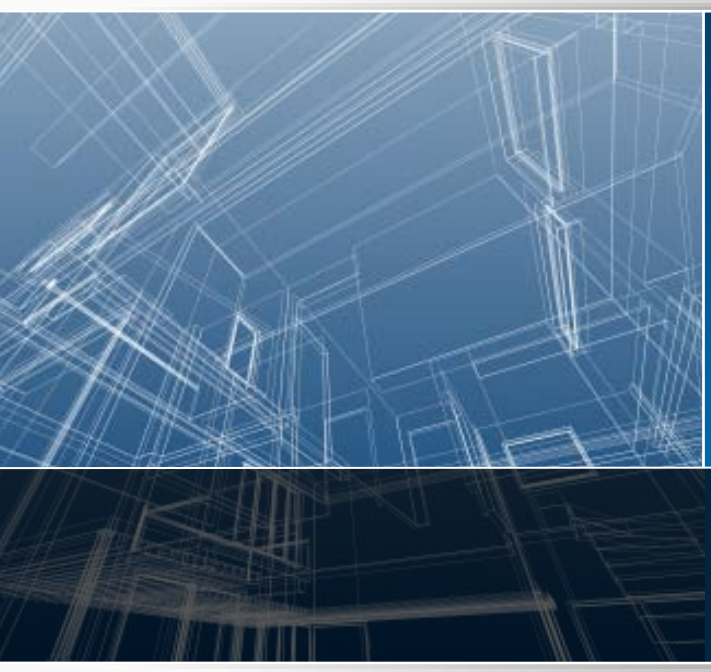
Digital Sandbox

Software products and services for analytic risk management



Evaluating Pattern of Life Indicators to Prioritize Potential Insider Threats

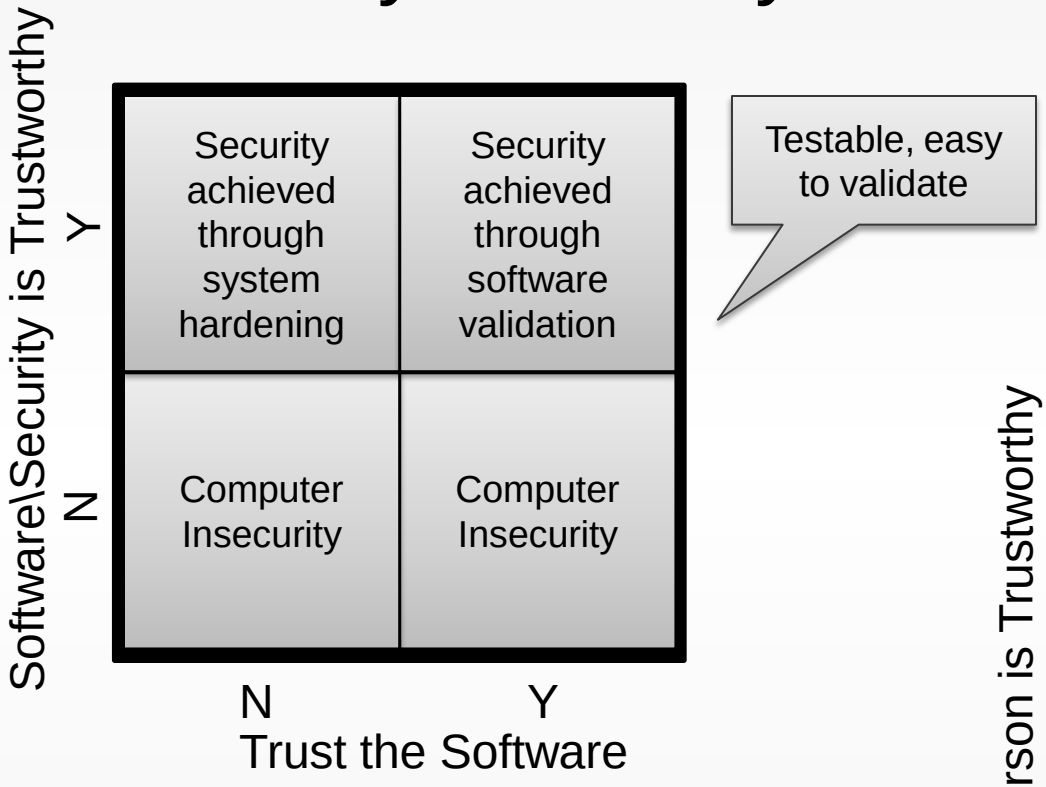
Mini Metricon 6.5

A few opening thoughts about metrics and data

- The data you have isn't the data you want
  - It reflects the past (which may not look like the future)
  - It tells you what machines recorded, not what humans thought
- The models we build don't often yield beneficial results
  - Look for the last pattern, which may not be relevant
  - Yield high false alarms, then become irrelevant
  - Don't represent causality, and therefore limit countermeasures
- Most SME's have limited expertise
  - Expert pool is limited to IT domain
  - Experts are biased towards being presented with evidence (post incident) vs. representing their knowledge (pre-incident)

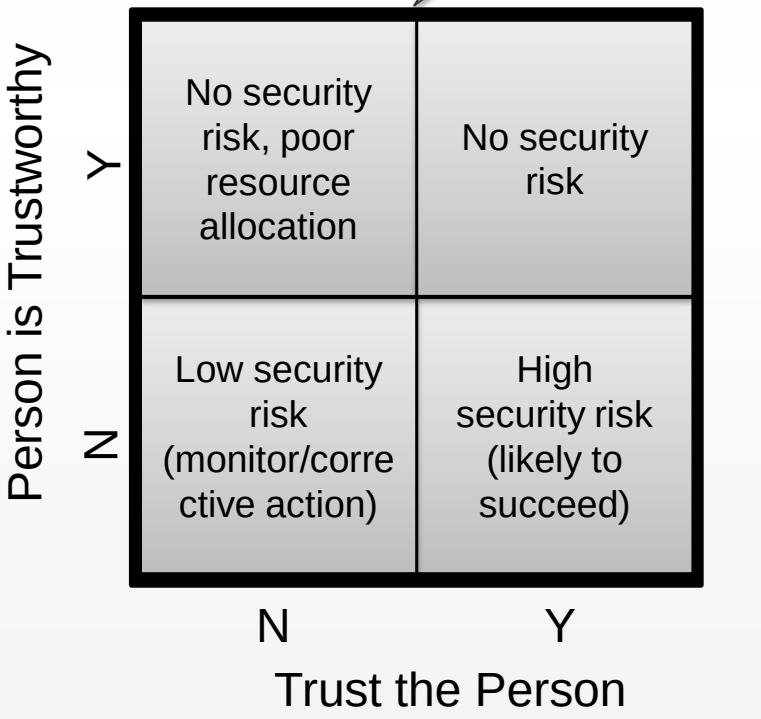
Developing an Insider Threat Management System requires predictive analytics that consider pattern of life data – credit, public records, employment, social – in addition to computer and network data.

Technological *and* social components necessary for a truly hardened cyber system

