RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-F01

STIX, TAXII, CISA: The impact of the US Cybersecurity Information Sharing Act of 2015

Bret Jordan CISSP

Director of Security Architecture
Blue Coat Systems

Mark Davidson

Director of Software Development
Soltra

#RSAC

Today we will answer

- What is CISA?
- Will CISA improve cyber information sharing?
- Does CISA enable spying?
- How can we improve threat sharing?
- How can STIX and TAXII help?

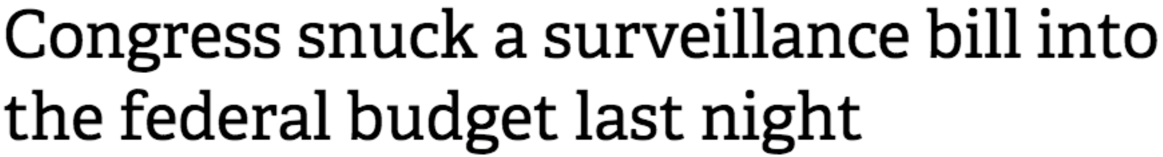
Cybersecurity Information Sharing Act 2015

CISA at a glance

- Started as CISPA in November 2011
- Passed in December 2015
  - Claims to enhance information sharing
  - Widely criticized for enabling spying
  - Is not going away any time soon
- Lets look at a few headlines to see what do people have said

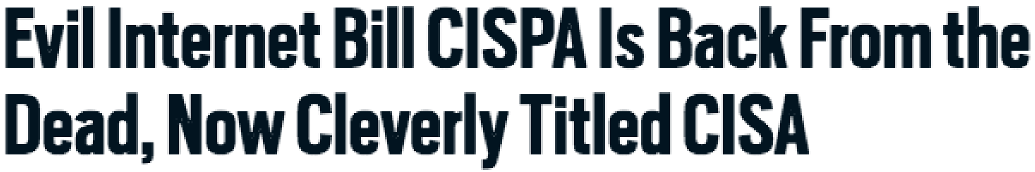
Headlines

THE VERGE



Congress snuck a surveillance bill into the federal budget last night

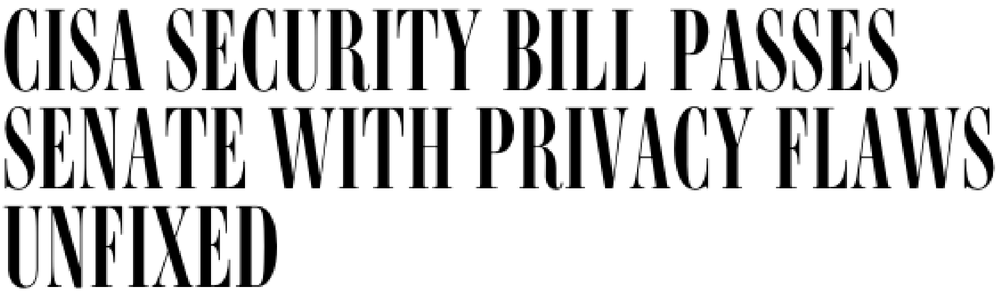
KELLY WEILL



Evil Internet Bill CISPA Is Back From the Dead, Now Cleverly Titled CISA

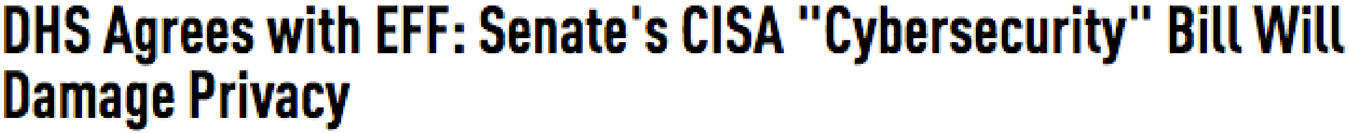
THE DAILY BEAST

WIRED



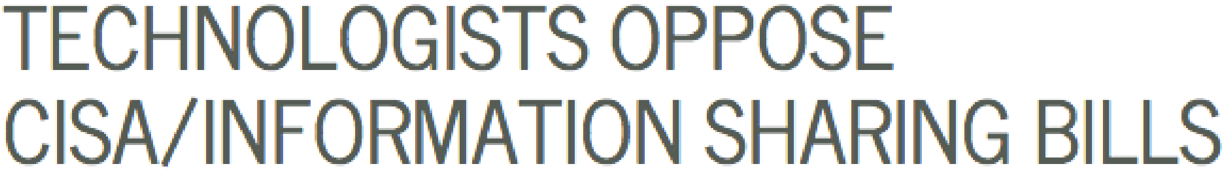
CISA SECURITY BILL PASSES SENATE WITH PRIVACY FLAWS UNFIXED

Headlines – cont.



DHS Agrees with EFF: Senate's CISA "Cybersecurity" Bill Will Damage Privacy

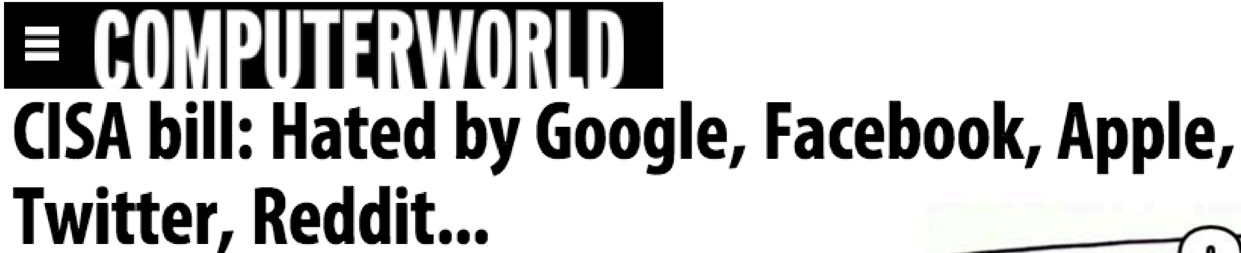
Stanford Law School



TECHNOLOGISTS OPPOSE CISA/INFORMATION SHARING BILLS

The Center for Internet and Society

Headlines – cont.



≡ COMPUTERWORLD

CISA bill: Hated by Google, Facebook, Apple, Twitter, Reddit...

Headlines – cont.

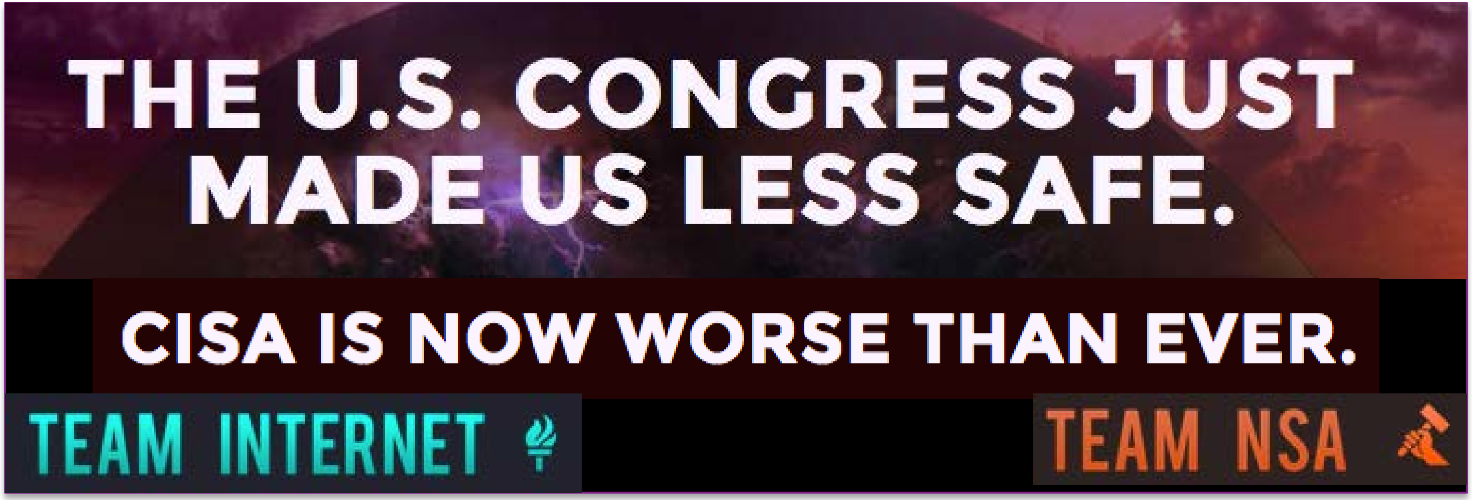
- CISA: No Safe Harbor
- The US legislature has encouraged American companies to share threat intelligence with the government by absolving them of some of the data privacy liability concerns that stilled their tongues in the past.
- Yet, the federal government can do nothing to absolve companies of their duties to European data privacy regulations.

