Carnegie Mellon
Software Engineering Institute

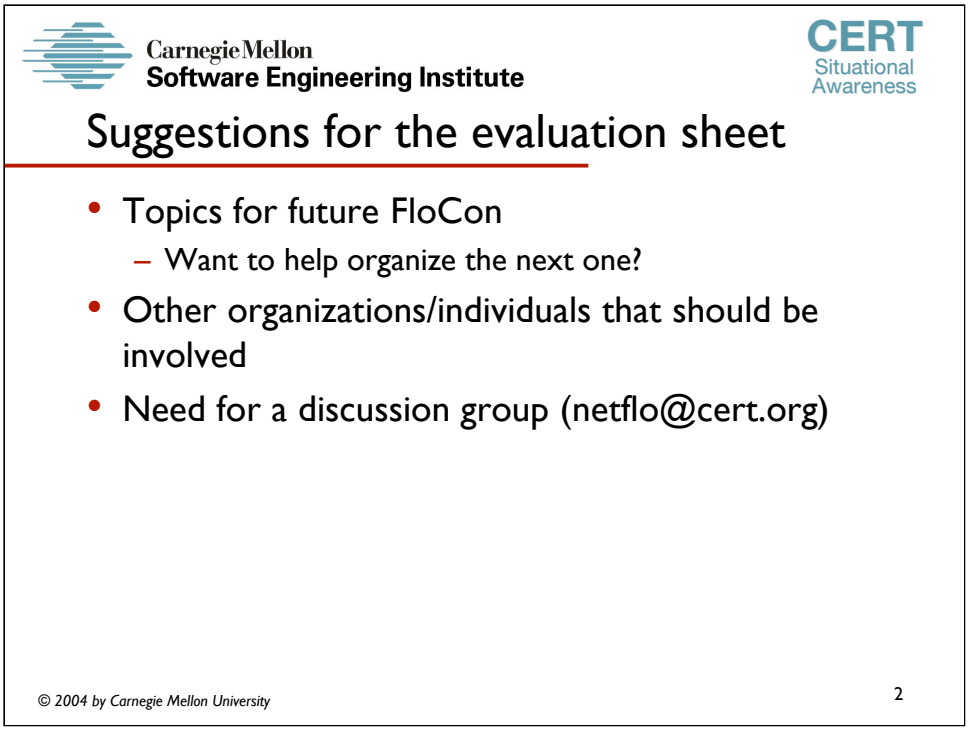
CERT
Situational
Awareness

Wish List

Tom Longstaff

CERT® Network Situational Awareness Group
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

The CERT Network Situational Awareness Group is part of the Software Engineering Institute. The Software Engineering Institute is sponsored by the U.S. Department of Defense.



JTF,

DoE thread in the DoE security conference – add research from DoE labs

U. Of Ill. – cisco wants to be involved. ARGUS developers

CAIDA – program committee format. Not one organization. More operational folkes ATT Sprint, etc.

CERT
LE FBI. Nanog – ISP SEC BoF

ACSAC – Dec conference on collecting network data. Offered on the Tues of ACSAC

Webcast? – not usually done.

Moving too fast to wait a year.

Tech exchanges with regionals

Good group and open discussions between sessions

Architecture session – everyone gets 5 minutes to present

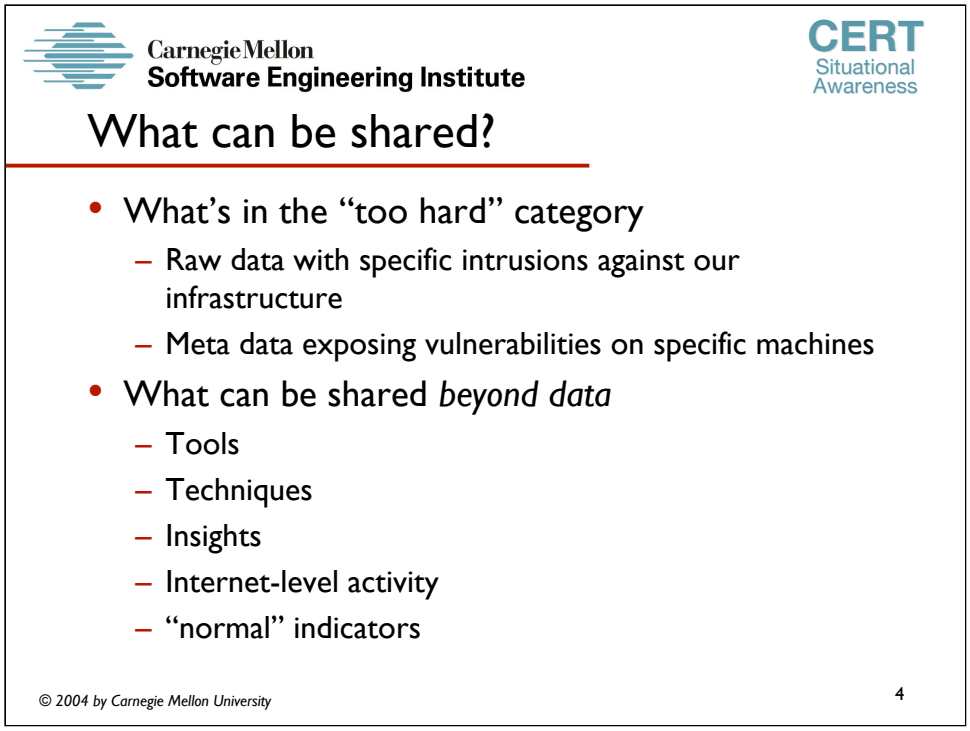
Ask for a 2 page position paper. Forms a proceedings.

