RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-T10

What's Next?
Teaching Machines to Speak Security

Aharon Chernin

CTO
Soltra
@AharonChernin

What's Wrong With IT?

- Information Security tries to get them to code securely
- Like pulling teeth getting IT to a baseline and written policies
- IT is surprised every second Tuesday of the month
- Never ever patch 3rd party software
- Have you tried to leverage IT to find a file hash?

Information Technology went Strategic

Faced with the Rapid Pace of Operational Technology Advancement…

- Created Interoperability Standards and Specifications
- Built Platforms Based on Standards and Specifications
- Abstracted Away Complexity and Automated
- Focused on Machines

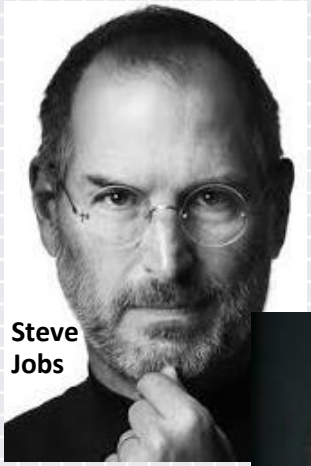
InfoSec Still Tactical

Faced with the Rapid Pace of Advancing of Threats…

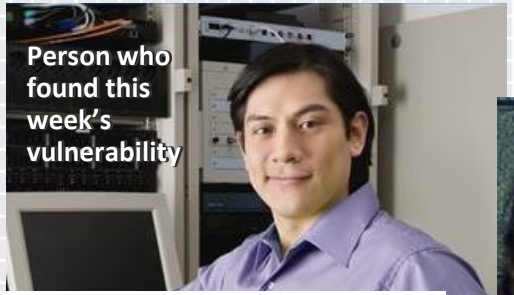
- Hired More Contractors
- Built More Web Portals, Proprietary API's, Created Spreadsheets
- Bought More Complex Software Products
- Focused on Manpower

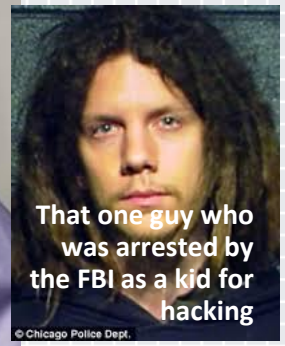
Evidenced By Who We Admire

IT Industry Admires:



InfoSec Industry Admires:

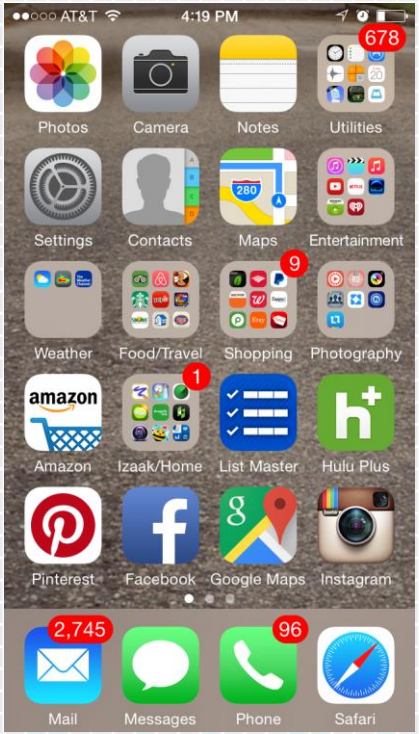




(These photos are not really them)

Evidenced By the Software We Make

IT

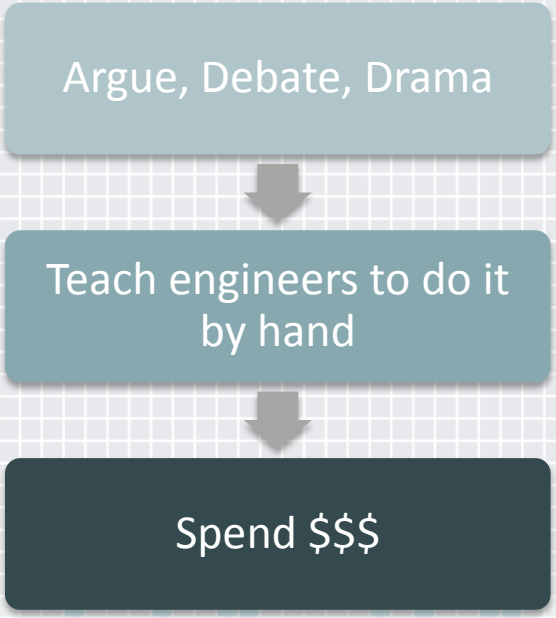


InfoSec

Evidenced By How We Deal With Standards

IT Industry

InfoSec Industry



Why Does This Matter?

While IT isn't perfect,

we shouldn't ignore the problems they have solved.

How InfoSec Works Today

Security Tools	Security Content
IDS / IPS	Provided by Vendor
Firewall	Provided by Vendor
Proxy Servers	Provided by Vendor
Configuration Compliance	Provided by Vendor
Vulnerability Scanning	Provided by Vendor
Host-based agents	Provided by Vendor

Rethink Security Content Strategy

Security Tools	Security Content
IDS / IPS	Provided by Community Y
Firewall	Provided by Community X
Proxy Servers	Provided by Community X and Y
Configuration Compliance	Provided by Vendor X and Community Y
Vulnerability Scanning	Provided by Vendor Y and Community X
Host-based agents	Provided by Vendor C and Community Y

Separate the content from the tooling.

Rethink Security Content Strategy

Security Tools	Security Content
IDS / IPS	STIX / TAXII
Firewall	STIX / TAXII
Proxy Servers	STIX / TAXII
Configuration Compliance	CCE, XCCDF, OVAL
Vulnerability Scanning	CVE, CVSS, OVAL
Host-based agents	STIX/TAXII, OVAL

Maybe even implement some specifications…

Some Hate Standards

They have good reasons!

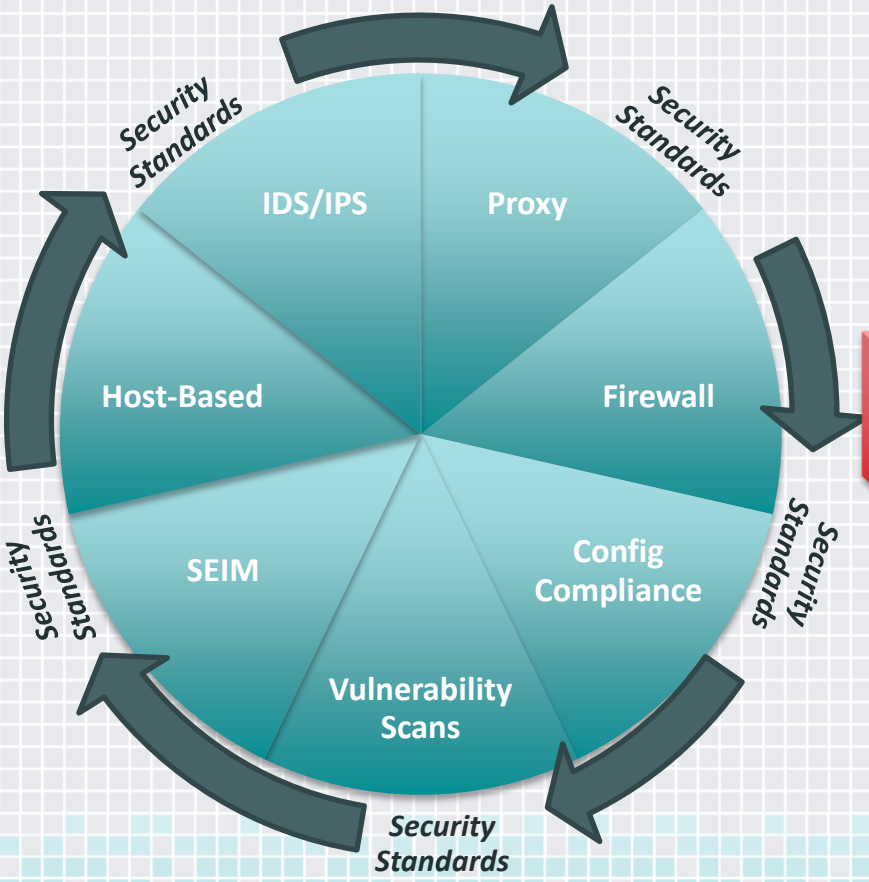
- Specifications take time to take hold
- Critical mass adoption is required
- Industry leaders have to evangelize
- Technologists need to build with them
- Not easy to implement and follow
- Fundamentally a different approach

