Threat Intelligence for Incident Response

Kyle Maxwell, Senior Analyst (@kylemaxwell)

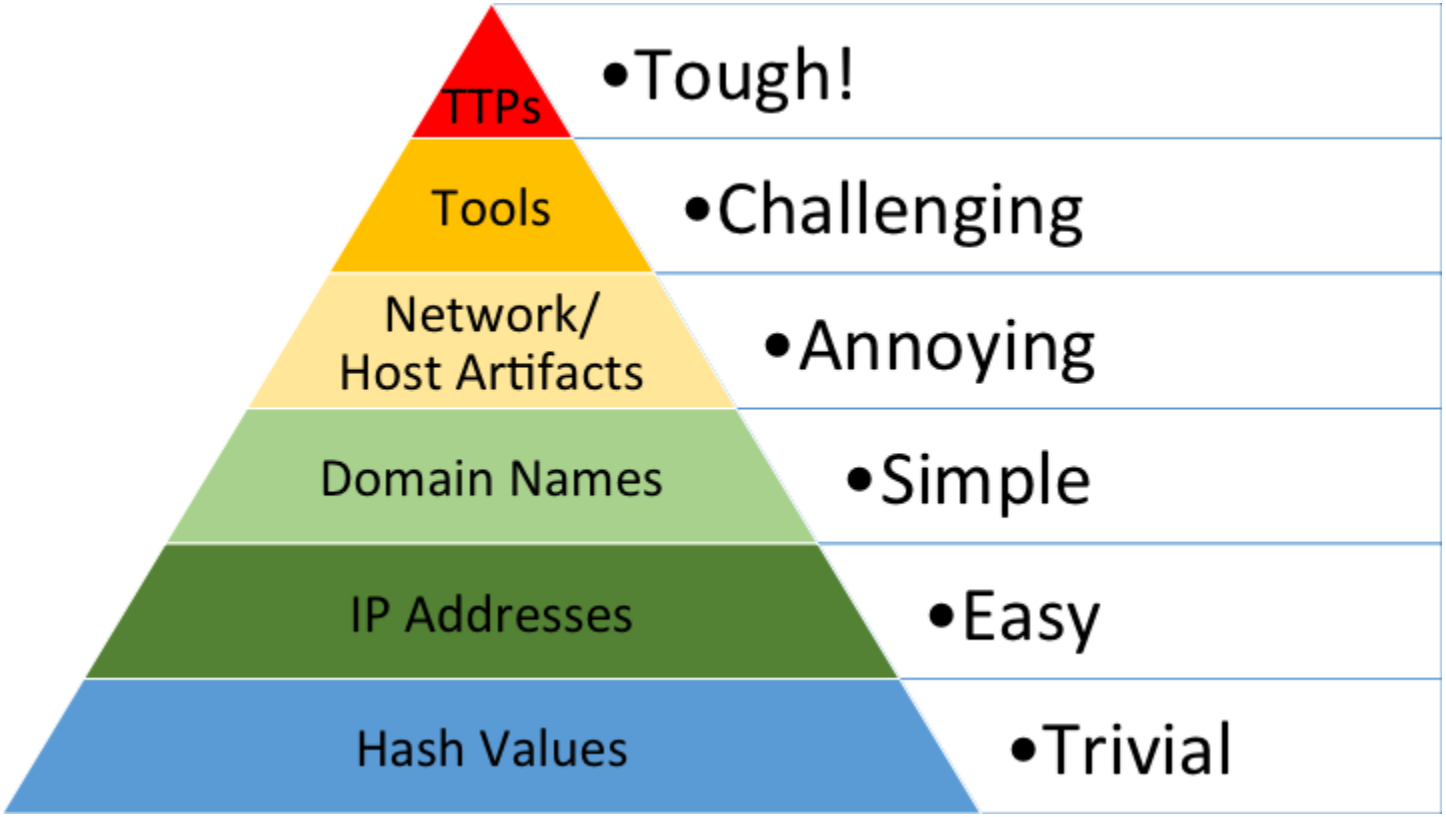
2014-02-11

Taxonomy

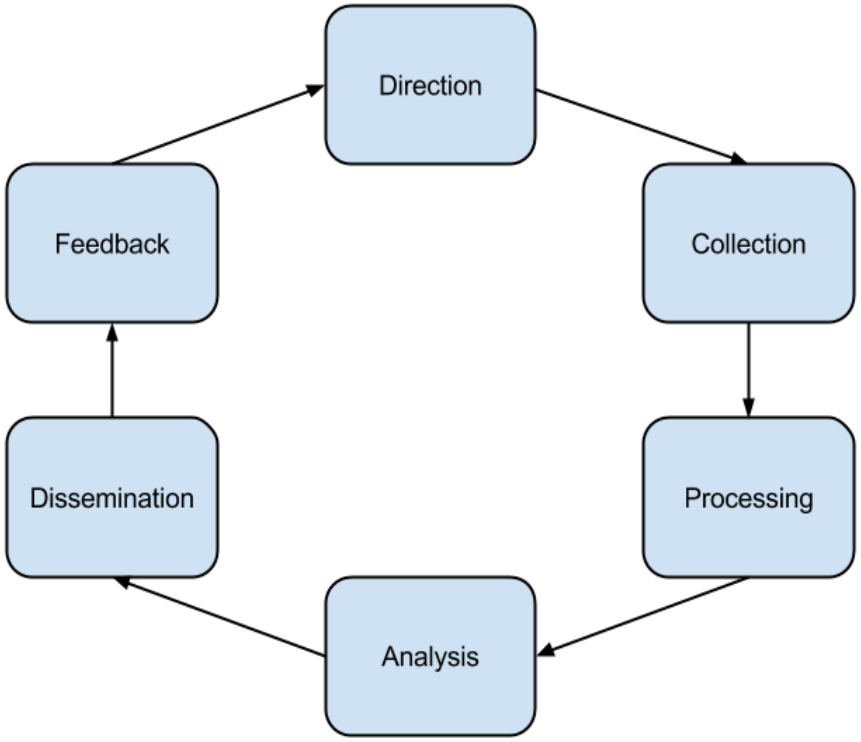
Strategic
Operational
Tactical

Taxonomy: Open vs Closed Source

Taxonomy: Pyramid of Pain



