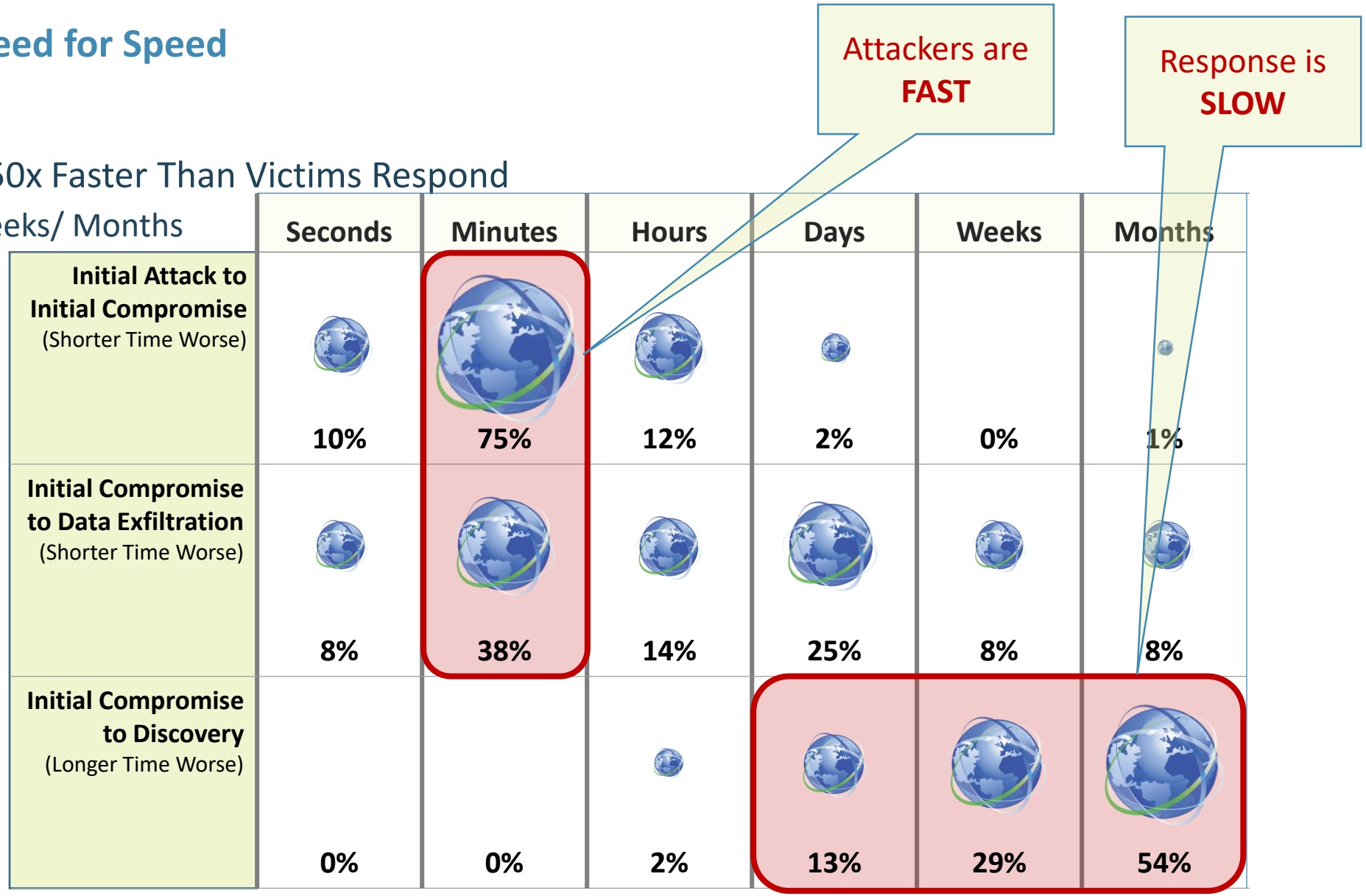
Cyber Threat Intelligence
CTI

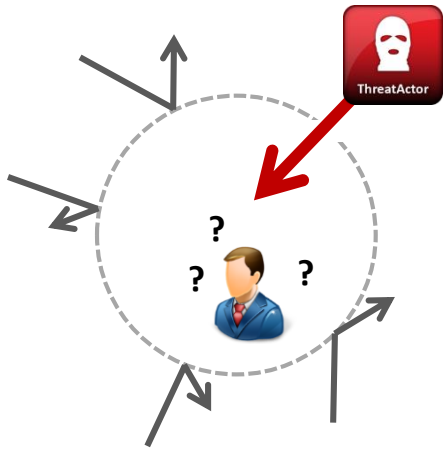
The Need for Speed

- Attackers Act 150x Faster Than Victims Respond
  - Minutes vs. Weeks/ Months



Evolution of Cyber Security Defense

Yesterday's Security



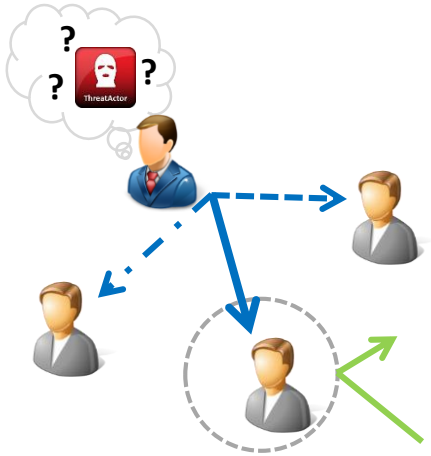
Network Awareness

Protect the perimeter and patch the holes to keep out threats share knowledge internally.

Increasing Cyber Risks

- Malicious actors have become much more sophisticated & money driven.
- Losses to US companies now in the tens of millions; WW hundreds of millions.
- Cyber Risks are now ranked #3 overall corporate risk on Lloyd's 2013 Risk Index.

Present Day Problem



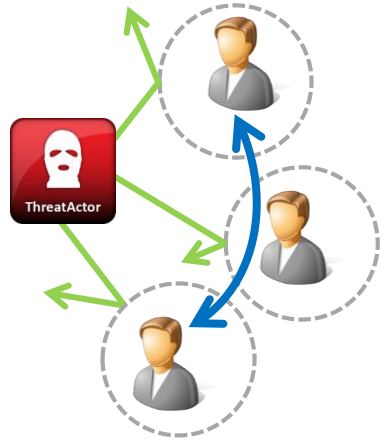
Intelligence Sharing

Identify and track threats, incorporate knowledge and **share what you know manually** to trusted others.

Manually Sharing Ineffective

- Time consuming and ineffective in raising the costs to the attackers.
- Not all cyber intelligence is processed; probably less than 2% overall = high risk.
- No way to enforce cyber intelligence sharing policy = non-compliance.

Future Solution



