Threat Intelligence for Incident Response

Kyle Maxwell, Senior Analyst (@kylemaxwell)
2014-02-11
Taxonomy

Strategic
Operational
Tactical
Taxonomy: Open vs Closed Source
Taxonomy: Pyramid of Pain

- **TTPs**: Tough!
- **Tools**: Challenging
- **Network/Host Artifacts**: Annoying
- **Domain Names**: Simple
- **IP Addresses**: Easy
- **Hash Values**: Trivial
Intelligence Cycle

Direction

Collection

Processing

Analysis

Dissemination

Feedback
Direction

What will the program achieve?
Who will act on the intelligence?
What do they need?

What will you do with it?
Collection

What do you have?
What do you need?
What can you get?
How will you store it?
Processing: Scalability
Processing: Automation
Analysis

\textsf{analyst(caffeine, data)} \rightarrow \textsf{knowledge}
VERIS Framework

Actor – Who did it?
Action – What did they do?
Asset – What did they do it to?
Attribute – How was it affected?

Documentation, classification examples, enumerations:
http://veriscommunity.net
Analysis
Dissemination
Feedback: Improvement
Now what?

@kylemaxwell
kyle.maxwell@verizon.com