Top 5 Ideas from the Practitioner Track Working Session – 17 August 2010

1. The context of the situation would give you a basis by which to consider appropriate indicators. Models should apply multiple contexts to a scenario to generate multiple hypotheses, which would result in situational indicators for the practitioners.

2. A data model that connects the idea of context and analytic judgment based on past signatures or electronic and human data that may exist. Then the model will connect the idea and analytic judgment to identify a person that has insight into the attack.

3. The model of meta-data (data about data) and one’s ability to put an amount of confidence to it

* How it relates it to people and their knowledge
* Ability to be able to categorize the threat and how serious it is

4. A model that picks up fingerprints of hackers that are doing practice attacks based on web traffic patterns and volume.

5. A data model of both volumes of traffic, content, and domains to develop early indicators of unusual and unexpected behavior as a tool for practitioners.