Situational Awareness

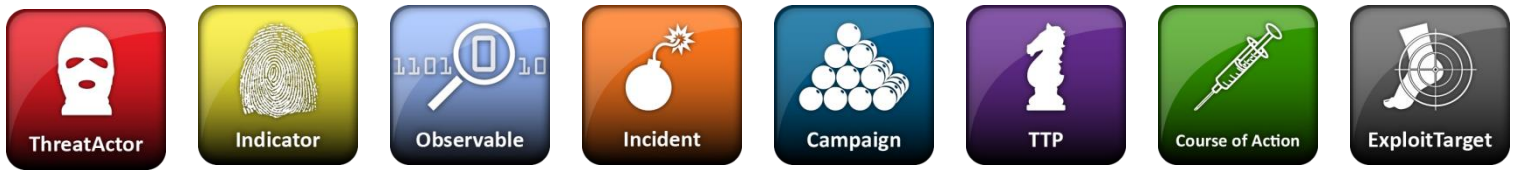
Automate sharing – develop clearer picture from all observers' input and pro-actively mitigate.

We are Solving the Problem

- Security standards are maturing
- FS-ISAC has become the trusted model for sharing industry threat intelligence.
- Soltra Edge Cyber Intelligence Sharing Platform revolutionizing sharing and utilization of threat intelligence.

What is cyber intelligence

- Information about cyber threats
  - Bad people, things, or events
  - Plans to attack victims
  - Tactics used by bad people
  - Actions to deal with bad events
  - Weaknesses targeted by bad people



Why cyber intelligence is important

- Tactical Uses
  - Proactively detect or defend against attacks before they happen
  - Diagnose infected corporate systems
- Strategic Uses
  - Compile and track bad people or things that don't like you, your industry, or your company – report out and potentially sent to authorities
  - Improve your security posture - The more you understand the things, people, and organizations that are attacking you, the have the better you can defend yourself

- Intelligence Can Help Protect You!

