RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: 9678

STIX Patterning: Viva la revolución!

Trey Darley

Director of Standards Development
New Context

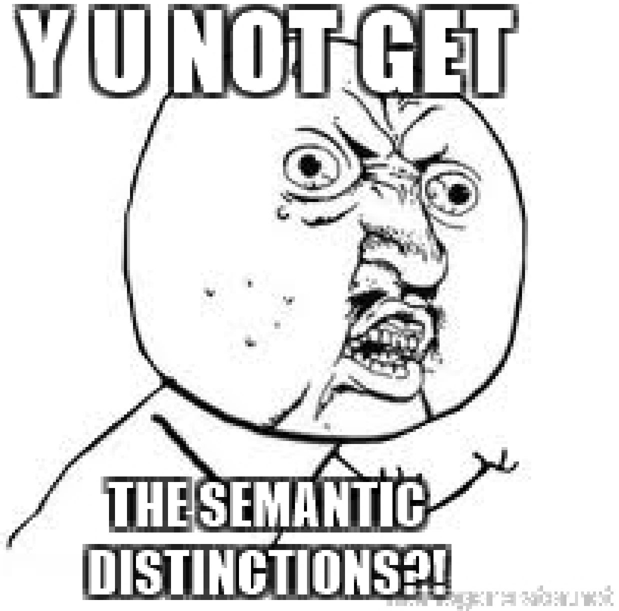
Jason Keirstead

Senior Technical Staff Member
IBM Security

This slide [is] intentionally left blank.

History vs. mystery

"What the hell were you guys smoking?!"



What was wrong in STIX 1.x

- Too many ways to define matches (multiple meanings of "Equals")
- Too many ways to define expressions (ANDs and ORs in *both* Indicators and Observables)
    - One analysis found twelve different ways to compare two IP addresses
- Lists are just plain "weird" (##comma## - need I say more?)
- Despite all this complexity, lacked fundamental capabilities such as temporal matching (A followed by B)

But (Snort|YARA|OpenIOC|Sigma) already exist?!

- Snort only makes sense on the network
- YARA library only works on a file-like blob
  - Neither allows encoding of malware behaviour information

- OpenIOC limited in expressivity; also limited in network coverage
- Basic use case: malware matching signature **X** will beacon with traffic that looks like **Y** before dropping **Z**
  - Combination of file attributes, network attributes, sequential / temporal matching
  - This extremely simple use case is **impossible** to model using any single one of these standards

- Sigma: https://github.com/Neo23x0/sigma
  - This project started after we'd already achieved our Committee Specification Draft for STIX 2.0. It has similar goals to STIX Patterning but is more focused on logs.

Questions we asked

- Should we think beyond simple CTI use cases of "find this IOC" ?
- What if our cybersecurity tools could share rules and searches for analytics and correlations?
- What factors have been preventing this from emerging in the industry? Could we have an opportunity to finally move the needle?
- What if SIEM vendor lock-in were to just die in a fire?