InformationWeek DARKReading

The Messy Situation & Not-Very-Safe Harbor

Headlines – cont.

- And some have gone so far as to create a score board site
  - DecidetheFuture.org/cisa/



THE U.S. CONGRESS JUST MADE US LESS SAFE.

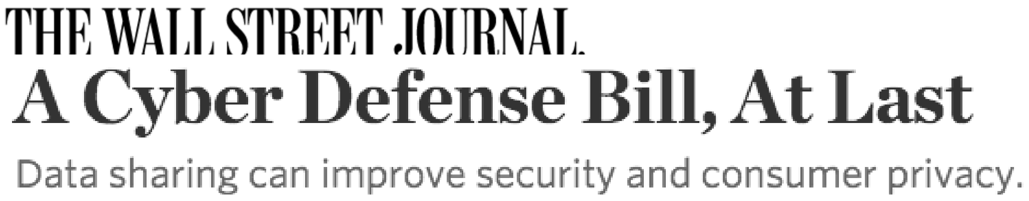
CISA IS NOW WORSE THAN EVER.

TEAM INTERNET

TEAM NSA

Headlines – cont.

- Apparently some people publically like CISA
  - Some just quietly agree with it



THE WALL STREET JOURNAL.

A Cyber Defense Bill, At Last

Data sharing can improve security and consumer privacy.

FINANCIAL SERVICES | Information Sharing and Analysis Center

"The Financial Services Sector Coordinating Council (FSSCC) applauds the U.S. Senate

Headlines – cont.

- Best summary we found
- CISA addresses the manner in which the federal government and non-federal entities may share information about cyber threats and the defensive measures they may take to combat those threats.

PUBLISHED BY

FOLEY HOAG LLP

SECURITY, PRIVACY AND THE LAW

LEGAL PERSPECTIVES ON THE EXPANDING UNIVERSE OF INFORMATION SECURITY & PRIVACY ISSUES

Why do people not like CISA?

- Spying bill in disguise and a threat to personal privacy
- Broad immunity clauses and vague definitions
- Aggressive spying authorities
- Would not have helped the recent breaches
- It allows vast amounts of PII data to be shared with the gov’t

Questions we should be asking

- Why was CISA implemented in the first place?
- Can CISA improve operational cyber security?
- What are the real privacy issues with CISA?
- Does CISA actually enable spying and force companies to share?
- What personal information is actually contained in CTI?
- Is CISA the magic solution? Or are there other roadblocks?

CISA conclusions

- Helps information sharing a little
  - Does not solve everything
  - Will not make organizations instantly safe from cyber attacks
  - Represents one piece of the cyber security puzzle
- Spying claims **have not** been disproven
- Heavy on sensationalism light on action
- Does not require organizations to participate or share anything

Cyber Threat Intelligence (CTI) Sharing

What is information sharing?

- We believe that everyone gets the general idea
  - Fundamentally, we need an ecosystem where **actionable CTI is shared automatically** across verticals and public / private sectors in near real-time to address the ever increasing cyber threat landscape
- What are the benefits?

Why should you share CTI?

- Gain proactive defense
- Reduce your long-term risk
- Potentially lower your cyber insurance premiums
- Enable herd immunity
- Improve your operational understanding of the threats

The history of CTI is colorful

- Over the years the security community and various vendors have proposed several solution to this problem with mixed levels of success, those proposed solutions, to name a few, are:
  - IODEF (2007), CIF (2009), VERIS (2010)
  - OpenIOC (2011), MILE (2011)
  - OTX (2012), OpenTPX (2015)
  - ThreatExchange (2015)
  - CybOX (2012), STIX (2013), TAXII (2013)

The history of CTI is colorful – cont.

- Despite the competition and various attempts at threat sharing, STIX, TAXII, and CybOX have quickly gained world-wide support from an international community of financial services, CERTS, vendors, governments, industrial control systems, and enterprise users

Threat sharing happens today

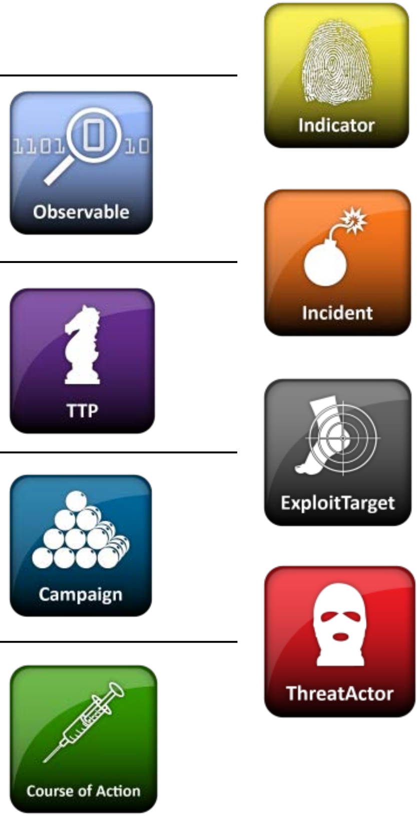
- It is important to note that cyber threat sharing has been going on for some time, long before CISA
  - ISACs, ISAOs, eco-systems, opensource, and commercial offerings
- The problem is, the way sharing has been done to date
  - Generally unstructured data
  - Ad-hoc manual communications such as email / IM / IRC / paper
  - Some automated tools along with DIY solutions

Future of CTI

- Simplicity and ease of use
  - To help this, STIX, TAXII, and CybOX are moving to JSON
  - STIX 2.0 is explicitly graph based
  - TAXII 2.0 is native web
- CTI is working towards plug-n-play interoperability
- Real-time communication of indicators and sightings across products, organizations, and eco-systems

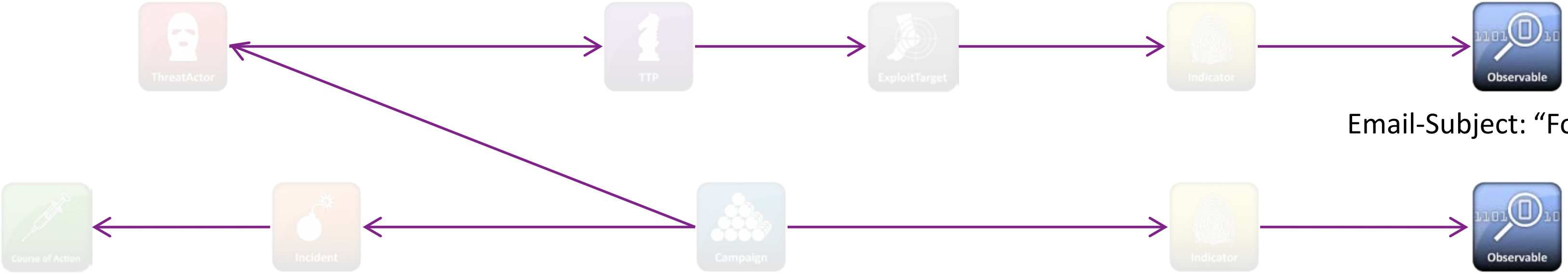
The problems STIX solves

- How to describe the threat?
- How to spot the indicator?
- Where was this seen?
- What exactly were they doing an how?
- What are they looking to exploit?
- Why were they doing it?
- Who is responsible for this threat?
- What can I do about it?