Intelligence Cycle



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

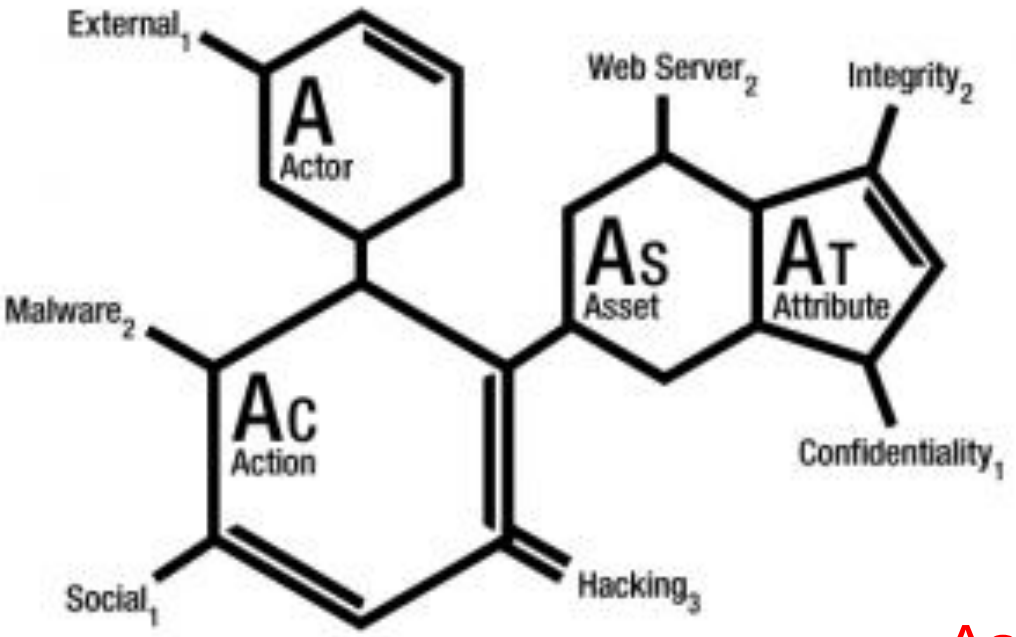
Processing: Automation

Hed Kodin

Analysis

```
analyst(caffeine, data) ->
        knowledge
```

VERIS Framework



Actor – Who did it?

Action – What did they do?