Some Will Fight Against Me

- **Commoditizes What Only Large Organizations Can Do Today**
- Not-So-Good Reasons
  - Enjoy Vendor Lock-In?
  - Forces a “Manual” Intelligence Workflow
  - Requires Organizations to make Custom Platforms and Software
- Does Standardization Prevent Analysts Doing Analysis?
  - HTML standard didn't stop people from making web pages
  - Standards just get the data into tools
  - Standards can give Analysts the Freedom (Time) for Analysis

Our Security Network Goes From This…

…To This.



Security Content Router

Security Specifications

Community

Community

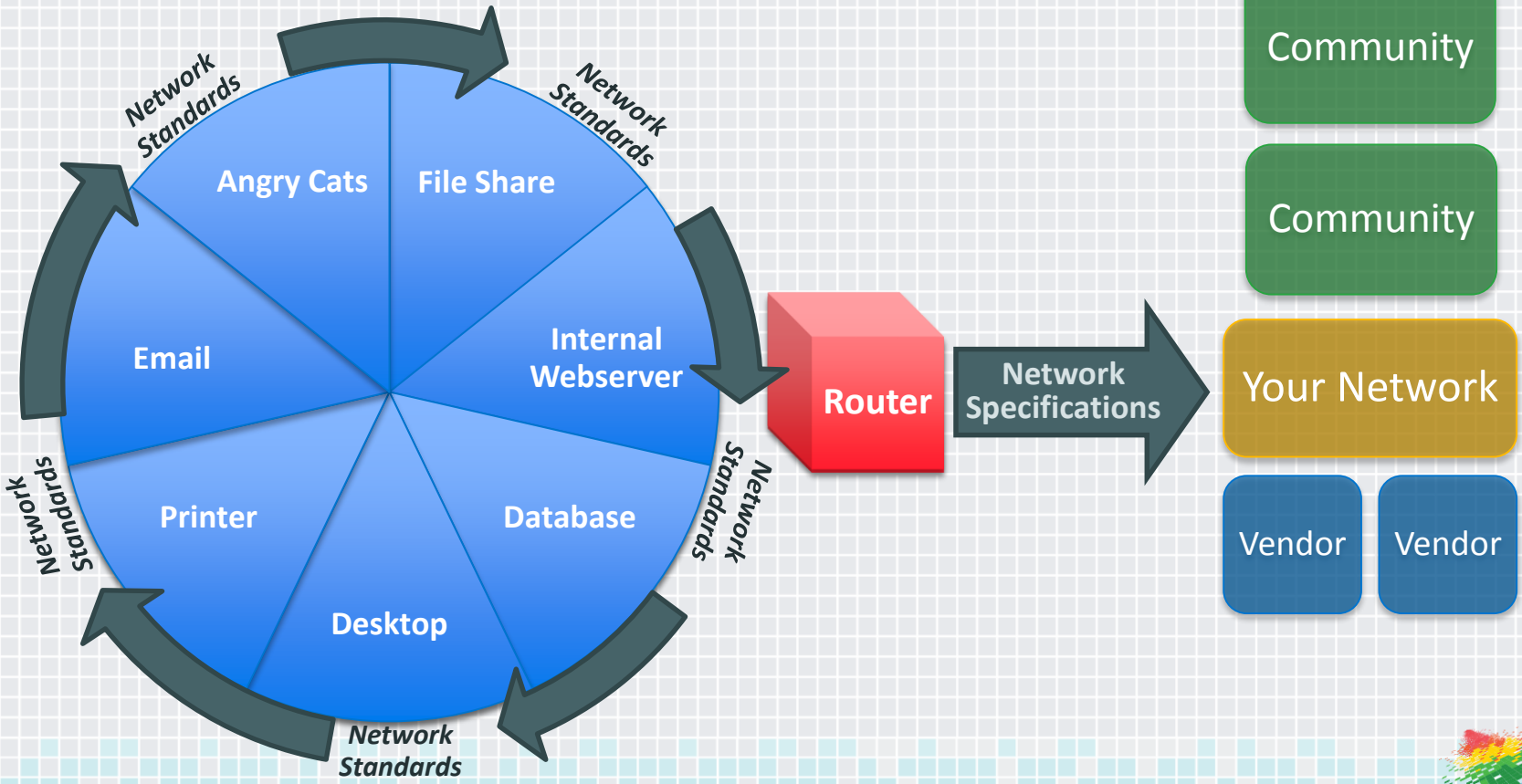
Vendor

Vendor

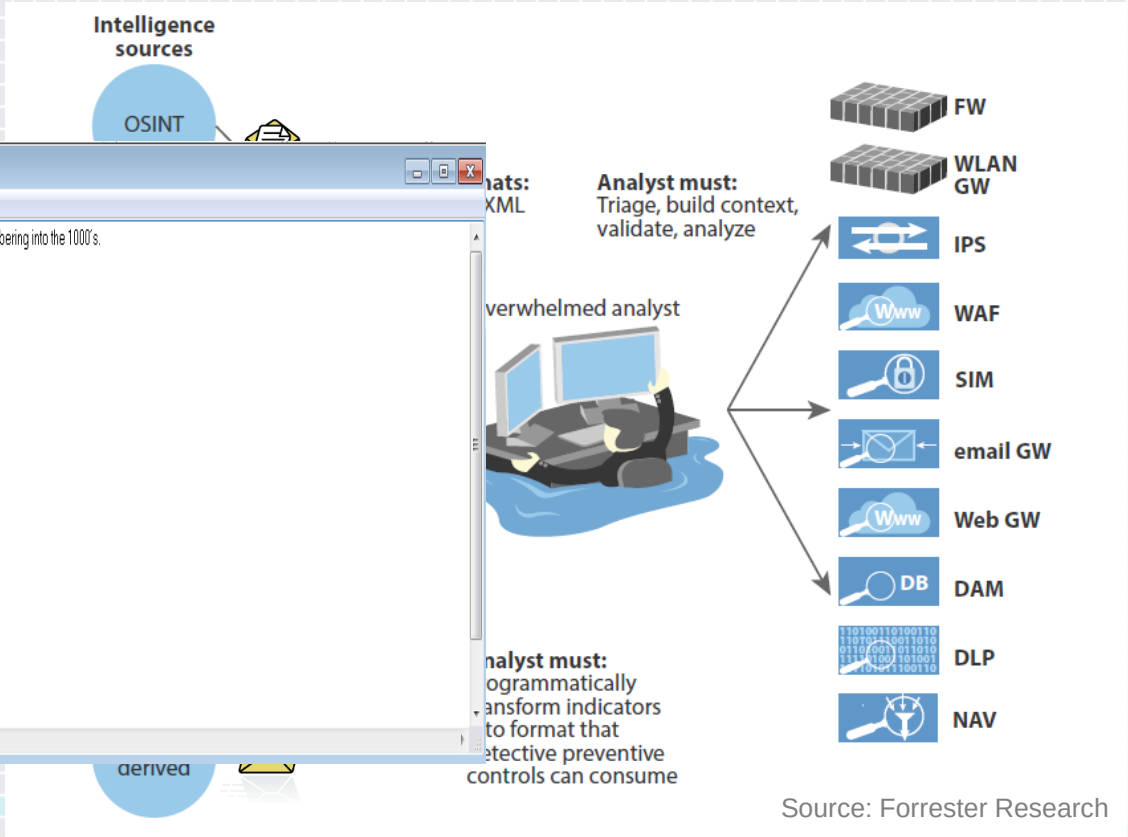
Vendor

Vendor

Look Familiar?



The challenge: process data efficiently



