Issues

* Alert correlation:
  + Alert format (recommend IDMEF).
  + Alert aggregation into hyper-alert.
  + Connect hyper-alerts to graph.
  + Abstract nodes of a graph to general class 🡪 to make causal network.
* Security flaw (attack tree):
  + How a professional define a flaw as an attack tree.
  + How to match causal networks (from above) and attack trees (in database).
* System scan
* Visualization