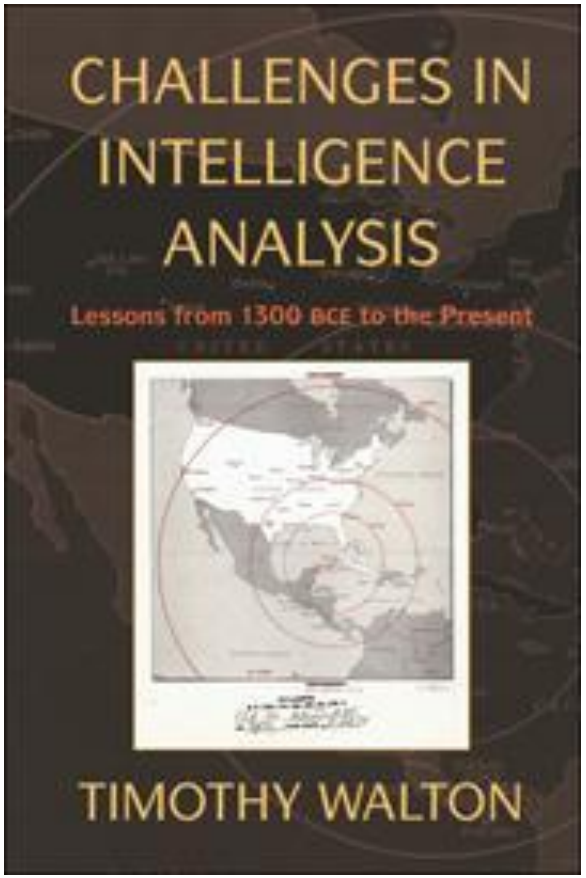
Asset – What did they do it to?

Attribute – How was it affected?

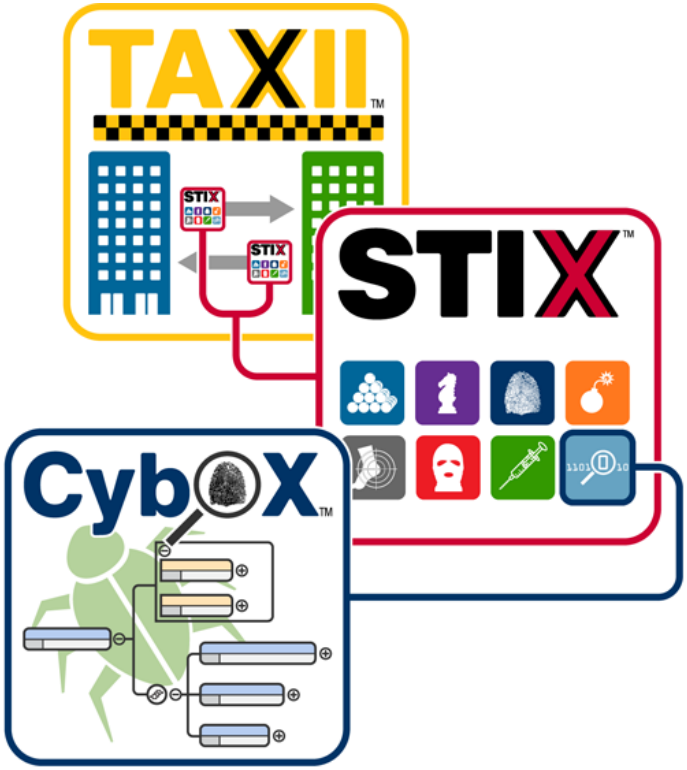
Documentation, classification examples, enumerations:
http://veriscommunity.net

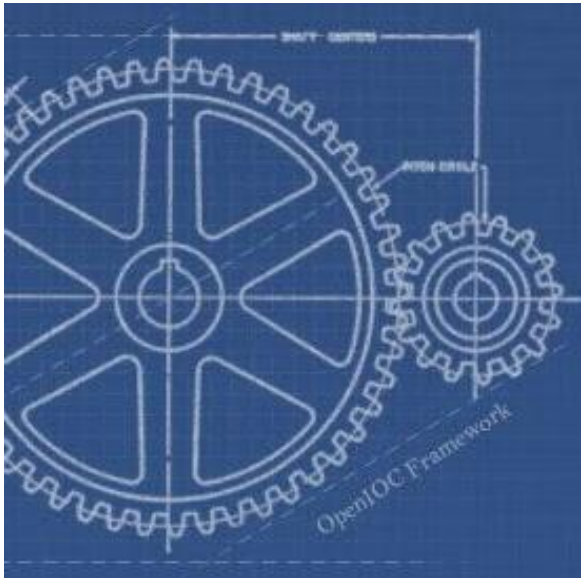
Analysis


The Analyst's Cookbook
Volume 2
Domenic Vallone
Nicole Pillar, Eds.

