIRST CSIRT Framework, this training helps new teams to establish themselves and get basic services running. Each module is accompanied by an extensive Lab session focused on applying the introduced concepts
- **FIRST Fusion course:** This course helps incident response professionals determine the methods and techniques needed to analyze and fuse information. It provides them with the tools needed to identify relationships and commonalities amongst the data, ultimately helping their business or organization to better respond to security threats

Initial development will be expanded based on the community input gathered during the framework development, and will be extended with additional courses based on community needs.

Where a good fit, FIRST will adopt third party materials rather than developing new materials. However, all intellectual property must finally be owned by FIRST, in order to enable us to ensure it remains relevant and updated, and can be made available at no cost to the community. Providers of certified training materials will be listed on the FIRST web site.

Training will be developed according to these tenets:

- Within a maturity model to be developed as part of the education framework, **FIRST will develop basic and intermediate level training**, but leave advanced training up to commercial providers;
- FIRST Training will be **focused on the team**, rather than the individual, in order to address the need for incident response team development;
- All **FIRST training materials will be released to the community at no cost**;
- FIRST will use several partners to develop the materials, but will leverage its community resources for **quality assurance**. All materials will be reviewed at least once every three years.

Training delivery

Delivery of training will take place both by FIRST and its partners.

Training will be delivered according to these tenets:

- While materials are available at no cost, training provided by FIRST will be **delivered at low cost**, ensuring participation and the scalability of the effort;
- Training will be delivered in **close partnership with FIRST partners to address community needs**. Focus will be on developing CSIRT capability in areas and industries where it is least present today.
- FIRST members and non-members will be able to leverage materials to provide training in house. FIRST will provide resources to enable self-training, but **for public training will develop a quality assurance and certification mechanism** so the quality of any delivery of a FIRST course is high.
- **FIRST will leverage experts with real world experience to provide training**. When actual incident responders teach, attendees don't just learn, but they connect with a wider community.
- When content is delivered on behalf of FIRST, FIRST will provide **paid transportation, accommodation and per diem** in accordance with our travel policy to approved instructors.

Contact information

Updated information on the program can be found at:
https://www.first.org/global/education

The FIRST Education Program is operated as an initiative of the Forum for Incident Response and Security Teams, under the auspices of the FIRST Board of Directors. For more information, contact the FIRST education team at first-educ@first.org.