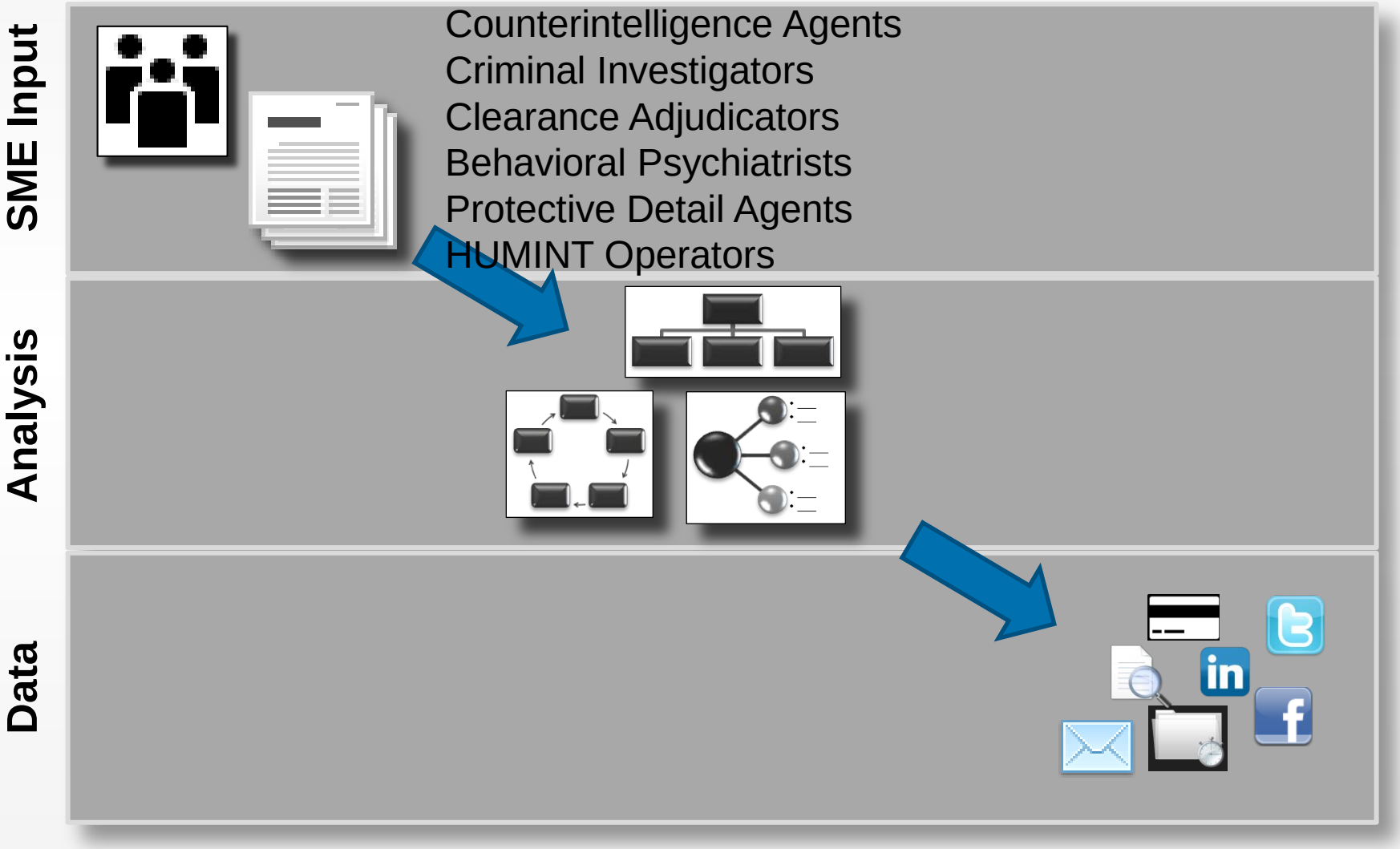


Testable, easy to validate

What makes a person (un)trustworthy ?