"We're here to put a dent in the universe." — Steve Jobs

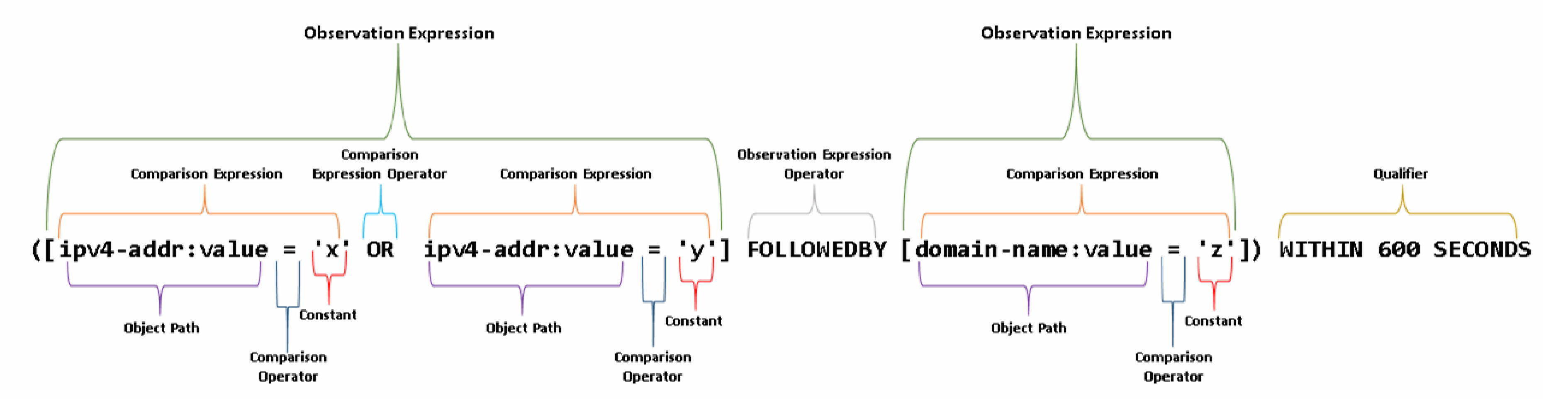
Basic design principles

- One way to do things (not 12)!
- Base things on a **grammar**, not nested XML or JSON
  - Makes things easier for humans to understand, **and** for machines to parse!
- Base that grammar on something that as many folks are familiar with as possible
  - Candidates: SQL, Lucene, YARA, Snort/OpenSig…
  - We ended with SQL-like after some debate
- Define a grammar that allows sharing descriptions of advanced threats, not just simple atomic IOCs (ip = 1.2.3.4)
- Define it in a way that was expandable in the future without "breaking changes"

Overview of STIX Patterning

"What's the frequency, Kenneth?"

Basic structure of a STIX Pattern



```
([ipv4-addr:value = 'x' OR ipv4-addr:value = 'y'] FOLLOWEDBY [domain-name:value = 'z']) WITHIN 600 SECONDS
```