Anatomy of threat intelligence

- Cyber Observables
  - Identifies the specific patterns observed (either static or dynamic)
  - Examples
    - An incoming network connection from a particular IP address
    - Email subject line, MD5 / SHA1 hash of a file

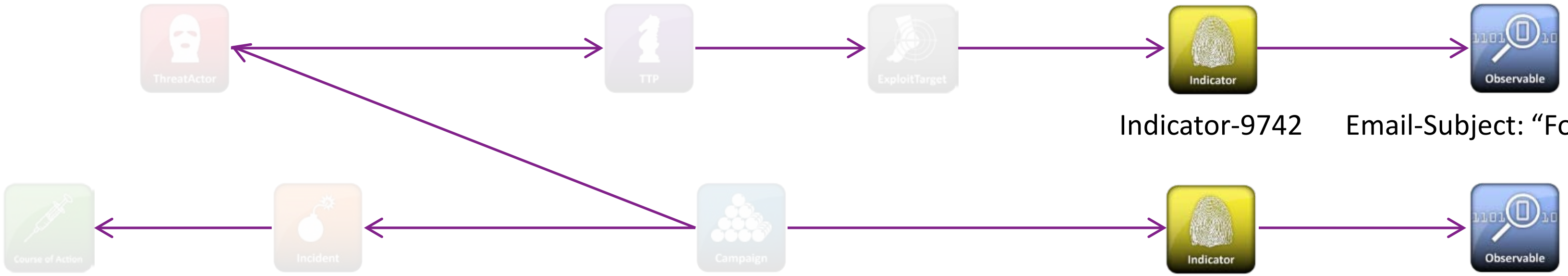


Email-Subject: “Follow-up”

MD5 hash…

Anatomy of threat intelligence – cont.

- Indicators
  - Identifies contextual information about observables
  - Examples
    - Traffic seen from a range of IP addresses it indicates a DDoS attack
    - File seen with a SHA256 hash it indicates the presence of Poison Ivy



Indicator-9742

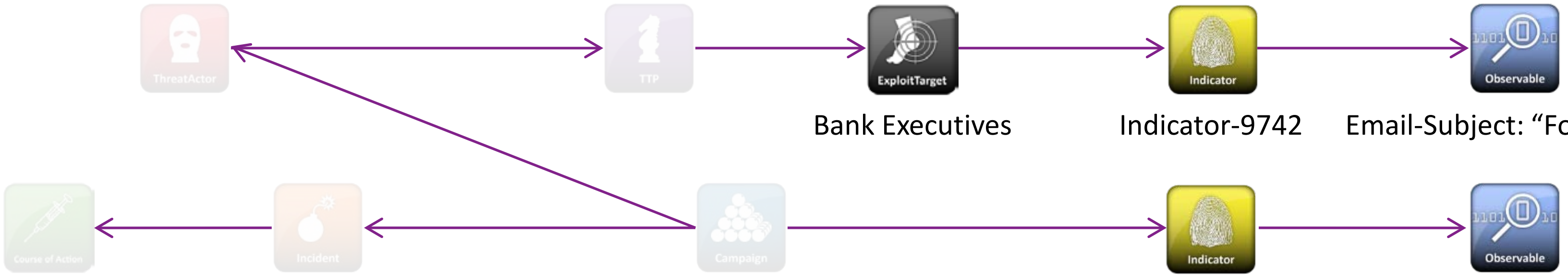
Email-Subject: “Follow-up”

MD5 hash…

Indicator-985

Anatomy of threat intelligence – cont.

- Exploit Targets
  - Identify vulnerabilities or weaknesses that may be targeted and exploited by the TTP of a Threat Actor
  - Examples
    - A particular DB configuration leads to a vulnerability in the product



Bank Executives

Indicator-9742

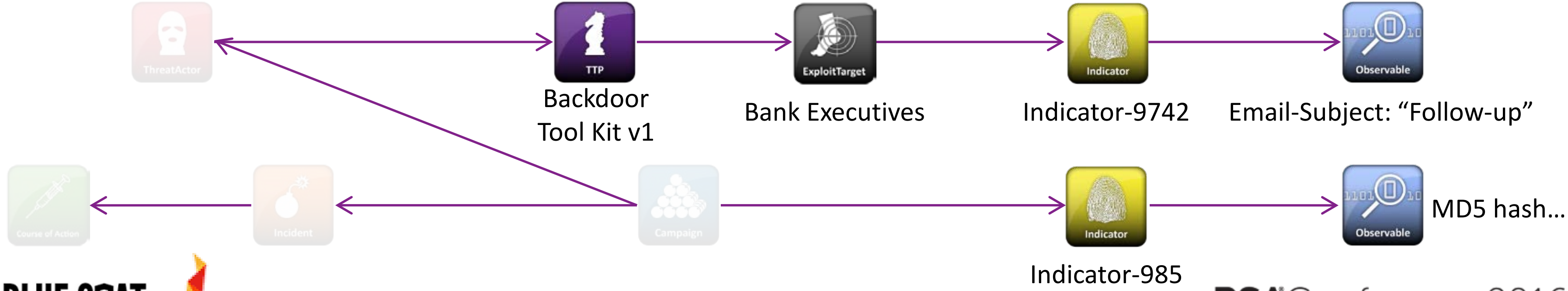
Email-Subject: “Follow-up”

MD5 hash…

Indicator-985

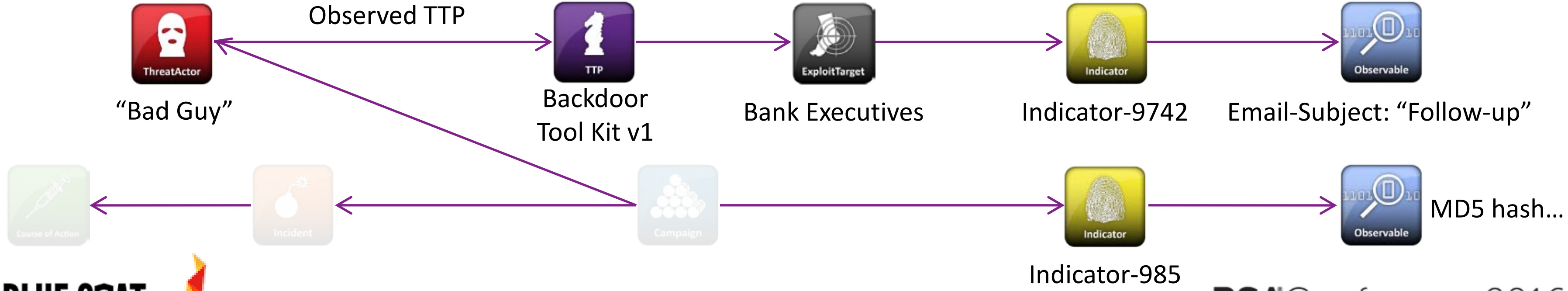
Anatomy of threat intelligence – cont.

- TTPs (Tactics, Techniques, and Procedures)
  - The behaviors or modus operandi of cyber adversaries (e.g. what they use, how they do it, and who do they target)
  - Examples
    - These particular IP address are used for their C2 infrastructure



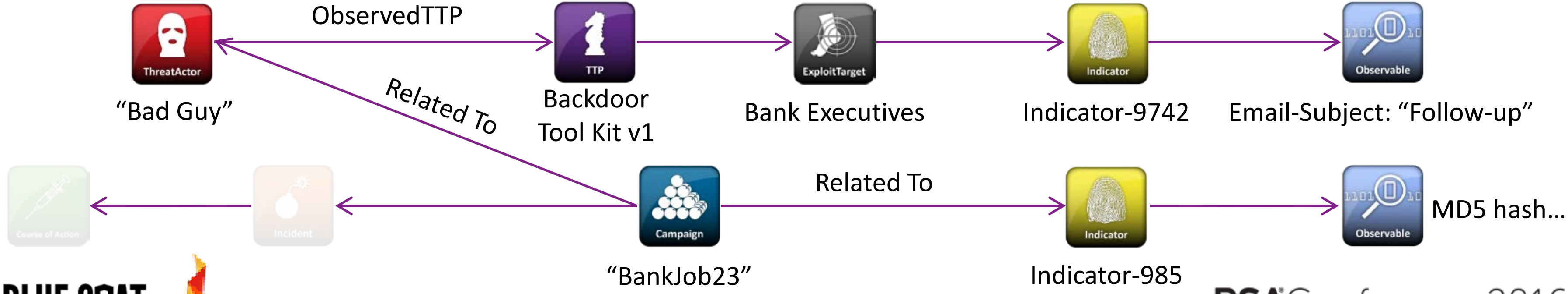
Anatomy of threat intelligence – cont.