Where Does cyber intelligence Come From?

- Buy It
  - Purchase from professional intelligence providers
- Collect for Free
  - From inside your organizational environment
  - The Internet has many Open Source Intelligence (OSINT) feeds available
- From Friends
  - Information Sharing Communities or ISACs
  - Business partners, associates, peers, etc.
- Get from Authorities
  - Government .

Intelligence Life-Cycle

- What Do We Do With It? (What are we supposed to do with it?)

Security Operations Intelligence Starts Here

#4 Disseminate

#3 Analyze

#1 Collect

#2 Process

Graphic Source: FBI

Machines Can Help, But First…

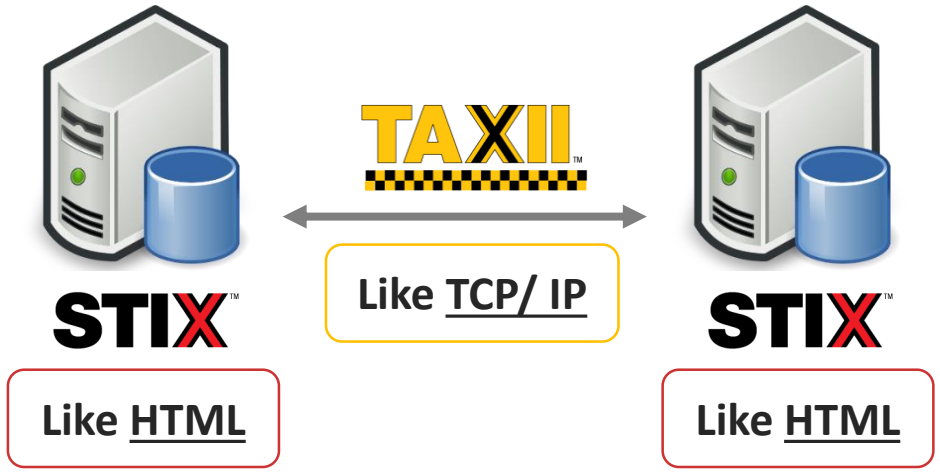
…Machines Need a Language to Talk about Threats

STIX - Structured Threat Intelligence eXpression

- Structured language used by machines to describe cyber threats

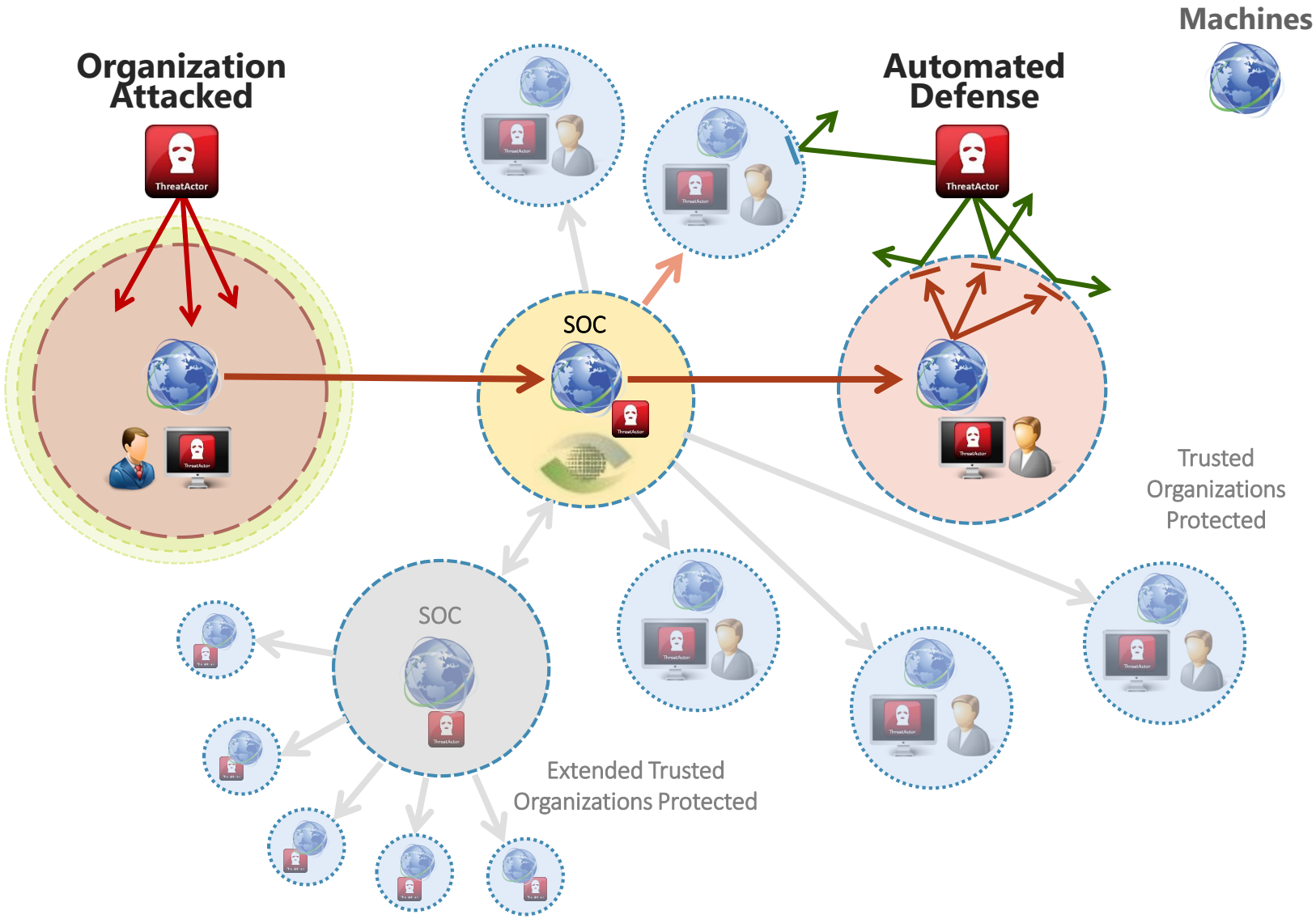
TAXII – Trusted Automated eXchange of Indicator Information