Source: Forrester Research

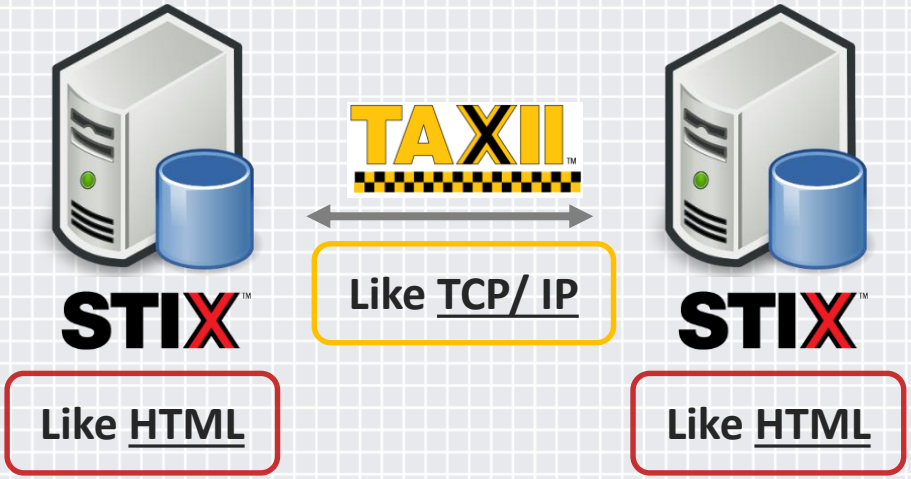
Machines can help, but need a language

- **STIX – Structured Threat Intelligence eXpression**

  Structured language used by machines to describe cyber threats

- **TAXII – Trusted Automated eXchange of Indicator Information**

  Transport mechanism for cyber threat information represented in STIX



STIX Constructs

Atomic

What threat activity are we seeing?

Tactical

What threats should I look for on my networks and systems and why?

Operational

Where has this threat been seen?

What can I do about it?

Strategic

Who is responsible for this threat?

Why do they do this?

What do they do?

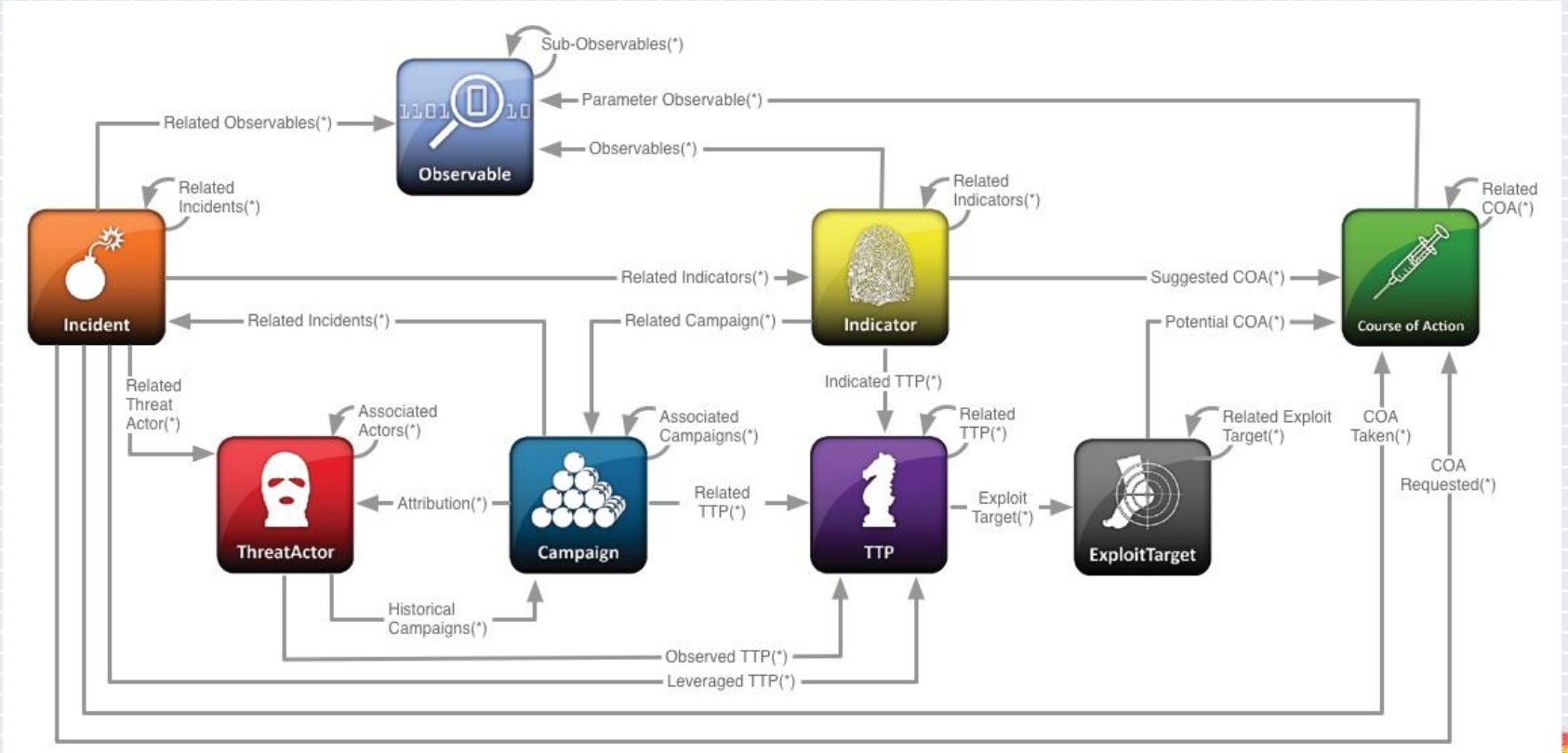
What weaknesses does this threat exploit?