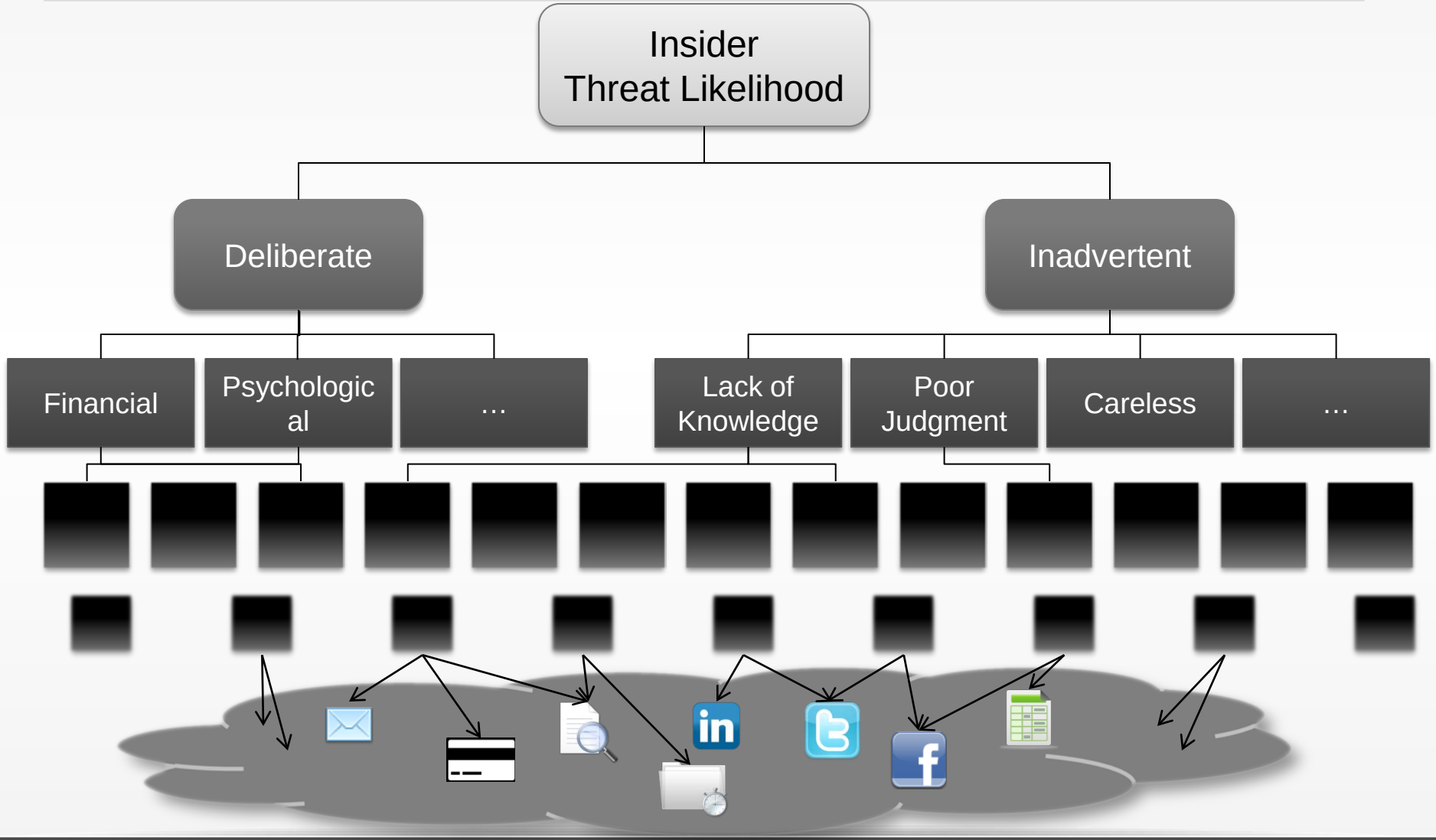
Model-driven approach



Model untrustworthiness by monitoring characteristics tied to illicit behavior

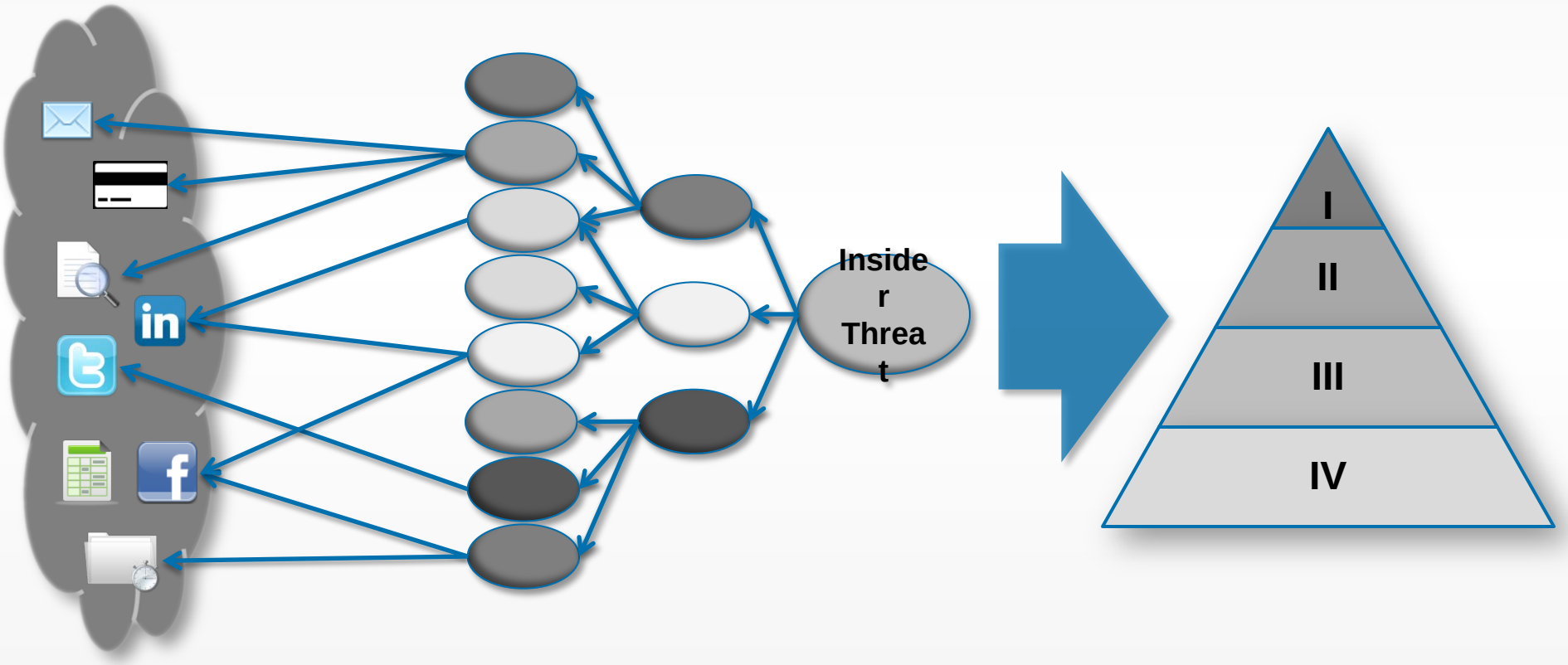
- Layers of prioritization is key to modeling ambiguous concepts
  - prioritize concepts
  - prioritize data
  - prioritize results
- Model design can facilitate or inhibit prioritization
  - data driven approach
  - model driven approach