- Threat Actors
  - Identifies the characterizations of malicious actors (or adversaries) representing a threat, based on previously observed behavior
  - Examples
    - Threat Actor is also known as Comment Crew and Shady Rat



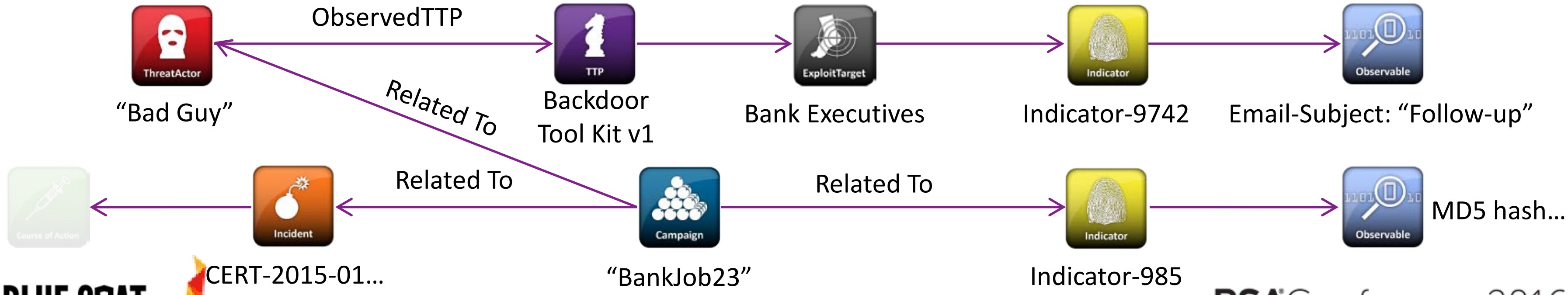
Anatomy of threat intelligence – cont.

- Campaigns
  - Is the perceived instances of the Threat Actors pursuing specific targets
  - Examples
    - Particular Threat Actors with ties to organized crime targeting banks



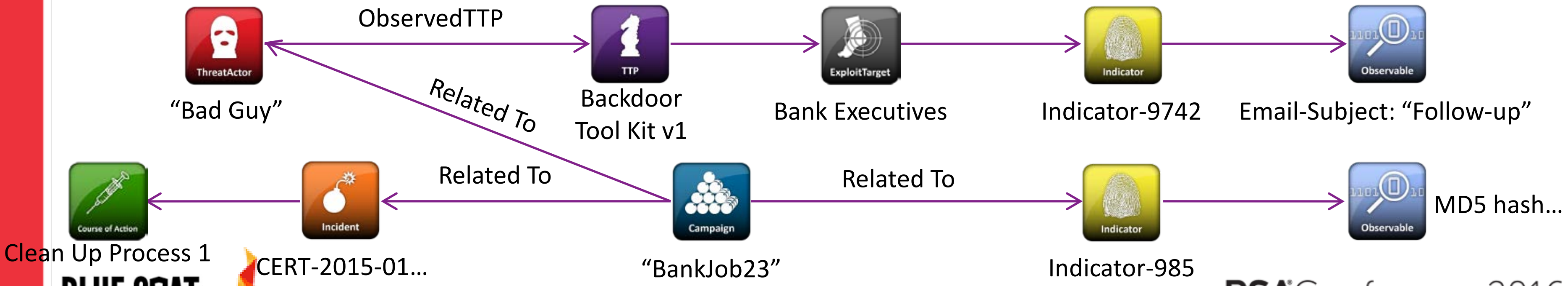
Anatomy of threat intelligence – cont.

- Incidents
  - These are the specific security events affecting an organization along with information discovered during the incident response
  - Examples
    - A John's laptop was found on 2/10/16 to be infected with Zeus.



Anatomy of threat intelligence – cont.

- Course of Actions
  - Enumerate actions to address or mitigate the impact of an Incident
  - Examples
    - Block outgoing network traffic to 218.77.79.34
    - Remove malicious files, registry keys, and reboot the system



Do Indicators contains PII?

- People typically think NO (hashes, IPs, URLs, Registry Keys, etc)
- BUT…
  - Exfiltrated data can contain PII
  - Attack data can contain PII
  - Log data can contain PII
- … It can, so be careful !!

STIX 2.0 Indicator – Example

```json
{
  "type": "indicator",
  "id": "indicator--089a6ecb-cc15-43cc-9494-767639779123",
  "spec_version": "2.0",
  "created_at": "2016-02-19T09:11:01Z",
  "description": "file used by malware x",
  "indicator_types": [ "malware" ],
  "observables": [
  {
    "type": "file-object",
    "hashes": [ {
      "type": "md5",
      "hash_value": "3773a88f65a5e780c8dff9cdc3a056f3"
    } ],
    "size": 25537
  }
}
```

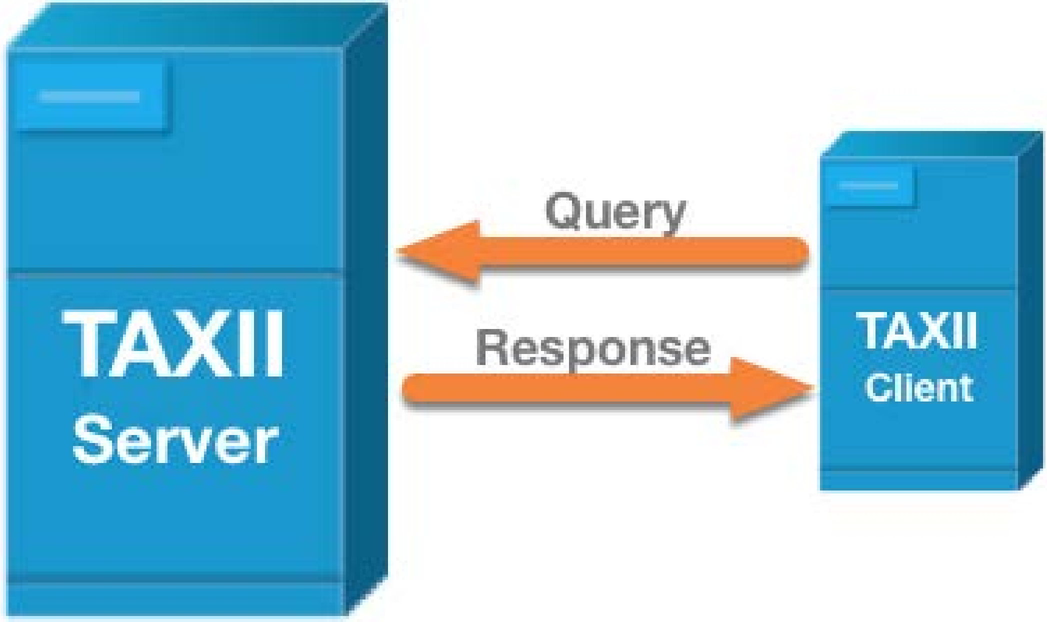
TAXII

- TAXII is an open protocol for the communication of cyber threat information. Focusing on simplicity and scalability, TAXII enables authenticated and secure communication of cyber threat information across products and organizations.
- TAXII 2.0 is a REST based JSON solution over HTTPS
  - This should make things easier for developers to implement and vendors to incorporate