- Transport mechanism for cyber threat information represented in STIX



stix.mitre.org taxii.mitre.org

Intelligence driven Community Defense



STIX Constructs

- An open standard to categorize cyber threat intelligence information

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?

What weaknesses does this threat exploit?

Strategic

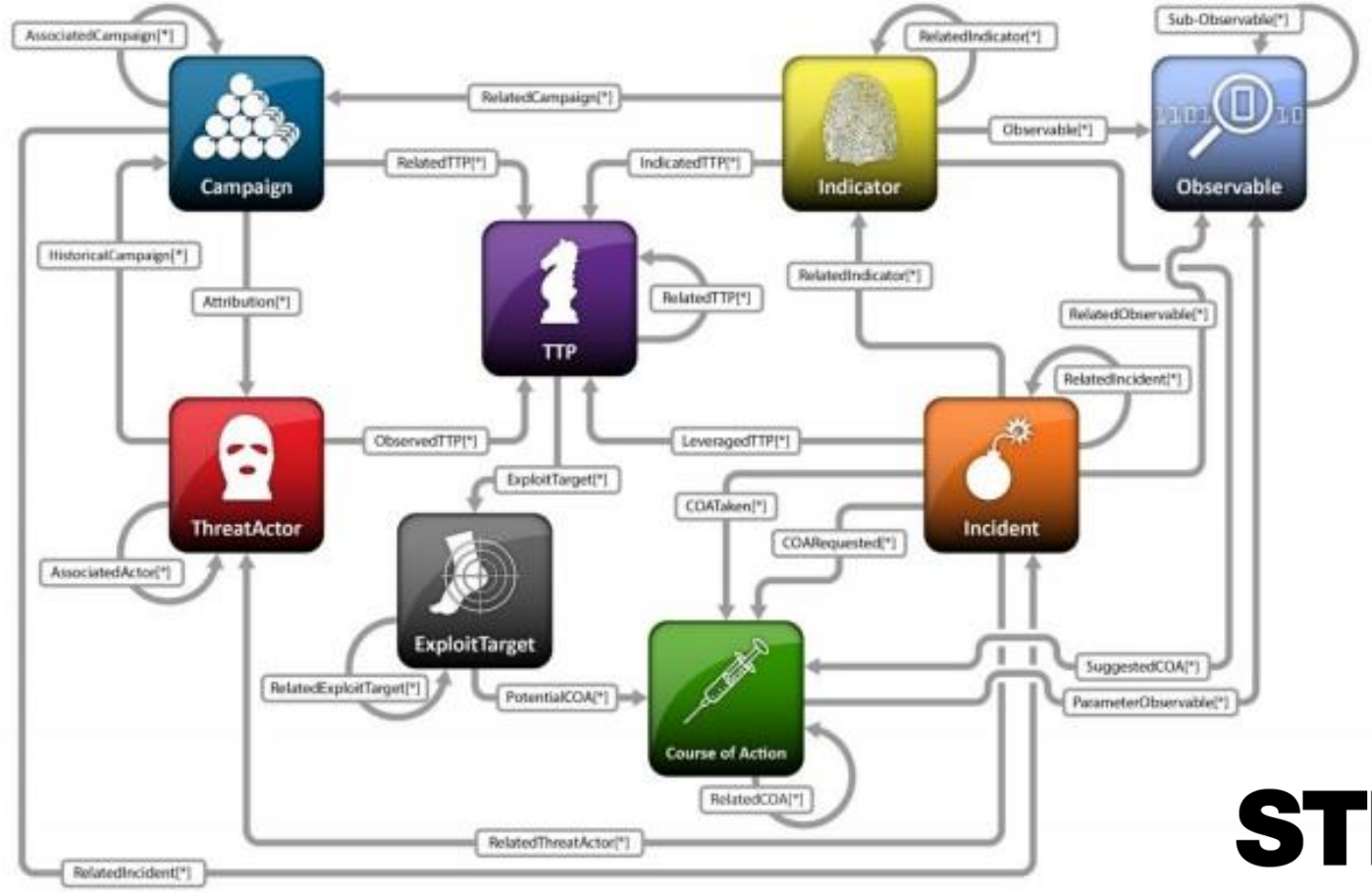
Who is responsible for this threat?