Observation Expression

Comparison Expression

Comparison Expression Operator

Comparison Expression

Observation Expression

Observation Expression Operator

Comparison Expression

Qualifier

Object Path

Constant

Comparison Operator

Object Path

Constant

Comparison Operator

Object Path

Constant

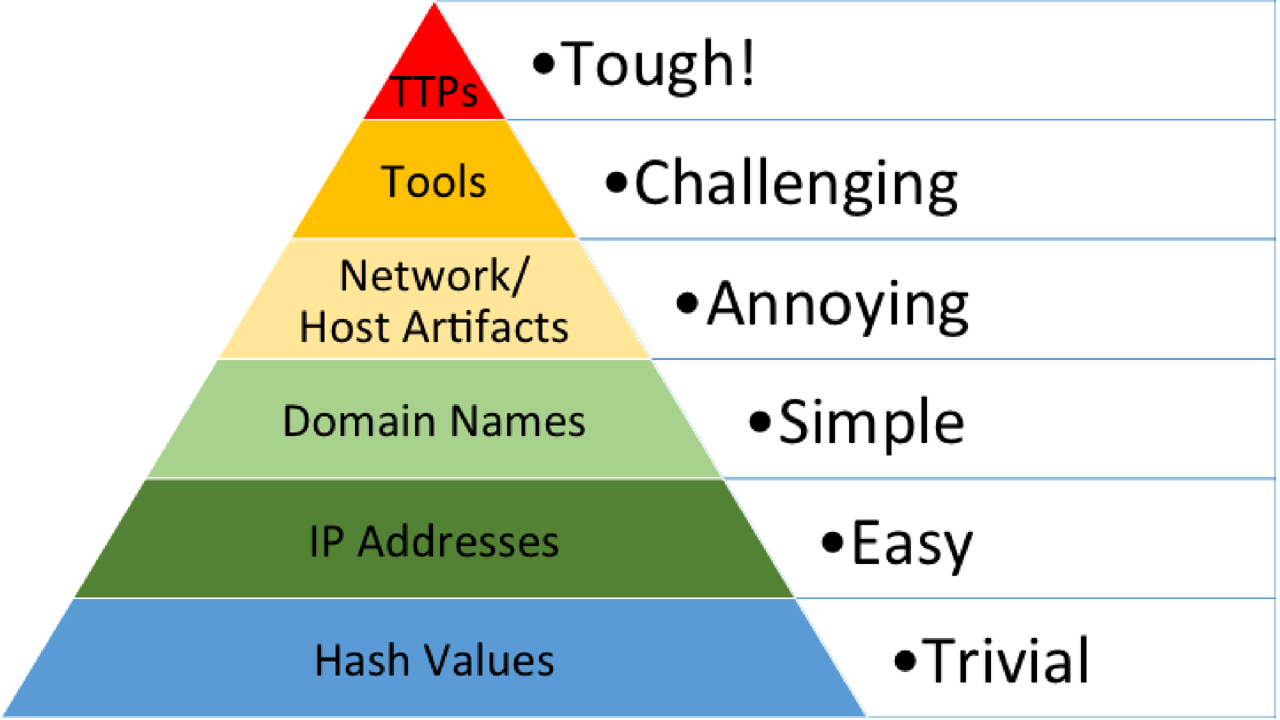
Comparison Operator

How this ties to STIX Cyber Observables

- Cyber Observables provide a data model for describing *things* you've either *actually seen*, or *are looking for*.
- STIX Patterning is a language for describing chaotic maliciousness one *might* see.
- SCO (STIX Cyber Observables) : nouns :: STIX Patterning : language
- SCO : DB Tables :: STIX Patterning : SQL

THIS SOUNDS INCREDIBLY COMPLICATED, I JUST WANTED TO FIND AN IP ADDRESS

The Vision



TTPs •Tough!

Tools •Challenging

Network/ Host Artifacts •Annoying

Domain Names •Simple

IP Addresses •Easy

Hash Values •Trivial

} Long-term goal for STIX Patterning

} What most people are doing today

It's not that bad, see!

Finding an IP

```
[ip-addr:value = '8.8.8.8']
```

Finding a URL

```
[url:value MATCHES
'^(?:https?:\/\/)?(?:www\.)?example\.com\/.*']
```

Finding one of two registry keys

```
[windows-registry-key:key =
'HKEY_CURRENT_USER\\Software\\CryptoLocker\\Files
' OR windows-registry-key:key =
'HKEY_CURRENT_USER\\Software\\Microsoft\\CurrentV
ersion\\Run\\CryptoLocker_0388']
```

Currently-defined Cyber Observables

- Artifact
- AS
- Directory
- Email Address
- Email Message
- File
  - Archive Extension
  - NTFS File Extension
  - PDF File Extension
  - Raster Image File Extension
  - Windows PE Binary File Extension
- IPv4 Address
- IPv6 Address
- MAC Address
- Mutex
- Network Traffic
  - HTTP Request Extension
  - ICMP Extension
  - Network Socket Extension
  - TCP Extension
- Process
  - Windows Process Extension
  - Windows Service Extension
- Software
- User Account
  - UNIX Account Extension
- Windows Registry Key
- X.509 Certificate

Use cases and examples

File-based Pattern (vs. YARA)

Basic File with Hexadecimal Payload

STIX Indicator Pattern

```
[file:contents_ref.payload_bin MATCHES '\\x65\\x78\\x61\\x6d\\x70\\x6c\\x65' AND file:size > '31284']
```

Corresponding YARA Rule

```
rule Example
{
    strings:
       $hex_string = { 65 78 61 6d 70 6c 65 }

    condition:
       $hex_string and filesize > 31284
}
```

File-based Pattern (vs. YARA) Continued…

Basic File with Textual Payload

STIX Indicator Pattern

```
[file:contents_ref.payload_bin MATCHES 'this is an example']
```

Corresponding YARA Rule

```
rule Example
{
    strings:
       $text_string = “this is an example”

    condition:
       $text_string
}
```

Network-based Pattern (vs. Snort)

Basic TCP Network Traffic

STIX Indicator Pattern

```
[network-traffic:src_ref.type = 'ipv4-addr' AND network-traffic:src_ref.value = '192.0.2.1' AND network-traffic:dst_ref.type = 'ipv4-addr' AND network-traffic:dst_ref.value = '203.0.113.10' AND network-traffic:dst_port = '21' AND network-traffic:protocols[*] = 'tcp']
```