STIX Architecture

The Power of Structured Intelligence

- Key to Effective Strategic Cyber Intelligence Analysis and Threat Tracking
- Ability to Pivot, View, Analyze, and Enrich Complex Relationships
- Most Importantly… We Agree on a Common Language

STIX Architecture



STIX Sample: Email Message Object

```
<cybox:Observable id="cybox:observable-6f45ce72-30c8-11e2-8011-000c291a73d5">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:object-6dc7fc5a-30c8-11e2-8011-000c291a73d5">
        <cybox:Defined_Object xsi:type="EmailMessageObj:EmailMessageObjectType">
          <EmailMessageObj:Attachments>
            <EmailMessageObj:File xsi:type="FileObj:FileObjectType" object_reference="cybox:object-6dcae276-30c8-11e2-8011-000c291a73d5"/>
          </EmailMessageObj:Attachments>
          <EmailMessageObj:Links>
                                <EmailMessageObj:Link type="URL" object_reference="cybox:guid-6dcb5fda-30c8-11e2-8011-000c291a73d5“/>
                                <EmailMessageObj:Link type="URL" object_reference="cybox:guid-6ec9050e-30c8-11e2-8011-000c291a73d5“/>
                    </EmailMessageObj:Links>
          <EmailMessageObj:Header>
            <EmailMessageObj:To>
              <EmailMessageObj:Recipient category="e-mail">
                <AddressObj:Address_Value datatype="String">jsmith@gmail.com</AddressObj:Address_Value>
              </EmailMessageObj:Recipient>
            </EmailMessageObj:To>
            <EmailMessageObj:From category="e-mail">
              <AddressObj:Address_Value datatype="String">jdoe@state.gov</AddressObj:Address_Value>
            </EmailMessageObj:From>
            <EmailMessageObj:Subject datatype="String">Fw:Draft US-China Joint Statement</EmailMessageObj:Subject>
            <EmailMessageObj:Date datatype="DateTime">2011-01-05T12:48:50+08:00</EmailMessageObj:Date>
            <EmailMessageObj:Message_ID datatype="String">
                                                CAF=+=fCSNqaNnR=wom=Y6xP09r_wfKjsm0hvY3wJYTGEzGyPkw@mail.gmail.com
            </EmailMessageObj:Message_ID>
          </EmailMessageObj:Header>
          <EmailMessageObj:Optional_Header>
            <EmailMessageObj:Content-Type datatype="String">
                                                multipart/mixed; boundary=90e6ba10b0e7fbf25104cdd9ad08
            </EmailMessageObj:Content-Type>
            <EmailMessageObj:MIME-Version datatype="String">1.0</EmailMessageObj:MIME-Version>
            <EmailMessageObj:X-Mailer datatype="String">Microsoft CDO for Windows 2000</EmailMessageObj:X-Mailer>
          </EmailMessageObj:Optional_Header>
```

Anatomy of a STIX document

- Package
  - Header
  - Report
    - Reference to Indicator A
    - Reference to Campaign A
  - Indicator A
    - Observable
    - Observable
    - Indicator B
      - Observable
  - Campaign A
    - Reference to Indicator A
- /Package

Envelope

Human readable context

Assertion about fact

Fact

Hey look, it's a composite indicator

STIX/TAXII and Content Quality

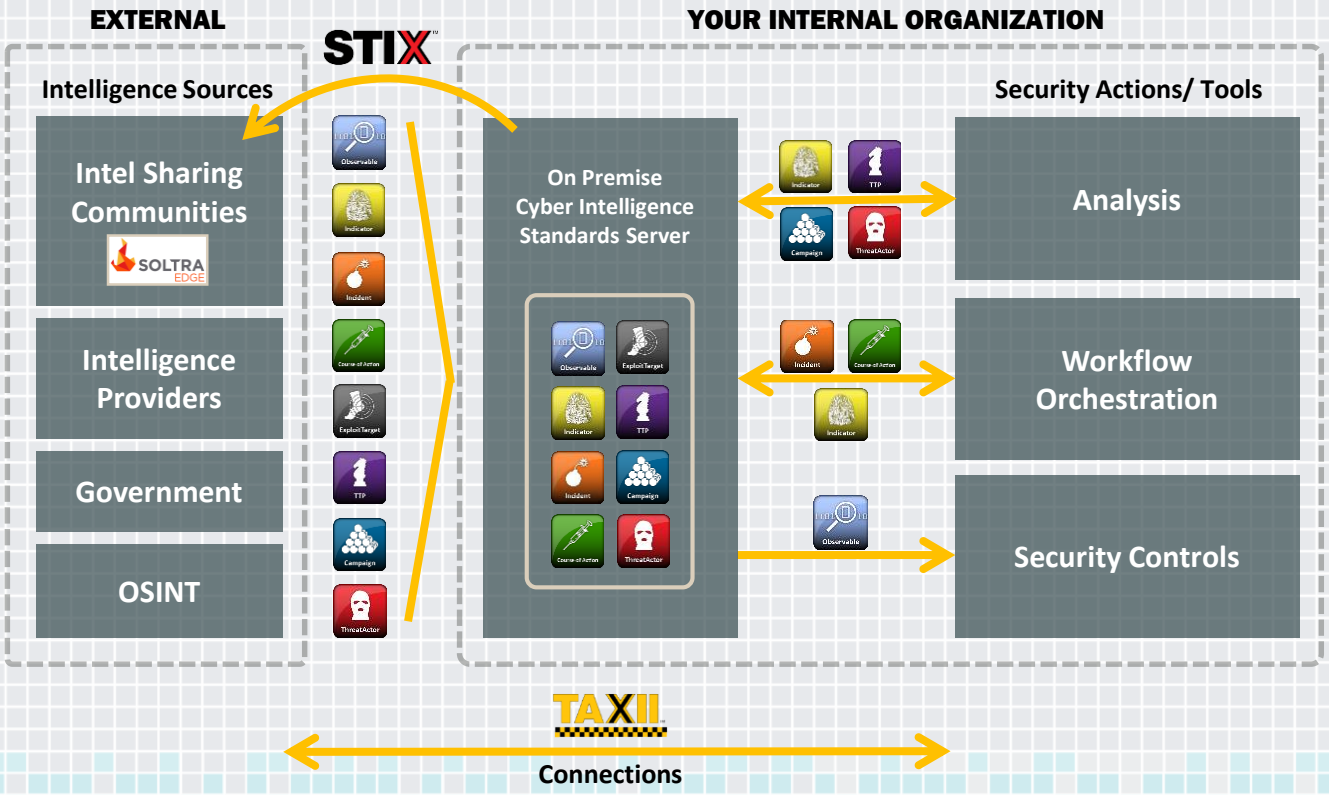
STIX & TAXII Improves Content Quality

- Delivers data to an Analyst Automatically vs Manual
- Integration of Quality Controls within Tooling
- Allow InfoSec Poverty Level Organizations to Participate
- Common Way to Measure Confidence Helps Us Measure Quality