Why do they do this?

What do they do?

STIX Architecture

- The Power of Structured Intelligence
  - Key to effective strategic cyber intelligence analysis and threat tracking



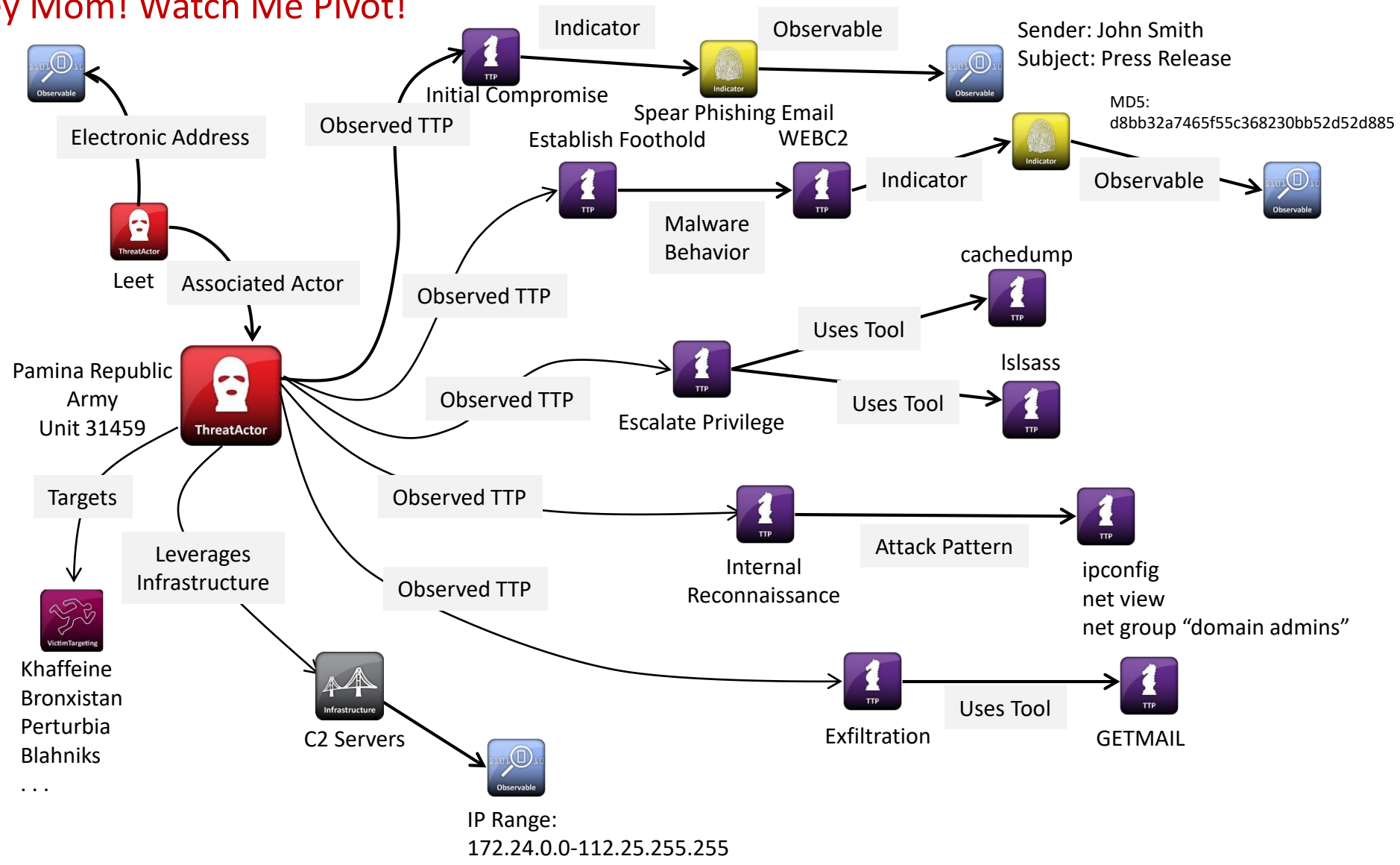
STIX Sample

- 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>
```

How Humans View Intelligence

- Hey Mom! Watch Me Pivot!



Maturing an Ecosystem

- **Sharing Communities**
  - CSIRTs
  - Government
  - Individuals
- **Security Vendors**
  - Service Providers
  - Vendor Products
- **Consumers of Security Products and Intelligence**
  - Large
  - Medium
  - Small

Visualization

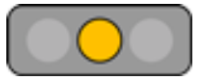
Example :

STIX Visualizer : https://oasis-open.github.io/cti-stix-visualization/
short URL: https://bit.ly/2W8nzYO

Examples : https://oasis-open.github.io/cti-documentation/stix/examples.html

short URL: https://bit.ly/2UMuUNK

15

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

16

PAP (Permissible Actions Protocol)