Corresponding Snort Rule

```
alert tcp 192.0.2.1 any -> 203.0.113.10 21
```

Network-based Pattern (vs. Snort), Con't

HTTP Network Traffic with User Agent

STIX Indicator Pattern

```
[network-traffic:dst_ref.type = 'ipv4-addr' AND network-traffic:dst_ref.value = '203.0.113.11' AND network-traffic:dst_port = '80'
AND network-traffic:protocols[*] = 'tcp' AND network-traffic:extended_properties.http-ext.request_header.User-Agent =
'Mazilla/5.0']
```

Corresponding Snort Rule

```
alert tcp any any -> 203.0.113.11 80 (content:"User-Agent|3a|

Mazilla/5.0"; http_header;)
```

Watching for "Fileless" UAC Bypass

```
[

     ( windows-registry-key:key =
     'HKEY_CURRENT_USER\\Software\\Classes\\exefile\\shell\\runas\\command' AND windows-registry-
     key:values[*].name = 'isolatedCommand' )

]

OR

[

     ( windows-registry-key:key = 'HKEY_CURRENT_USER\\Microsoft\\Windows\\CurrentVersion\\App
Paths\\control.exe' AND windows-registry-key:values[*].data != "C:\\Windows\\System32\\cmd.exe" )

]
```

Bad Powershell!

Suspicious Powershell has been used

```
[

    process:command_line MATCHES
    '((.*NewObject(System)?NetWebClient.*DownloadFile.*((StartProcess)|(shellexecute)|(win32_proc
    ess)|(start)|(saps)).*)|(.*((iex)|(InvokeExpression)).*NewObject(System)?NetWebClient.*Downlo
    adString.*)|(.*NewObject(System)?NetWebClient.*DownloadString.*((iex)|(InvokeExpression)).*)|
    (.*IEX.*\[SystemDiagnosticsProcess\]\:\:Start.*)|(.*StartBitsTransfer.*InvokeItem.*))'

]
```

Necurs Botnet

Looks for a particular malware payload followed by HTTP beaconing traffic generated by the payload:

```
[file:name = 'rekakva32.exe' AND file:parent_directory_ref.path MATCHES 
'C:\\Users\\[\\w\\s]+\\AppData\\Local\\Temp'] FOLLOWEDBY [network-
traffic:protocols[*] = 'http' AND network-traffic:extensions.'http-request-
ext'.request_method = 'post' AND network-traffic:extensions.'http-request-
ext'.request_header.'User-Agent' = 'Windows-Update-Agent']
```

Source: https://isc.sans.edu/forums/diary/Necurs+Botnet+malspam+pushes+Locky+using+DDE+attack/22946/

OSS tools and libs

GitHub all the things!

- There are a bunch of open-source tools and libraries for STIX2:
  - Implemented in Python, Golang, Java, Scala, Javascript, PHP, etc.
  - Comprehensive list maintained here: https://goo.gl/y7ru68

We're Not Done!

Beyond indicators - analytics use cases

- Threat Intelligence sharing has received a lot of focus; however the analytics to actually **find** things, not so much
- People rebuild the same analytics over and over because they either don't know of, or have access to, what has been done many times before
- **In order to share analytics in a scalable fashion, a vendor-neutral language for said analytics has to be developed**
- **We believe SCO Pattern could be the basis for this**
- **CAR** - The MITRE Cyber Analytics Repository
  - PRE-ATT&CK and ATT&CK based analytics - https://attack.mitre.org
  - Long-term goal: ability to define these analytics in STIX Patterning
  - Collaborative ecosystem for analytics development

Correlation rules

- SIEM correlation rules share a lot of the same challenges as analytics
  - In fact, they **are** analytics! Imagine!
- Future vision / desire is for SIEM vendors to support SCO Pattern as a method to define searches and rules
  - Reduce / eliminate vendor lock-in
  - Enable broader ecosystem of cross-vendor solutions sharing tools
  - Seamless integration of STIX 2.0 compatible threat intelligence with SIEM correlation engines
- Again, speak to your vendor!
  - Nothing moves ahead without customers demanding it

It's not perfect...yet.

