Visualization of Network Flow Data

Network flow data has very low information content; consequently you need a lot of data, or need to know something specific about it. We introduce three methods or reasons to visualize such data: Descriptive, Retrospective Analysis and exploratory.

**Describe**
What's happening? What's typical? See the big picture.

**Analyze**
Something happened. Describe it. Who, what, where, when…? Profile a network or a host IP

**Explore**
I can describe Activity X in network terms, can I find instances of it occurring? Look for anomalies

---

**Generic data preparation process**
- Get raw data
- Process into what we want
- rwfilter
- Render into Vis
- Vis

**SilK and Rayon data preparation process**
- Prepare proper format
- recount, reusing, restats
- sort
- rycategories, rytimeseries...
- Vis.png

**Youtube traffic: one sensor eight days**

---

**How to get the data you need with SilK**

---

http://www.cert.org/flocon