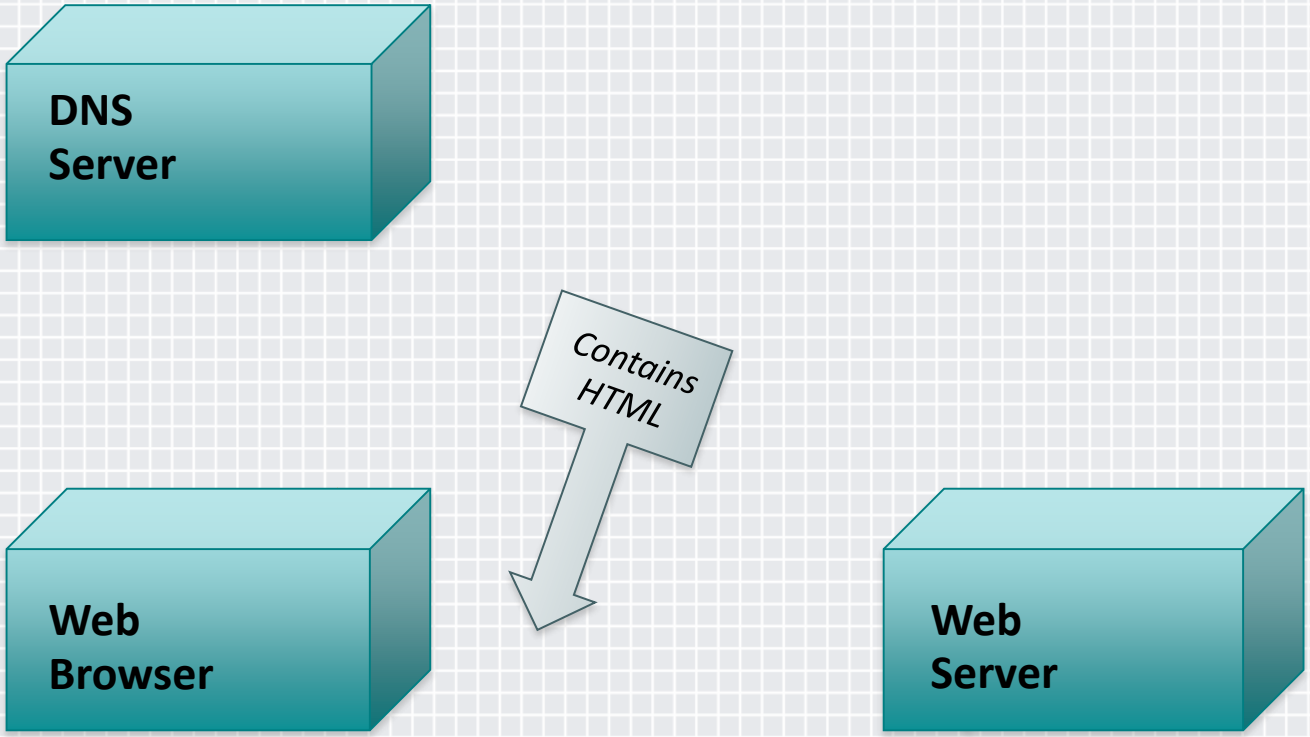
Why an Information Security Network?

- Scales Intelligence Communications
- Anonymizes Easily
- Open to All Who Adopt Security Standards
- No Proprietary and Black-Box Product Stacks or Vendor Lock-In
- Plug-n-Play Integration with Security Tools