SME Engineered Model

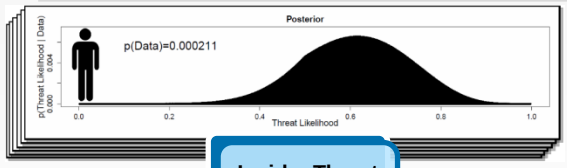


Digital Sandbox modeling process

Data Sources **Model** **Prioritized Output**



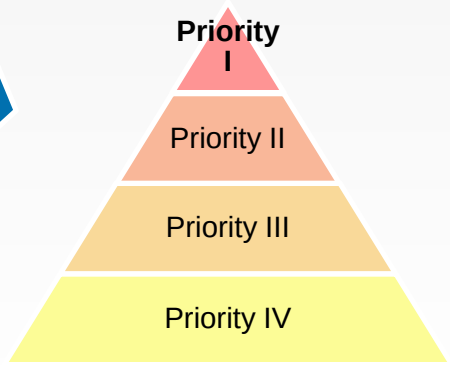
Continuous Evaluation Process



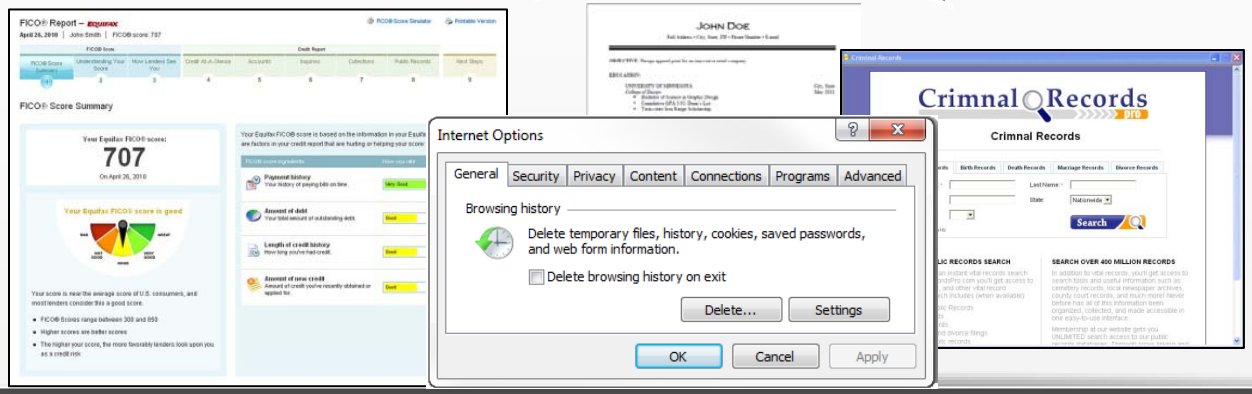
Insider Threat Likelihood

- **Deliberate**
  - Financial
  - …
  - Psychological
- **Inadvertent**
  - Lack of Knowledge
  - Poor Judgment
  - …
  - Careless

Engineered Model becomes Bayesian Model



Instant notification of Priority I Individuals



HR data, browsing history, annual employee evaluations

Discuss