The Forum of Incident Response and Security Teams (FIRST)

Dr. Serge Droz
Chair, Board of Directors
serge.droz@first.org
Agenda

- What we want
- Introduction to FIRST
- Overview of projects and initiatives
- FIRST in 2020
- Questions and Answers
Historical map of trade routes, Library of the University of Texas at Austin
State of Cyberspace

Access to knowledge

Collaboration

Prosperity
State of Cyberspace

SUSTAINABLE DEVELOPMENT GOALS
Threats

Criminals

Disinformation

States

Hate

Surveillance
Remedies

Norms

Education

Incident Response
Remedies

Norms

**GGE 2015**

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.
Incidents are global

**Diginotar:** National Crisis in NL, Discovered by Iranian User, Reported by Germany, dependance on US, Victims in Iran
Trust inhibitors

- Hidden Agendas
- Placing the CERT in the wrong spot
- Sanctions
Trust inhibitors: Wrong spot

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. **A State should not use authorized emergency response teams to engage in malicious international activity.**
Trust inhibitors: Sanctions
FIRST
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
**Global Coordination:** In an emergency you can always find the teams you need to support you in our global community.

**Global Language:** Incident responders around the world speak the same language and understand each other’s intents and methods.

**Automation:** Let machines do the boring calculations, so humans can focus on the hard questions.

**Policy and Governance:** Make sure others understand what we do, and enable us rather than limit us.

**FIRST’s Mission**
Global FIRST membership

495 teams in 92 countries
Membership application process

1. **IDENTIFY TWO SPONSORS**
   - Contact the FIRST Secretariat, and identify a primary and secondary sponsor among existing membership

2. **SITE VISIT**
   - Have the primary sponsor perform a site visit to assess CSIRT maturity

3. **SUBMIT APPLICATION**
   - File application forms
   - Have PGP keys signed
   - Obtain letters of support from sponsors

4. **FIRST MEMBER REVIEW**
   - Application is sent to members
   - Members provide input
   - Any concerns are addressed

5. **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 organisation

- 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

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

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

Technical Colloquium
- Organized by individual members
- National or regional event
- Typically 10-15 events per year
Global events August 2017-2018

- FIRST Events
  - Annual Conference
  - Symposia
  - TCs
  - Training Courses
  - Outreach
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
Scoring system for software vulnerabilities

- Allows integration of environmental factors
- Interactive training

Common Vulnerability Scoring System

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

Traffic Light Protocol (TLP)

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

IEP

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

Passive DNS

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

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

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

**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 share our vision of a strong incident response community
<table>
<thead>
<tr>
<th>Time</th>
<th>Talk</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00</td>
<td>Welcome</td>
<td>Serge Droz</td>
</tr>
<tr>
<td>9:30</td>
<td>Remediation Ballet: Choreographing your team to victory</td>
<td>Simon Freiberg and Jason Solomon (Google)</td>
</tr>
<tr>
<td>10:30</td>
<td>Integrating red teaming and CSIRT</td>
<td>Jordi Aguilà (e-la Caixa CSIRT, ES)</td>
</tr>
<tr>
<td>11:00</td>
<td>Coffee break</td>
<td></td>
</tr>
<tr>
<td>11:15</td>
<td>A Field Guide to communicating a security incident</td>
<td>Izzi Lithgow (CERT NZ)</td>
</tr>
<tr>
<td>12:00</td>
<td>DFIR Acquisition presentation</td>
<td>Sam Bonanno (ACSC)</td>
</tr>
<tr>
<td>12:30</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Talk</td>
<td>Presenter</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>13:45</td>
<td>The Policy Implications of Incident Response</td>
<td>Maarten Van Horenbeeck (Zendesk), Serge Droz (OS-CERT)</td>
</tr>
<tr>
<td>14:45</td>
<td>IR using Jupyter Notebooks</td>
<td>Serge Droz (OS-CERT)</td>
</tr>
<tr>
<td>15:15</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>15:30</td>
<td>Measuring CSIRT Maturity using SIM3</td>
<td>Maarten Van Horenbeeck (Zendesk)</td>
</tr>
<tr>
<td>16:00</td>
<td>Responding to Incidents in Industrial Environments</td>
<td>Hinne Hettema (Port of Auckland, NZ)</td>
</tr>
<tr>
<td>17:00</td>
<td>Closing remarks</td>
<td>Serge Droz (OS-CERT)</td>
</tr>
<tr>
<td>19:00</td>
<td>Networking reception - Sandy Court @ Westin Denarau Fiji Resort</td>
<td></td>
</tr>
</tbody>
</table>
## And our training days

<table>
<thead>
<tr>
<th>Wednesday, November 6th 2019</th>
<th>Thursday, November 7th 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach workshop 1: Cyber Extortion</td>
<td>CSIRT Basic Training - Part 1</td>
</tr>
<tr>
<td>Adli Abdul Wahid (APCERT)</td>
<td>Maarten Van Horenbeeck (Zendesk)</td>
</tr>
<tr>
<td>Frangipani (Ballroom B)</td>
<td>Frangipani (Ballroom B)</td>
</tr>
<tr>
<td>Breach workshop 2: Critical Infrastructure Attack</td>
<td>CSIRT Advanced Training - Part 2</td>
</tr>
<tr>
<td>Serge Droz (OS-CERT)</td>
<td>Serge Droz (OS-CERT)</td>
</tr>
<tr>
<td>Gardenia (Ballroom C)</td>
<td>Adli Wahid (APNIC)</td>
</tr>
<tr>
<td></td>
<td>Gardenia (Ballroom C)</td>
</tr>
<tr>
<td>Malware Analysis When You’re in A Hurry</td>
<td>CSIRT Basic Training - Part 1</td>
</tr>
<tr>
<td>Hinne Hettema (Port of Auckland)</td>
<td>Maarten Van Horenbeeck (Zendesk)</td>
</tr>
<tr>
<td>Frangipani (Ballroom B)</td>
<td>Frangipani (Ballroom B)</td>
</tr>
<tr>
<td>CSIRT Advanced Training - Part 1</td>
<td>CSIRT Advanced Training - Part 3</td>
</tr>
<tr>
<td>Serge Droz (OS-CERT)</td>
<td>Serge Droz (OS-CERT)</td>
</tr>
<tr>
<td>Adli Wahid (APNIC)</td>
<td>Adli Wahid (APNIC)</td>
</tr>
<tr>
<td>Gardenia (Ballroom C)</td>
<td>Gardenia (Ballroom C)</td>
</tr>
</tbody>
</table>
Guest Facilities

- Sandy Point
- 1501 - 1578
- 1401 - 1476
- 1301 - 1374
- 1201 - 1227
- 1101 - 1181
- 1601 - 1681
- 1863 - 1869
- 1813 - 1819
- 1851 - 1861
- 1801 - 1811
- 1821 - 1835
- 1871 - 1885

Guest can charge costs at all Sheraton and Westin Resorts and the Denarau Golf & Racquet Club back to their rooms.

A regular shuttle service runs between Sheraton and Westin Resorts. The shuttle bus stops will provide information on hours of operation.
This could be the beginning …
Questions?

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