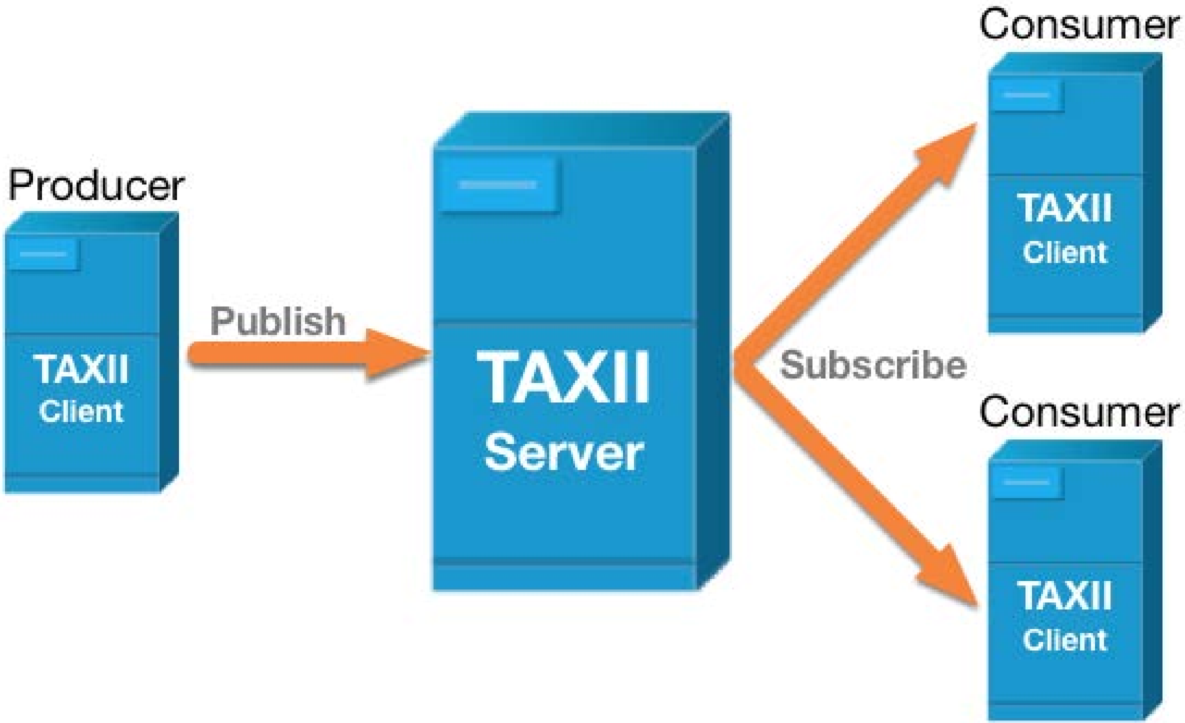
What will TAXII do for us?

- Enables the good citizen philosophy of “see something, say something”
- Enables plug and play interoperability
- Enables two fundamental ways of communicating threat intelligence
  - Lets look at these…

Collections via Request / Response



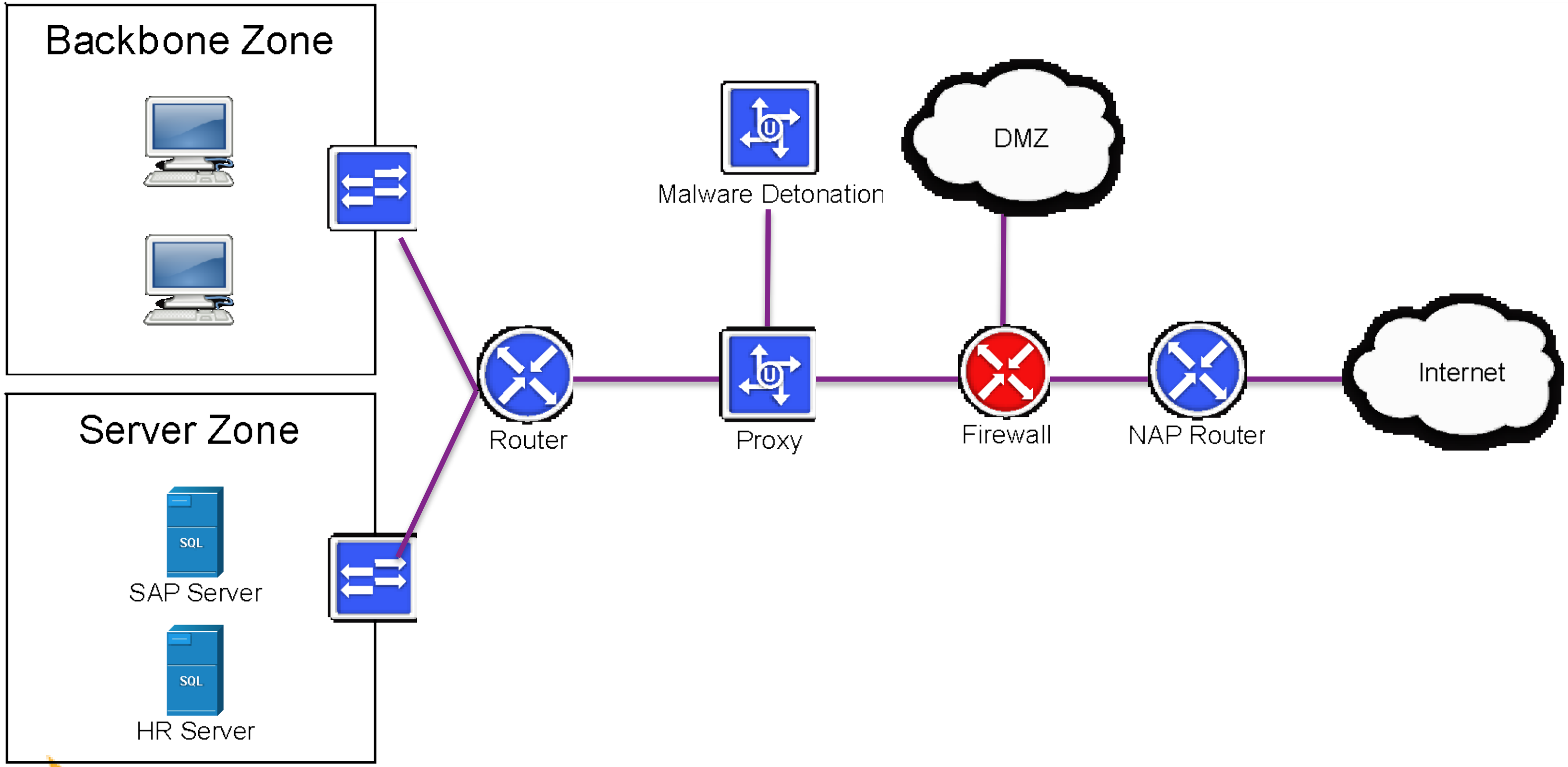
Channels via a Publish / Subscribe



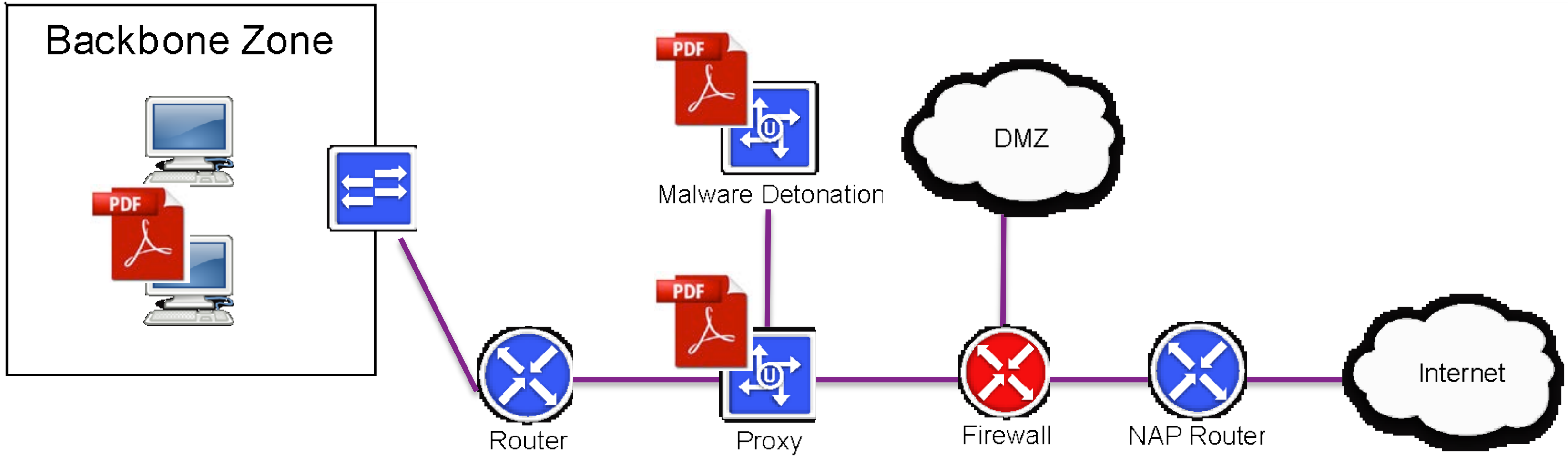
TAXII scenario

- The following workflow / scenario encompasses 4 common use cases for TAXII based channels
  - Internal to internal device communication
  - Analyst to analyst communication inside of the network
  - Organization to organization CTI / indicator publishing
  - Analyst to external analyst work group (circle of interest/trust) sharing