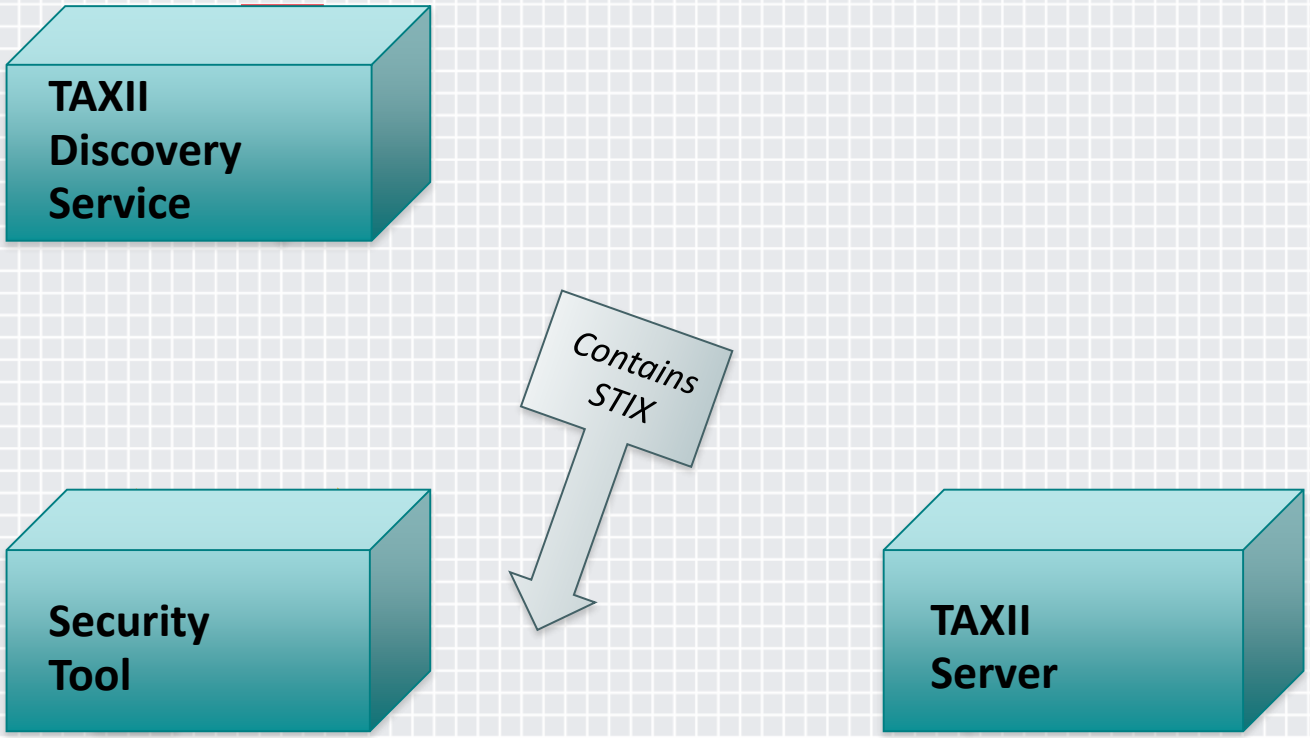
Freedom of an OPEN Ecosystem

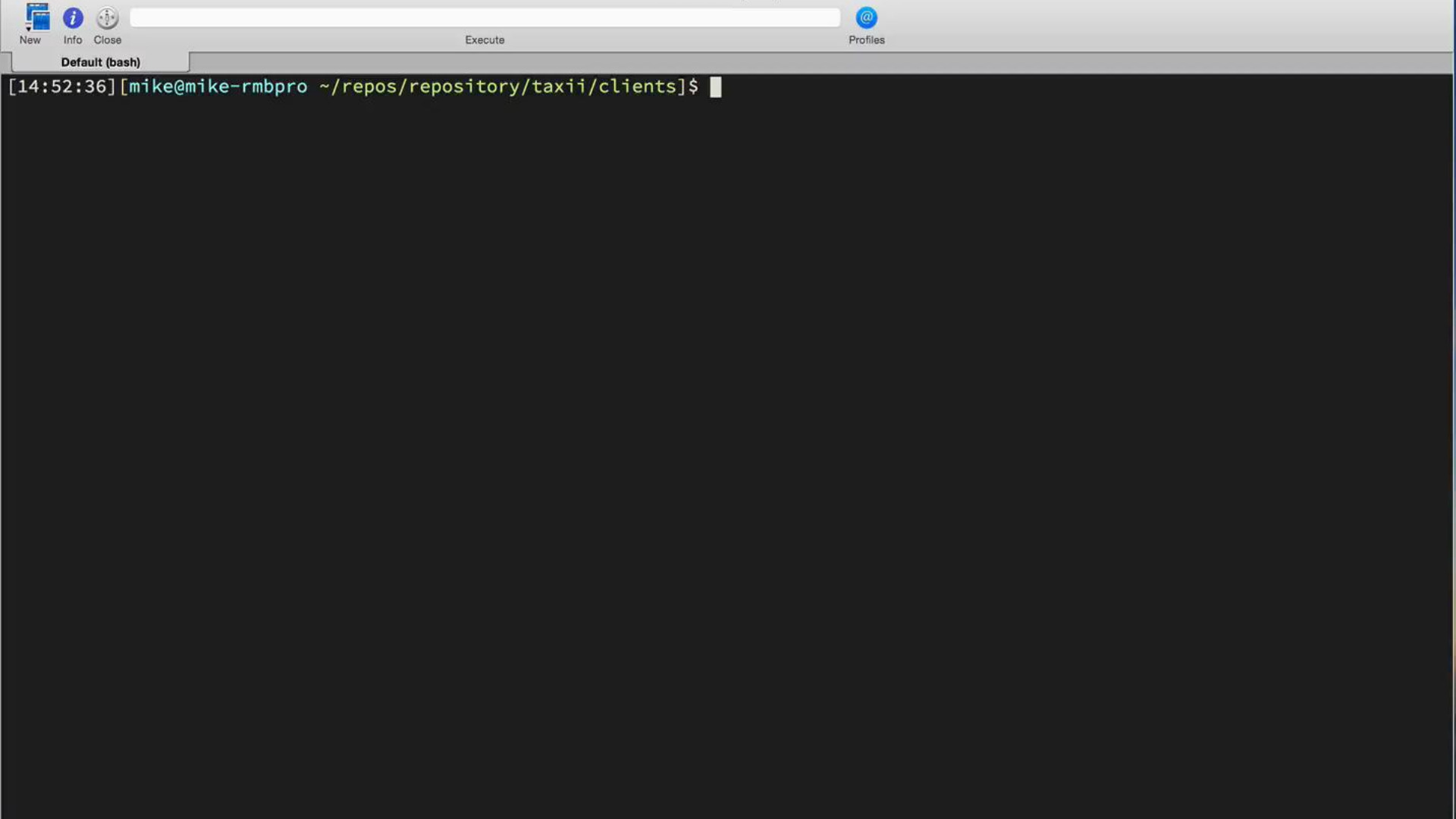


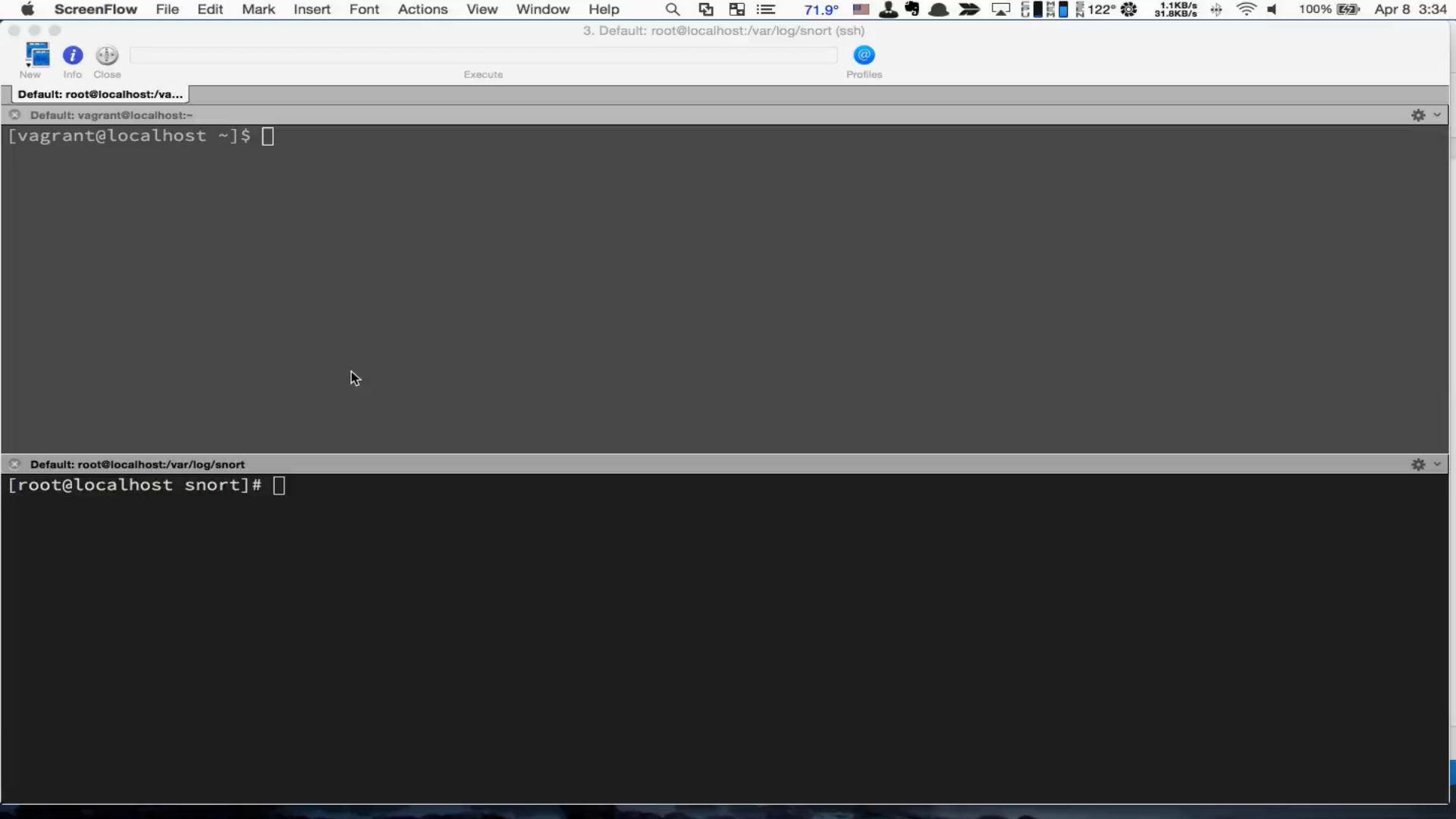
Act as a Client: Example Security Network



Act as a Client: Example Security Network




New
Info
Close
Execute
Profiles
Default (bash)
[14:52:36][mike@mike-rmbpro ~/repos/repository/taxii/clients]$


ScreenFlow File Edit Mark Insert Font Actions View Window Help
71.9°
122°
1.1KB/s
31.8KB/s
100% Apr 8 3:34
3. Default: root@localhost:/var/log/snort (ssh)
New
Info
Close
Execute
Profiles
Default: root@localhost:/va...
Default: vagrant@localhost:~
[vagrant@localhost ~]$
Default: root@localhost:/var/log/snort
[root@localhost snort]#

Welcome to the Edge.

