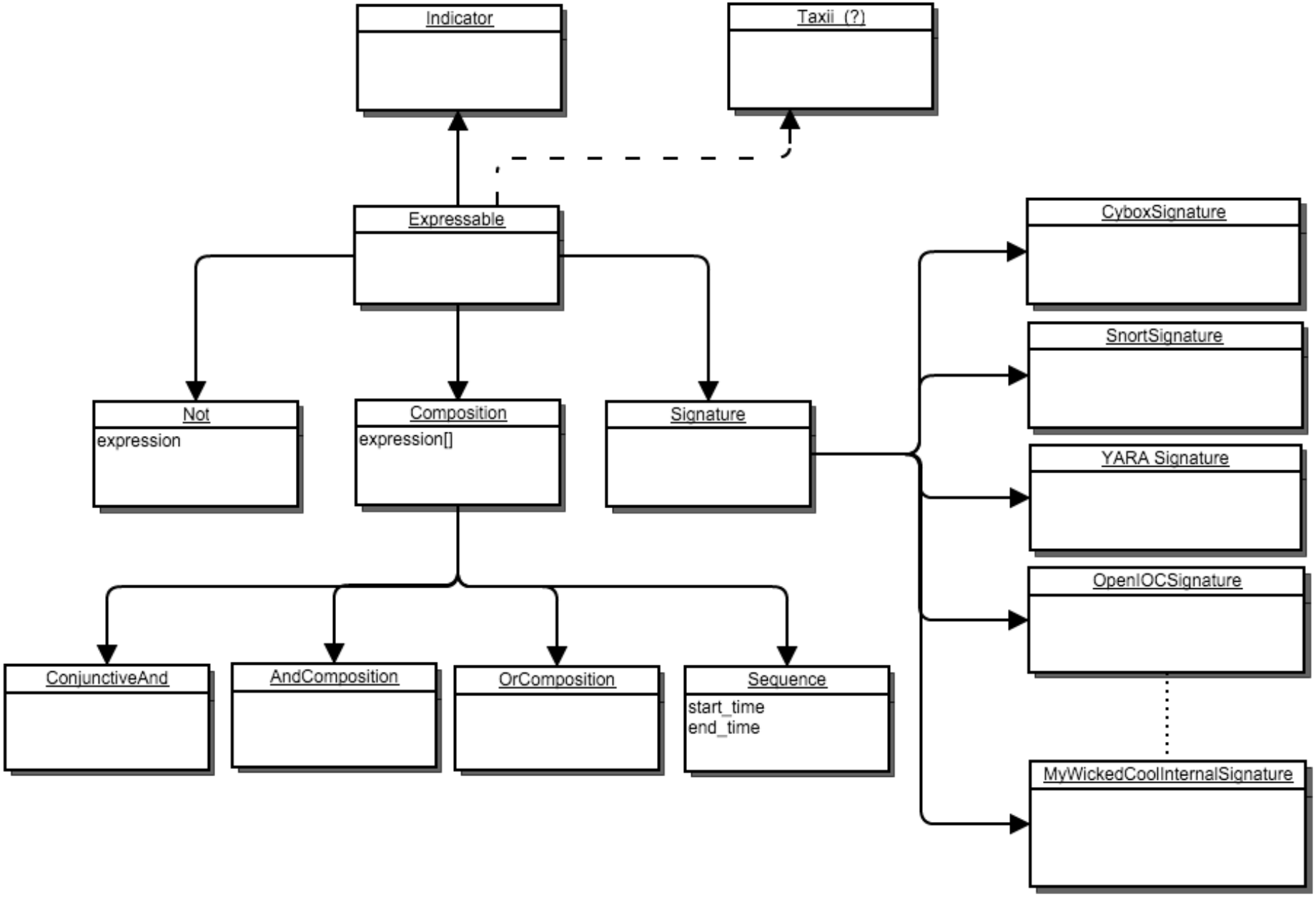
STIX Patterning "Problems"

- Multiple ways to do composition (indicator, observable…)
- Nested composition cumbersome (sometimes impossible)
- Lack of sequencing, time boxing
- Confusion around observable use case
- Implicit ties to CybOX

Proposal

- Language Logic should be separate from that on which it is acting
- AKA, *define* the “operators”, *abstract* the “operands”.
- “Expressable” is an id-able object that can be re-used
- Possible enables deprecate / remove the “observable” object, among many other things…


Indicator
Taxii (?)
Expressable
Not
expression
Composition
expression[]
Signature
CyboxSignature
SnortSignature
YARA Signature
OpenIOCSignature
MyWickedCoolInternalSignature
ConjunctiveAnd
AndComposition
OrComposition
Sequence
start_time
end_time

What the heck is a "ConjunctiveAnd"

- Differentiates between "All of the following expressions, on any object" and "All of the following expressions, on the same object
- Example: File Hash A and File Name B – on either file OR same file, or ONLY on same file.
- ConjunctiveOr is not required, due to nature of "or" (challenge?)

Example: "This file hash OR this Yara signature followed by this windows registry key, within 60 seconds"

```
{
  "type": "announcement",
  "id": "example.com:851a164e-c2cb-42d0-af7a-0eebb93355dc",
  "created_at": "2016-01-06T19:12:02.986050-05:00",
  "producer_ref": "example.com:example",
  "contents": [
    {
      "type": "indicator",
      "id": "example.com:628a75ab-7b63-4e88-9175-2c190e38233c",
      "created_at": "2016-01-06T19:13:17.778545-05:00",
      "producer_ref": "example.com:example",
      "pattern": {
        "type": "sequence",
        "duration": 60000,
        "expressions: [
            {
                "type":”or-composition",
                "expressions":[
                    {
                        "type":"cybox",
                        "key": "File_Hash:SHA256",
                        "condition": "equals",
                        "value": "730f75dafd73e047b86acb2dbd74e75dcb93272fa084a9082848f2341aa1abb60"
                    },
                    {
                        "type":"yara",
                        "contents":{ ... yara stuffs... }
                    } {

                ]
            {
                "type":"cybox"
                "key":"Windows_Registry",
                "condition":"equals",
                "value":"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce"
            }
        ]
      }
    }
}
```

Example 2: ”This Indicator OR This Other Indicator…


```
{
  "type": "announcement",
  "id": "example.com:851a164e-c2cb-42d0-af7a-0eebb93355dc",
  "created_at": "2016-01-06T19:12:02.986050-05:00",
  "producer_ref": "example.com:example",
  "contents": [
    {
      "type": "indicator",
      "id": "example.com:628a75ab-7b63-4e88-9175-2c190e38233c",
      "created_at": "2016-01-06T19:13:17.778545-05:00",
      "producer_ref": "example.com:example",
      "pattern": {
        "type": ”or-composition”,
        "expressions: [
            {
                "type":”indicator",
                ”indicator": “example.com:indicator:851a164e-c2cb-42d0-af7a-0eebb93355dc”,
            },
            {
                 "type":”indicator",
                 ”indicator": “example.com:indicator:951a164e-c2cb-42d0-af7a-0eebb93355dc”,
            }
         ]
      }
    }
}
```

End Result / Open Questions

- We have eliminated need for “observable”
- We have simplified how patterning is done (one way across all CTI)
- Potential: Could TAXII Query also be based on Expression…