Chris Sanders
Twitter: @chrissanders88 | Mail: chris@chrissanders.org
PhD Researcher | SANS GSE #64 | BBQ Pitmaster
What problem am I talking about today?
Symptoms of a Cognitive Crisis

1. Demand for expertise greatly outweighs supply
2. Most information cannot be trusted or validated
3. Inability to mobilize and tackle big systemic issues
What assumptions am I making?
A Universal Investigation Process

Observation → Question → Hypothesis → Answer → Conclusion

Alert → Investigation

Hunting for Observations → Investigation
What separates expert analysts/hunters from novices?
Mapping the Investigation

- **Sample:**
  - Novice and expert analysts

- **Methodology:**
  - 30+ case studies
  - Stimulated recall interviews
  - Focus on individual investigations of varying types
  - Perform key phrase analysis – analyze results
Key Phrase Mapping

- **Dual Process Theory**
  - Intuition: Implicit, unconscious, fast
  - Reflection: Explicit, controlled, slow

<table>
<thead>
<tr>
<th>Intuition</th>
<th>Metacognition</th>
<th>Reflection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experimentation</td>
<td>Evaluation</td>
<td>Analytically Viewing Data</td>
</tr>
<tr>
<td>Restructuring</td>
<td>Goal Setting</td>
<td>Rule-Based Reasoning</td>
</tr>
<tr>
<td>Imagination</td>
<td>Making Plans</td>
<td>Considering Alternatives</td>
</tr>
<tr>
<td>Incubation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Results

<table>
<thead>
<tr>
<th>Intuition</th>
<th>Metacognition</th>
<th>Reflection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experiment</td>
<td>Evaluation</td>
<td>Viewing Data</td>
</tr>
<tr>
<td>Restructuring</td>
<td>Goal Setting</td>
<td>Rule-Based Reasoning</td>
</tr>
<tr>
<td>Imagination</td>
<td>Making Plans</td>
<td>Considering Alternatives</td>
</tr>
<tr>
<td>Incubation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Novices

Experts
What is the X factor that makes a good hunter?
Curiosity and Experience

- High C
- Low E
- Low C
- Low E
- High C
- High E
- High C
- Low E

Jumpy
Excerls

Ineffective
Apathetic

Low C
Low E
Low C
High E
Assessing Curiosity

Average Investigation Activity per Day

<table>
<thead>
<tr>
<th>Time</th>
<th>Analysts</th>
<th>Hunters</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00 AM</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>2:00 AM</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>4:00 AM</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6:00 AM</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8:00 AM</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>18</td>
<td>43</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>43</td>
<td>51</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>26</td>
<td>49</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>24</td>
<td>42</td>
</tr>
<tr>
<td>6:00 PM</td>
<td>24</td>
<td>38</td>
</tr>
<tr>
<td>8:00 PM</td>
<td>12</td>
<td>18</td>
</tr>
<tr>
<td>10:00 PM</td>
<td>3</td>
<td>1.5</td>
</tr>
</tbody>
</table>
Assessing Curiosity

Average Investigation Activity per Day

Timing:
- 12:00 AM
- 2:00 AM
- 4:00 AM
- 6:00 AM
- 8:00 AM
- 10:00 AM
- 12:00 PM
- 2:00 PM
- 4:00 PM
- 6:00 PM
- 8:00 PM
- 10:00 PM

Activity Levels:
- 60
- 50
- 40
- 30
- 20
- 10
- 0

Analysts and Hunters
Does the sequence of the investigation matter?
Studying the Investigation Process

Investigation Theory: Lab 1

IDS Alert

The IDS alert shown here was generated a few minutes ago. Please investigate this alert using the given data sources and make a determination about whether an incident has occurred, what hosts were victims, and any malicious hosts you encounter.

SURICATA ALERT: FY3 Malware Download  
Timestamp: 7/8/2016 09:30:00  
10.0.0.5 -> 8.8.8.8  
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"FY3 Malware Download"; flow:to_server,established; http_method:GET content:"fy3.exe"; http_uri:unknown;)

What data source would you like to investigate?

- Alert Packet
- Network Flows
- Packet Capture
- Live Process List
- Live Host File System
- Windows Registry
- Open Source Intelligence
- Windows Host Logs
Studying the Investigation Process

You completed the simulation in 00:03:33. This is compares to an average time of 00:03:31 for people who also chose a skill level of Beginner.
Is ‘too much data’ a real thing?

Data Suggests:

- Better organization of high context data sources can yield improvements in analysts performance
What data transformations were most often used in positive finding?

**ALERTS - % Used in Discovery of Declared Incidents**

- Pivot: 76%
- Aggregation: 23%
- Expansions/Reductions: 100%
- Visualization: 0%

**HUNTING - % Used in Discovery of Declared Incidents**

- Pivot: 92%
- Aggregation: 84%
- Expansion/Reduction: 100%
- Visualization: 0%
How can I do similar research?
Conclusion – Positive Deviance

1. Ask questions
2. Don’t complain
3. Measure something
4. Write about it
5. Change