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

<table>
<thead>
<tr>
<th>Software Security is Trustworthy</th>
<th>Trust the Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Security achieved through system hardening</td>
</tr>
<tr>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Computer Insecurity</td>
<td>Computer Insecurity</td>
</tr>
</tbody>
</table>

Testable, easy to validate

<table>
<thead>
<tr>
<th>Person is Trustworthy</th>
<th>Trust the Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>No security risk, poor resource allocation</td>
</tr>
<tr>
<td>N</td>
<td>No security risk</td>
</tr>
<tr>
<td>Y</td>
<td>Low security risk (monitor/corrective action)</td>
</tr>
<tr>
<td>N</td>
<td>High security risk (likely to succeed)</td>
</tr>
</tbody>
</table>

What makes a person (un)trustworthy?
Model-driven approach

SME Input
- Counterintelligence Agents
- Criminal Investigators
- Clearance Adjudicators
- Behavioral Psychiatrists
- Protective Detail Agents
- HUMINT Operators

Analysis

Data
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

Insider Threat Likelihood

Deliberate
- Financial
- Psychological
- ...

Inadvertent
- Lack of Knowledge
- Poor Judgment
- Careless
- ...

3/7/2012
Digital Sandbox modeling process

Data Sources

Model

Prioritized Output

Inside
Threat

I
II
III
IV
Continuous Evaluation Process

Insider Threat Likelihood

Deliberate
- Financial
- Psychological
- Lack of Knowledge
- Poor Judgment
- Careless

Inadvertent

Priority I
Priority II
Priority III
Priority IV

Instant notification of Priority I Individuals

Engineered Model becomes Bayesian

HR data, browsing history, annual employee evaluations

3/7/2012
Discuss