- Known gaps in SCO object model itself
- Known gaps in language
- We need your help!
- While we believe that STIX Patterning is amongst the most long-term significant innovations in STIX 2.x, it is nevertheless a work product coming out of a very small team of people. If we have succeeded in convincing you that we are not in fact smoking crazy goat-weed, please come join the party!

It's not just us...

accenture · aetna · AIRBUS · ALIEN VAULT · ANOMALI · AIT AUSTRIAN INSTITUTE OF TECHNOLOGY · ANZ

Bank of America · BMO Bank of Montreal · BOEING · circl · CISCO · Center for Internet Security · Cyber Threat Intelligence Network

DELL · difi · eclectic iq · EPRI · ERICSSON · FINANCIAL SERVICES ISAC · FireEye

FORNETIX · FORTINET · FUJITSU · G2 · GENIVIA · GEORGETOWN UNIVERSITY · Google

Hewlett Packard Enterprise · HUAWEI · Huntsman · IBM · iboss · 情報セキュリティ大学院大学 INSTITUTE of INFORMATION SECURITY · IJIS Institute

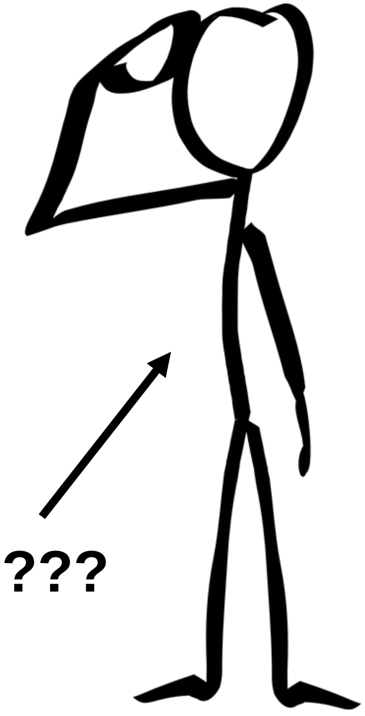
intel · APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY · JPMorganChase · KAISER PERMANENTE · LOOKINGGLASS · McAfee · MITRE

MTG · NHISAC · NATO OTAN · NC4 · NEC · NEW CONTEXT · NORTHROP GRUMMAN

paloalto NETWORKS · PERCH · Phantom · SEMPER FORTIS SOLUTIONS · sFractal Consulting LLC · SIEMENS · SOUTHERN CALIFORNIA EDISON

Symantec · SYNOPSYS · TELUS · THREATCONNECT · THREATQUOTIENT · TRUSTAR TECHNOLOGY · UNC CHARLOTTE

usbancorp · DEPARTMENT OF DEFENSE · U.S. DEPARTMENT OF HOMELAND SECURITY · NATIONAL SECURITY AGENCY · VERISIGN · ViaSat · XLAB



You???

Next Actions

- Ask your vendors (or product managers) about their roadmap.
- Come help us bring this vision to fruition.
- Go home and relax after a long and frantic week. :-)

Q&A

Who are we?

Jason Keirstead 🇨🇦

From a tiny city in Canada you've never heard of (Fredericton, NB)

Working in Security Intelligence arena since 2004 (Q1 Labs/IBM Security) across many domains including SIEM, risk and vulnerability management, security analytics, and threat intelligence

Working with STIX and TAXII community since 2014; OASIS CTI TC co-chair since 2016

Loves working on enterprise-scale challenges and interesting new problem domains, but a simple hacker at heart

Trey Darley (@treyka) 🇺🇸 🇧🇪

A Georgia boy (Atlanta, not Tbilisi) transplanted to Brussels by way of (a long story).

Currently Director of Standards Development at New Context, following years of infosec work, including stints at NATO and Splunk's Security Practice.

Part of the STIX/TAXII cabal since 2013; OASIS CTI TC co-chair since 2015; OASIS Technical Advisory Board member; official OASIS/FIRST liaison; benevolent bit-flipper;

Enjoys long walks, playing chess with his daughter, and tweaking his emacs config.

NEW CONTEXT IBM Security