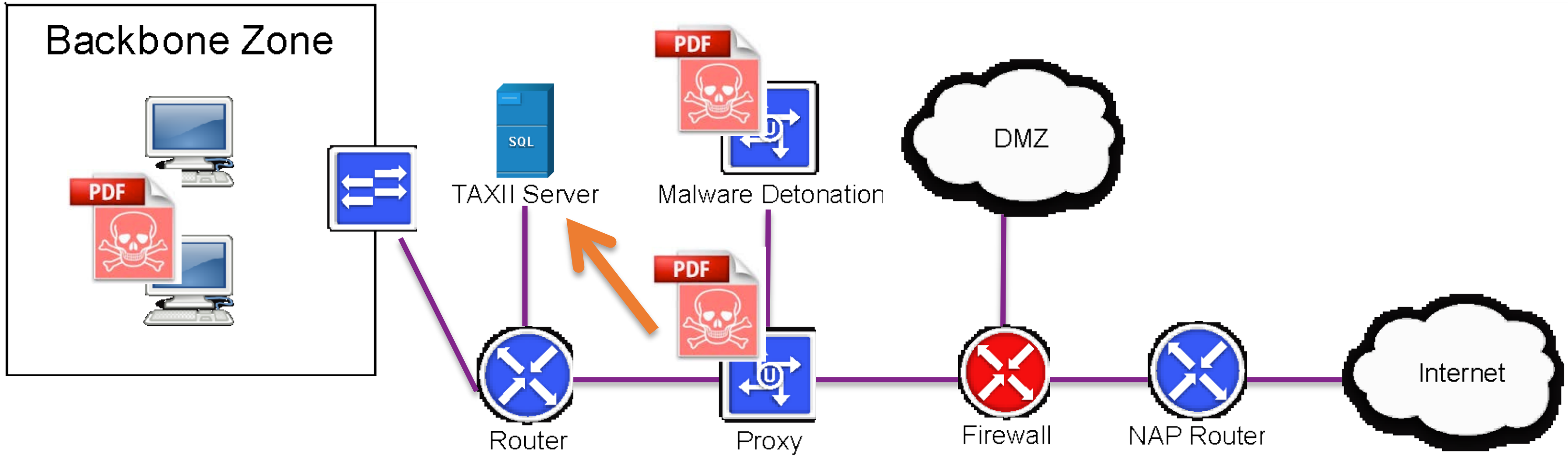
TAXII scenario – Setup



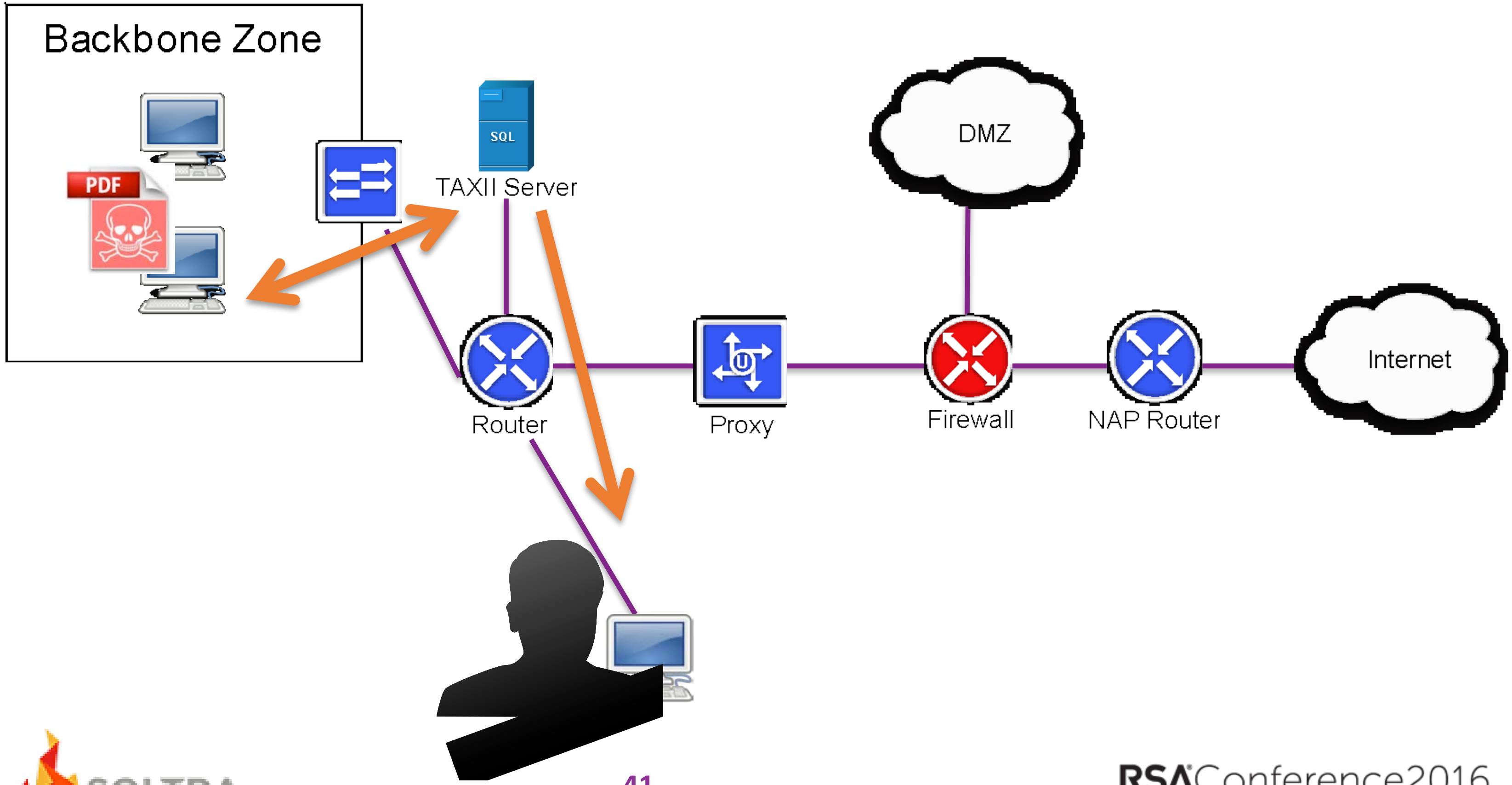
TAXII scenario – Step 1



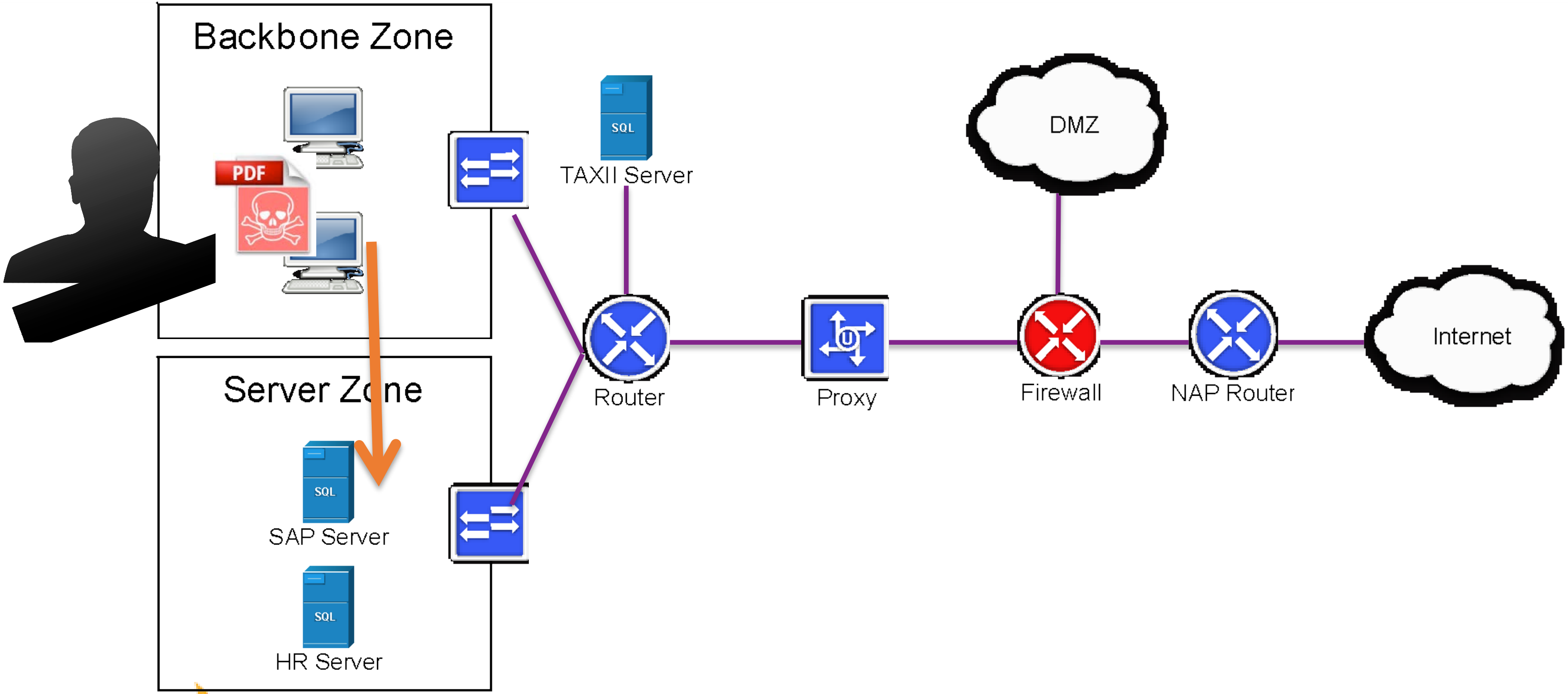
TAXII scenario – Step 2



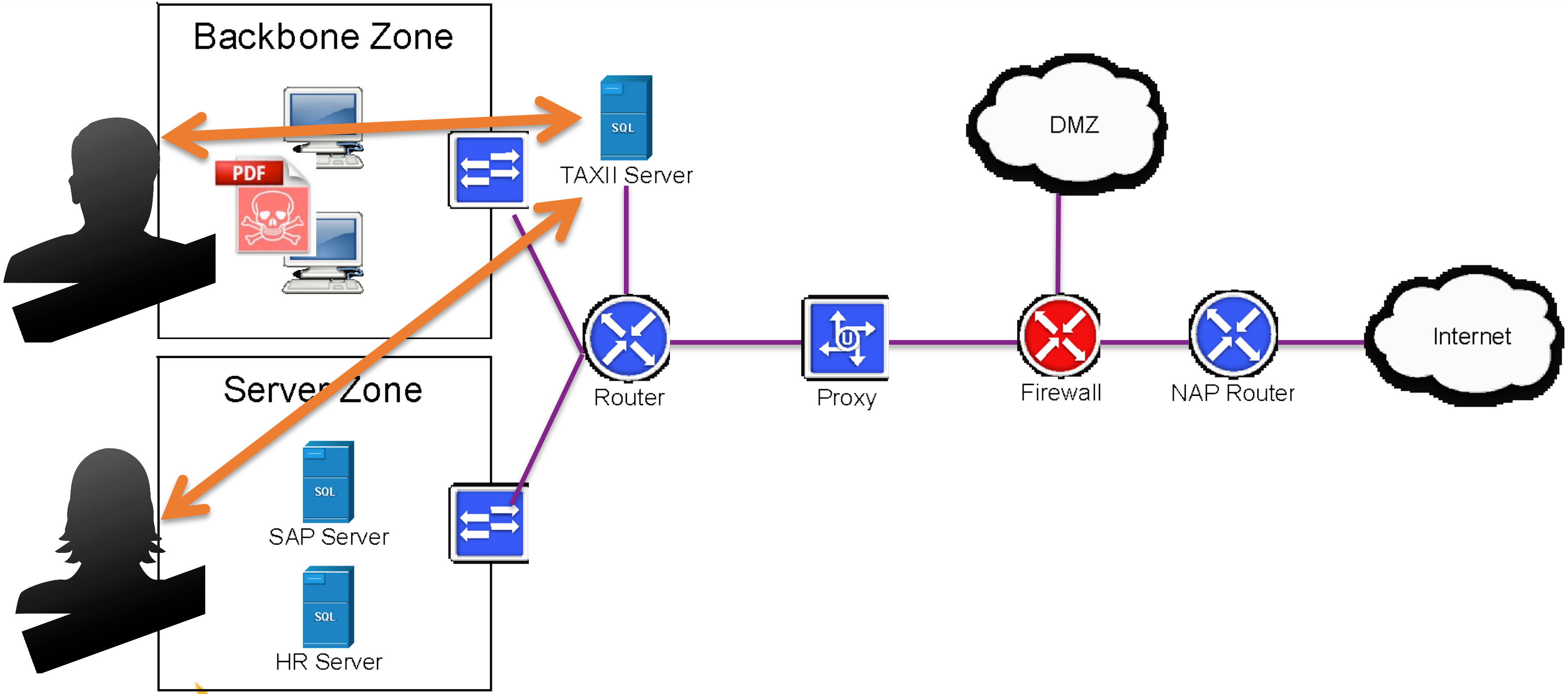
TAXII scenario – Step 3



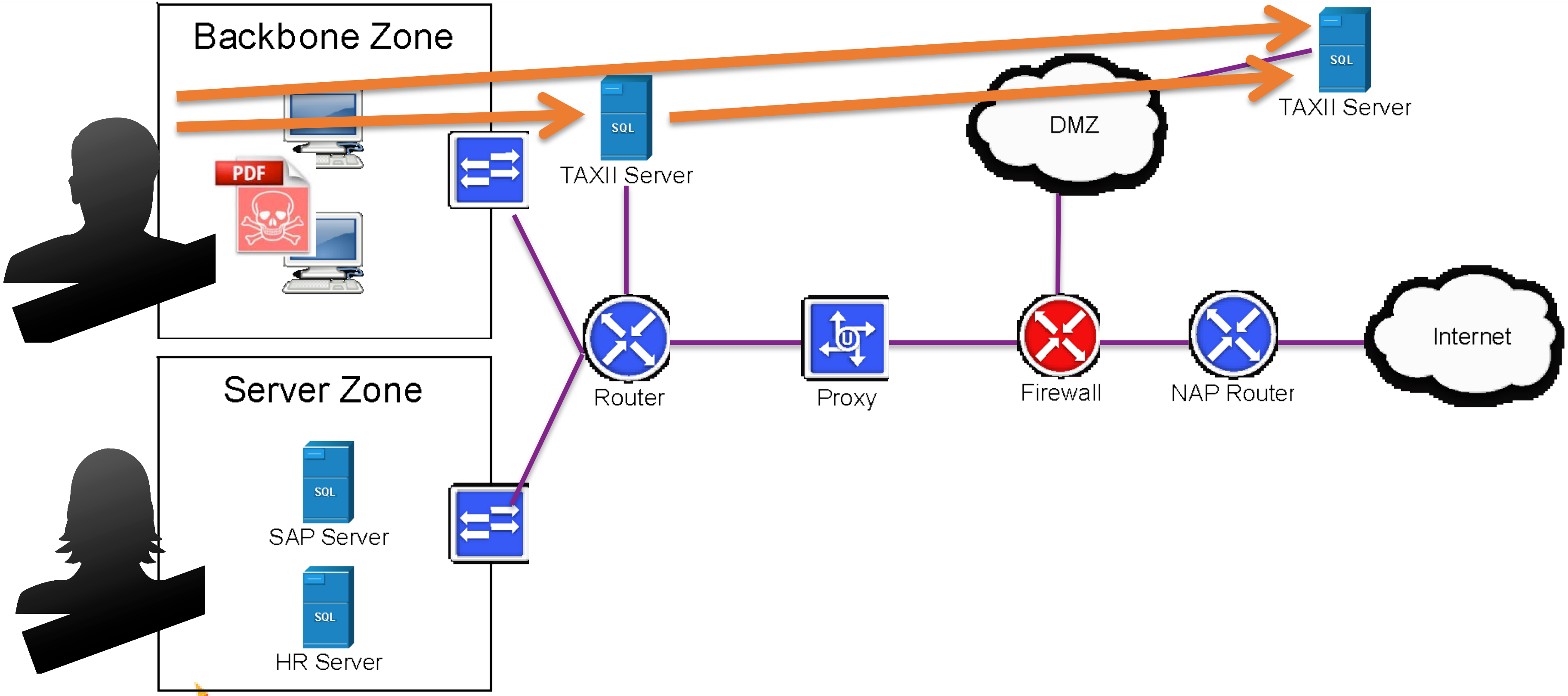
TAXII scenario – Step 4



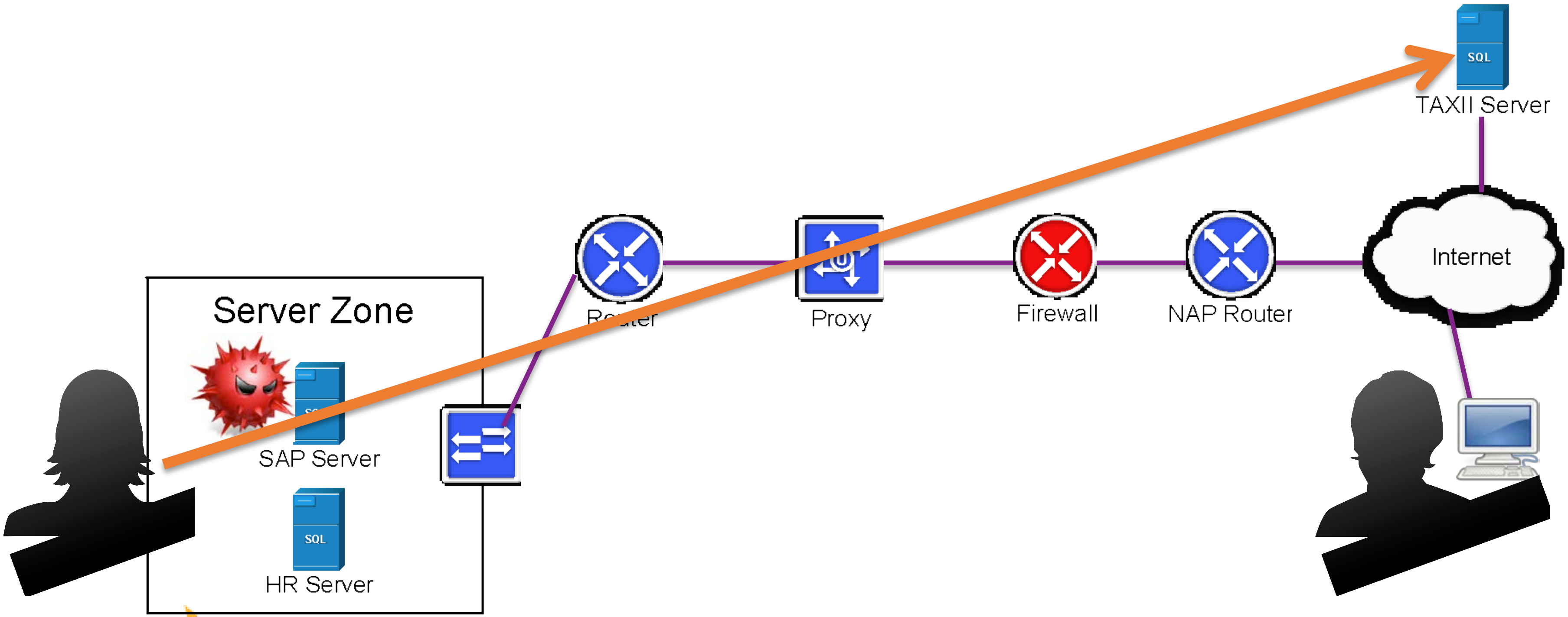
TAXII scenario – Step 5



TAXII scenario – Step 6



TAXII scenario – Step 7



Conclusions

- If we missed a key interaction, please come see us after this talk
- This scenario illustrates 4 interesting ways TAXII 2.0 channels could be used by an organization to improve their cyber defenses
- TAXII will enable organizations to communicate threat intelligence in automated ways by using both traditional request / response and channel based publish / subscribe
- STIX offers a rich ontology for descripting and documenting cyber intelligence

Roadblocks and Challenges to Threat Sharing

Roadblocks to success

- Divergent processes
- Your legal team
- Privacy concerns
- Inadequate technology
- Information handling issues

- Threat sharing solution space NOT YET SOLVED!

Divergent processes

- Nascent sharing ecosystems
  - Everyone is talking about it, but few are doing it
  - Hard to get started due to different maturity levels