Carnegie Mellon
Software Engineering Institute

CERT
Situational
Awareness

What do you want from Netflow?

- Distribution of flags
- Payload hash
- Start/End packet
- IPV6
- MPLS
- Eval network changes on netflow implementation
- IP packet frags
- Sizing characterization (mean/packets vs packet size)
- Methods of data reduction (sampling, compression, etc)
- ICMP data



Typical use/sharing policies (library of popular ones)

Obfuscation techniques (without destroying the utility of analysis – may be in the too hard list).

Bad lists/top hit lists/top "n" lists

Spikes (security portal for port/packet volumes)

Queries (to an oracle)

Representations of what you're not seeing (filter rules)

Algorithms we can run on summary data (merging data queries)

How to share others data that shows up in your collection.

Time factors (real time vs historical)

Common modal failures

Attribution information (whois type data) meta data – perhaps all who have the need can make a contribution.

Accurate Geo-location information (techniques, methods, etc – false flag issue, practice, triangulation of multiple sources).

Visualization tools – tool demo session (for workshop?)

CISCO efforts for certs in packets (user to service to server authentication) tracked in Netflow.

Practices (where they can be shared)

Protocols to observe (BGP, etc)

Find more protocols of interest – identify the individuals to the group

Place for people to make comments. Usage and other information.

Domain knowledge to reference.

User interface/easily used flow tools. Faster ramp-up time. Automating low-hanging fruit to make easily tracked traffic automated. Build to more sophisticated environments. "65% of all inbound traffic hitting the router is blaster." Reporting tools. Results that can be understood by sponsors. Goal to change the policy. For DoD, DoE, other… need value that netflow is bringing compared to other technologies. Why to invest?

Share to survive the program. ROI and network situational awareness.

Integration of these tools (framework?)

Issues:

New analysts (mchugh to share tutorial). KB pulled together. Language related to netflow terminology (ala google).

Managers up to speed

Making a general case

Secure portal to get results on your data from others.

Set of specific examples of interesting behavior.

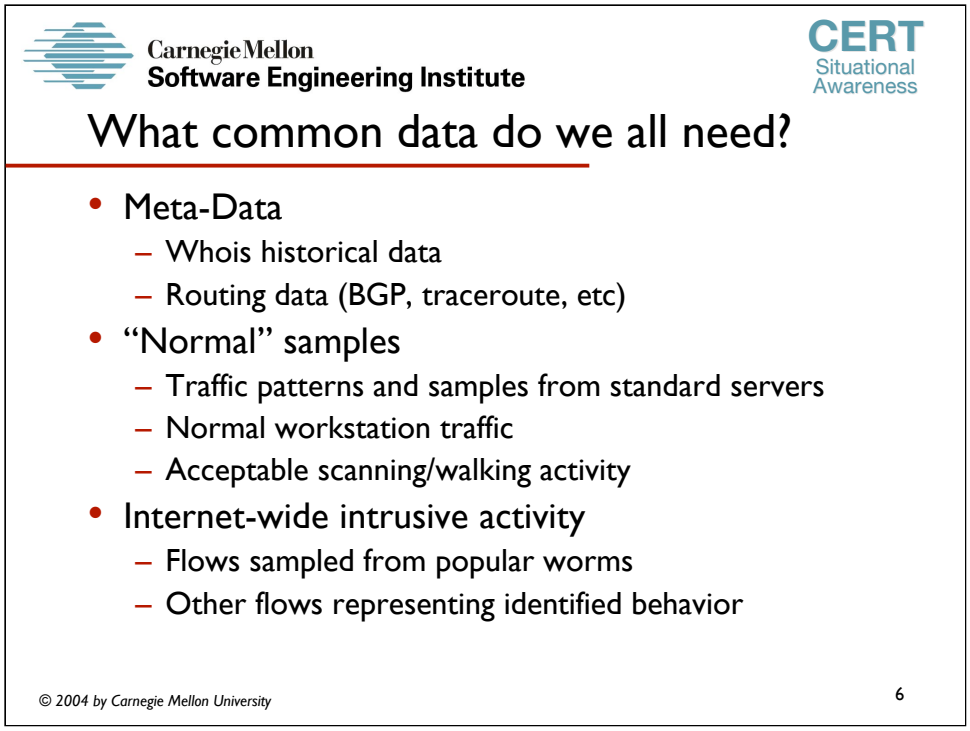
Compare and contrast CISCO netflow with ARGUS and others.

Low level analysts quickly trained on other environments (e.g., PNNL)

KB for analyst to share ideas and results (success results and how that was achieved). Understand the impact.

Pictures. Marketing strategy for selling netflow results. Translation to english.

People (sharing)?



People sharing leads to much greater data trust.

Examples of interesting behavior – scripts and visualizations.

How to continue conversations with legal? Need a practical context to ask questions. Test cases. Come up with an interesting scenario, but be less abstract.