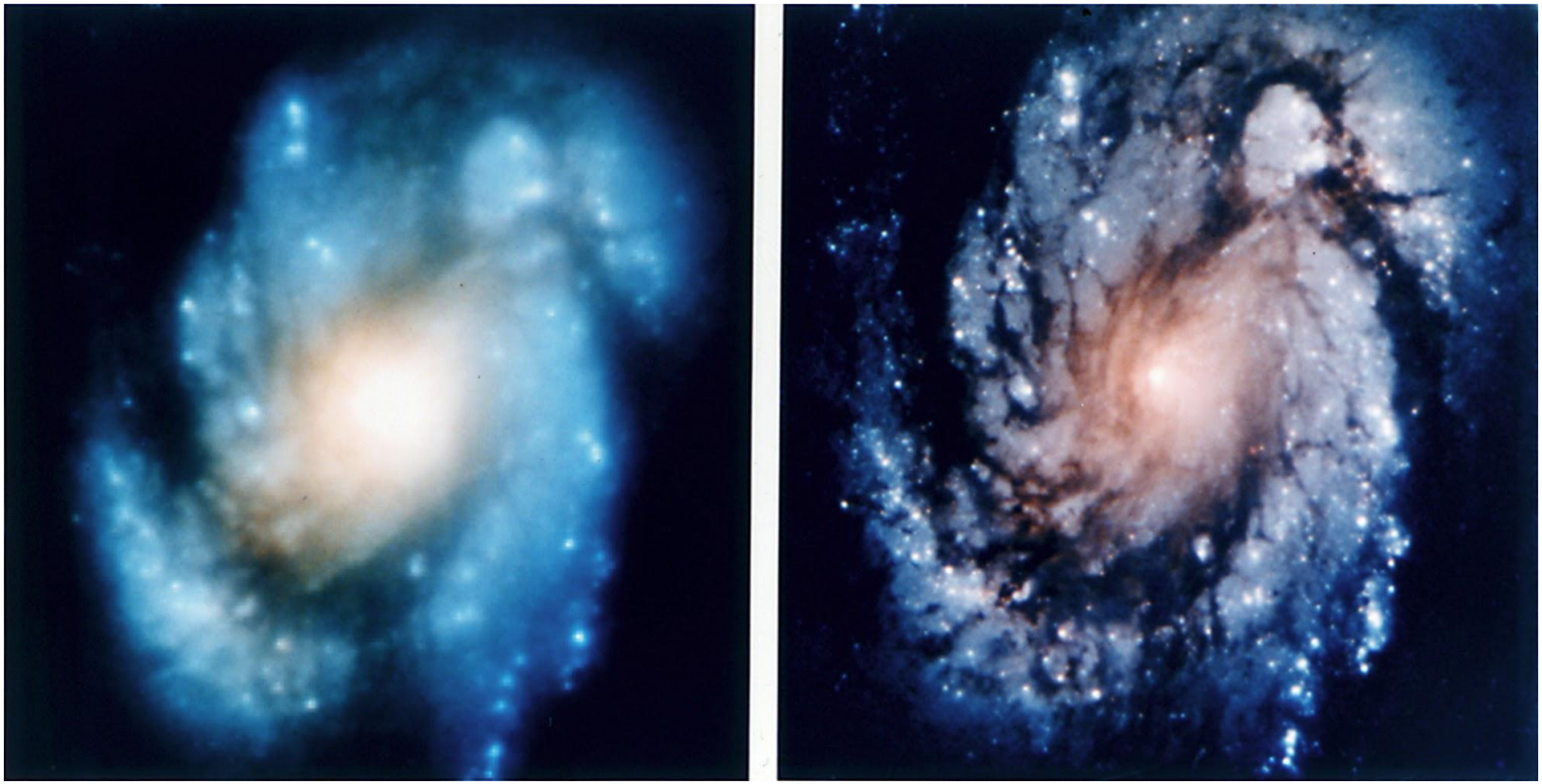

CHALLENGES IN INTELLIGENCE ANALYSIS
Lessons from 1300 BCE to the Present
TIMOTHY WALTON

Dissemination





Feedback: Improvement



Now what?

@kylemaxwell
kyle.maxwell@verizon.com