This new Edge installation is empty!

A great way to get started is to try the new STIX **Builders**, connect with a **Peer**, or import STIX data using **TAXII**.

Learn more

Viewing Feed: Default

Create INDICATOR

Top Contributors

Indicator Types

How to: Discovery Request using libtaxii

```
#!/usr/bin/env python

import libtaxii as t

import libtaxii.clients as tc

import libtaxii.messages_11 as tm11



taxii_version = t.VID_TAXII_XML_11

path = '/taxii-discovery-service'

host = 'hailataxii.com'

port = '80'

username = 'guest'

password = 'guest'

client = tc.HttpClient()

client.set_auth_type(tc.HttpClient.AUTH_BASIC)

client.set_auth_credentials({'username': username, 'password': password})

# identify collection management and polling endpoints

request = tm11.DiscoveryRequest(message_id=tm11.generate_message_id())
```

How to: Discovery Request with curl

```
curl -X POST --header "Content-Type:application/xml" \
    --header "X-TAXII-Accept: urn:taxii.mitre.org:message:xml:1.1" \
    --header "X-TAXII-Content-Type: urn:taxii.mitre.org:message:xml:1.1" \
    --header "X-TAXII-Protocol: urn:taxii.mitre.org:protocol:https:1.0" \
    -d '<taxii_11:Discovery_Request
xmlns:taxii="http://taxii.mitre.org/messages/taxii_xml_binding-1"
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
xmlns:tdq="http://taxii.mitre.org/query/taxii_default_query-1"
message_id="69069"/>' \
    "http://hailataxii.com/taxii-discovery-service"
```

How to: Feed Information Request with curl

```
curl -X POST --header "Content-Type:application/xml" \
    --header "X-TAXII-Accept: urn:taxii.mitre.org:message:xml:1.1" \
    --header "X-TAXII-Content-Type: urn:taxii.mitre.org:message:xml:1.1" \
    --header "X-TAXII-Protocol: urn:taxii.mitre.org:protocol:https:1.0" \
    -d '<taxii_11:Collection_Information_Request
xmlns:taxii="http://taxii.mitre.org/messages/taxii_xml_binding-1"
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
xmlns:tdq="http://taxii.mitre.org/query/taxii_default_query-1"
message_id="72511"/>' \
    "http://hailataxii.com/taxii-discovery-service"
```

How to: TAXII Poll Request with curl

```
curl -X POST --header "Content-Type:application/xml" \
   --header "X-TAXII-Accept: urn:taxii.mitre.org:message:xml:1.1" \
   --header "X-TAXII-Content-Type: urn:taxii.mitre.org:message:xml:1.1" \
   --header "X-TAXII-Protocol: urn:taxii.mitre.org:protocol:https:1.0" \
   -d '<taxii_11:Poll_Request xmlns:taxii="http://taxii.mitre.org/messages/taxii_xml_binding-1" xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
xmlns:tdq="http://taxii.mitre.org/query/taxii_default_query-1" message_id="35759" collection_name="system.Default">
  <taxii_11:Exclusive_Begin_Timestamp>2015-03-16T16:04:58.374363+00:00</taxii_11:Exclusive_Begin_Timestamp>
  <taxii_11:Inclusive_End_Timestamp>2015-03-17T16:04:58.374363+00:00</taxii_11:Inclusive_End_Timestamp>
  <taxii_11:Poll_Parameters allow_asynch="false">
    <taxii_11:Response_Type>COUNT_ONLY</taxii_11:Response_Type>
    <taxii_11:Content_Binding binding_id="urn:stix.mitre.org:xml:1.1"/>
  </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>' \
   "http://hailataxii.com/taxii-discovery-service"
```

Example STIX inside a TAXII Poll request

```
<taxii_11:Content_Block xmlns:taxii="http://taxii.mitre.org/messages/taxii_xml_binding-1" xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1" xmlns:tdq="http://taxii.mitre.org/query/taxii_default_query-1">
  <taxii_11:Content_Binding binding_id="urn:stix.mitre.org:xml:1.1.1"/>
  <taxii_11:Content>
    <stix:STIX_Package xmlns:cyboxCommon="http://cybox.mitre.org/common-2" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxVocabs="http://cybox.mitre.org/default_voca
bularies-2" xmlns:marking="http://data-marking.mitre.org/Marking-1" xmlns:simpleMarking="http://data-marking.mitre.org/extensions/MarkingStructure#Simple-1" xmlns:tlpMarking=
"http://data-marking.mitre.org/extensions/MarkingStructure#TLP-1" xmlns:TOUMarking="http://data-marking.mitre.org/extensions/MarkingStructure#Terms_Of_Use-1" xmlns:opensource
="http://hailataxii.com" xmlns:edge="http://soltra.com/" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:stixVocab
s="http://stix.mitre.org/default_vocabularies-1" xmlns:stix="http://stix.mitre.org/stix-1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="edge:Package-bfb3d64a-392
0-452b-8ad0-7dea7dd4be64" version="1.1.1" timestamp="2015-03-17T15:45:54.866228+00:00">
    <stix:STIX_Header>
      <stix:Handling>
        <marking:Marking>
          <marking:Controlled_Structure>../../../../descendant-or-self::node()</marking:Controlled_Structure>
          <marking:Marking_Structure xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
          <marking:Marking_Structure xsi:type="TOUMarking:TermsOfUseMarkingStructureType">
            <TOUMarking:Terms_Of_Use>torstatus.blutmagie.de | http://torstatus.blutmagie.de - HailATaxii.com (HAT) has made a 'best effort' attempt to find/determined
 the TOU (Term of Use) for this site's data, however none was found.
          </marking:Marking_Structure>
</stix:Handling>
    </stix:STIX_Header>
    <stix:Indicators>
      <stix:Indicator id="opensource:indicator-0b8f7a33-adc0-4c25-b412-7a7574af4aac" timestamp="2015-03-17T02:05:07.913185+00:00" xsi:type="indicator:IndicatorType" version
="2.1.1">
        <indicator:Title> This domain host178-25-dynamic.250-95-r.retail.telecomitalia.it has been identified as a TOR network "Exit Point" router</indicator:Title>
        <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
<indicator:Description> torstatus.blutmagie.de has identified this domain host178-25-dynamic.250-95-r.retail.telecomitalia.it as a TOR network "Exit Point" router
, which appears to be located in Italy.
 RawData: {'Bandwidth (KB/s)': 0, 'IP Address': u'95.250.25.178', 'Flags': {'Flag - Named': 0, 'Flag - Stable': 0, 'Flag - Bad Exit': 0, 'Flag - Authority': 0, 'Flag - Valid'
: 1, 'Flag - Guard': 0, 'Flag - Hibernating': 0, 'Flag - Fast': 0, 'Flag - Running': 1, 'Flag - Exit': 0, 'Flag - V2Dir': 0}, 'Platform': u'Tor 0.2.4.24 on Linux', 'Hostname': u'host178-25-dynamic.250-95-r.retail.telecomitalia.it', 'Uptime (Hours)': 5, 'Ports':
{'ORPort': 9001, 'DirPort': None}, 'Router Name': u'stratmikefend', 'Country Code': u'IT'}</indicator:Description>
        <indicator:Observable idref="opensource:Observable-ed98f4db-8c46-4468-9fd1-c0c8e92c144e">
        </indicator:Observable>
        <indicator:Producer>
          <stixCommon:Identity id="opensource:Identity-e04863ee-0352-4a38-a458-fb8c1b5ce844">
            <stixCommon:Name>torstatus.blutmagie.de</stixCommon:Name>
          </stixCommon:Identity>
          <stixCommon:Time>
            <cyboxCommon:Received_Time>2015-03-17T02:05:04+00:00</cyboxCommon:Received_Time>
          </stixCommon:Time>
        </indicator:Producer>
      </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
  </taxii_11:Content>
  <taxii_11:Timestamp_Label>2015-03-17T15:45:54.866768+00:00</taxii_11:Timestamp_Label>
</taxii_11:Content_Block>
```