PAP (for Permissible Actions Protocol) aims to indicate to analyst the posture to adopt: how much we accept that the attacker detect the current analysis.
As for TLP, PAP is declined in 4 values:

- **RED (3):** Non-detectable actions only. Recipients may not use PAP:RED information on the network. Only passive actions on logs, that are not detectable from the outside.

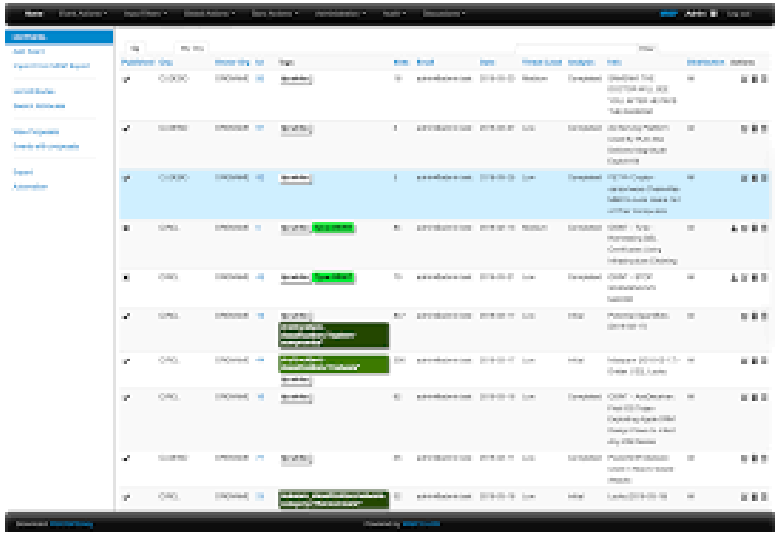
- **AMBER (2):** Passive cross check. Recipients may use PAP:AMBER information for conducting online checks, like using services provided by third parties (e.g. VirusTotal), or set up a monitoring honeypot.

- **GREEN (1):** Active actions allowed. Recipients may use PAP:GREEN information to ping the target, block incoming/outgoing traffic from/to the target or specifically configure honeypots to interact with the target.

- WHITE (0): No restrictions in using this information.

17

MISP
Threat Sharing



Demo

- https://misppriv.circl.lu/users/login

18