How to: Convert STIX into Something Interesting

- String manipulation We Have Been Doing for 40+ Years.
- Run Soltra Edge Converter (Adapter) on STIX Directly,
- Or… use Python libraries to Ingest STIX for Conversion
- Integrate, Rinse, Repeat.

Use Cases

- Create SIEM Watch Lists
- Generate Signatures for your Host-Based Tools
- Create IDS Signatures
- Query Non-Structured Data Stores
- Intelligence Sharing

Intelligence Sharing

- Producer/ Consumer Ecosystem
- Producer = Intelligence Vendor, Intel Author, Tools, etc
- Consumer = Intelligence Consumer, Analyst, Tools
- Can Connect to Network and Share Intelligence
- Is This Really Sharing?

Intelligence Sharing

- Measuring Success → Everyone Creating New Indicators
  - Intelligence Communication
- Consumers Can Still Give Back to the Community
  - Generation of Sightings
  - Notification of False Positives
  - Identification of Benign Observables
  - Quality Measurement of Sources

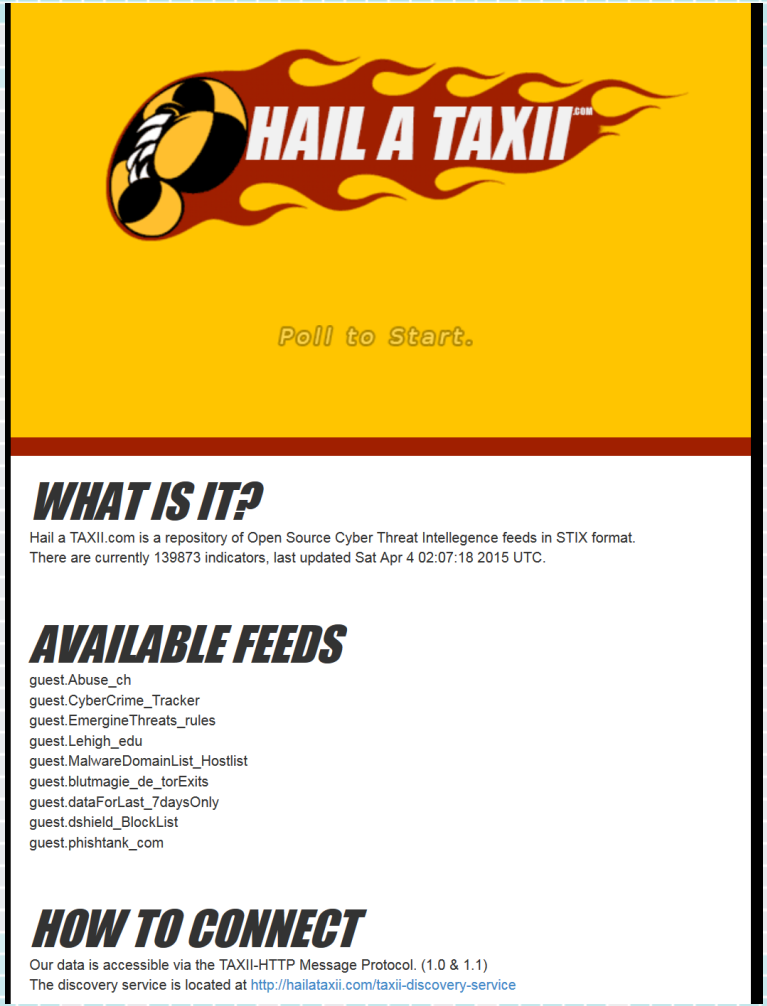
Why “Sharing” Matters

- **Friends in a Sharing Group** – probably relevant intelligence
- **Industry Peers** – definitely relevant intelligence
- **ISACs** – definitely relevant intelligence
- **Random Vendor Honeypot** – probably not much relevant intel
- **Random Sensor at Unknown Location** – not so much…

IS Standards are no longer only theory

- Organizations are Doing this Today
- Over 2,000 downloads of Soltra Edge (a STIX TAXII server)
- >1,500 Unique Visits to HailATAXII.com (free OSINT STIX)
- >100,000 TAXII Requests a Day at HailATAXII.com
- Some of the Largest Banks use STIX/TAXII
- Used by Several of the Largest ISACs

Not a Theory


HAIL A TAXII.com
Poll to Start.
WHAT IS IT?
Hail a TAXII.com is a repository of Open Source Cyber Threat Intellegence feeds in STIX format.
There are currently 139873 indicators, last updated Sat Apr 4 02:07:18 2015 UTC.
AVAILABLE FEEDS
guest.Abuse_ch
guest.CyberCrime_Tracker
guest.EmergingThreats_rules
guest.Lehigh_edu
guest.MalwareDomainList_Hostlist
guest.blutmagie_de_torExits
guest.dataForLast_7daysOnly
guest.dshield_BlockList
guest.phishtank_com
HOW TO CONNECT
Our data is accessible via the TAXII-HTTP Message Protocol. (1.0 & 1.1)
The discovery service is located at http://hailataxii.com/taxii-discovery-service

Other TAXII Servers

- Many Large ISACs
- Federal Intelligence Sources
- Intelligence Vendors
- Intelligence Communities
- Thousands of Soltra Instances

TAXII Enabled Clients

- Most major SIEMs adopted STIX TAXII (or on their 2015 roadmap)
- Proxy Vendor
- Major Firewall Vendor
- Many More are Under Development

Take a page out of the IT book

InfoSec Problems are Not New

- Are these New Problems?
  - Moving Data from Point A to Point B
  - Data Conversion
  - Automation
  - Product Integration
  - Vendor Lock-In
- How would a technologist solve these problems?

Apply what you've learned today:

Go Forth and Build a Security Network

- When You Get Back to Work
  - Ask Your Vendors When They Are Adopting STIX & TAXII
  - Make Purchasing Decisions Based on Their Responses
- Shortly Thereafter
  - Find a STIX and TAXII Platform
  - Demo and POC
- Goal
  - Walk Before Run – Make a single security tool "Detect" Based on Your STIX Intelligence

More Opportunities

- We'll Continue to Abstract Away and Hide Standards Use
- Vendors Listen to You, the Customer – Ask Them to Adopt
- Use STIX & TAXII to Measure Your Intelligence Sources
- **Think Strategically to Move our Industry Forward**