  - Lack of robust products and solutions
  - Trusting, vetting and deploying CTI
- People think about sharing the wrong way
  - It is not symmetric (e.g., Indicator for Indicator)
  - It is more than just lists of IPs, URLs, and file hashes

Your legal team

- Your general council will try to say NO!
  - Blind to the benefits of using or sharing CTI
  - Competition at the C-Level vs cooperation at the cyber level
- What protections are in place
  - IPR / PII / Reputation concerns
  - Liability (this is where CISA could help)
  - Withholding disclosure until research is done

Privacy concerns

- What privacy information is included in the data
  - Who has access to the raw data
  - What will this mean for safe harbor
  - What happens if you send it by accident?
- How can you stay in compliance and anonymize the data
- Who will be responsible for scrubbing the data?
  - Can you trust that?

Inadequate technology

- Lack of interoperable commercial solutions
- “Last mile” integration with network devices still forthcoming
- Maturing standards, so many to choose from
- Data Quality
  - Not all CTI is created equal
  - In fact, not all CTI will be valid for your organization

Information handling issues

- Over sharing creates noise especially with duplicated data while under-sharing reduces effectiveness
- Struggle with protecting the innocent and getting enough information to catch the bad guys
- Complex sharing policies might not be honored
- What happens if the bad guys get access to the data or worse, poison the data

Successful sharing groups have had

- High levels of maturity
- Similar processes and procedures
- Shared context within their eco-system
- Legal teams that understand the benefits and risk of CTI
- Pre-defined PII policies
- Understand how to use technology to meet their needs

Conclusions

Conclusions

- Threat sharing is moving to a better place
- CISA
  - Will probably not impact your day job
  - Might improve CTI sharing by removing some legal obstacles
  - Will help STIX and TAXII as DHS implements CISA using STIX/TAXII
  - Like all things has the potential of being misused

Apply what you learned today

- Next week you should
  - Visit the stixproject.github.io and get involved
  - Get ahead of the curve: Establish positive and educational relationships with legal and the C-suite and do this BEFORE you need something form them
  - Learn the basics of STIX: Observables, Indicators, and TTPs
  - Identify key stakeholders in your organization that can help you build a CTI sharing program

Apply what you learned today – cont.

- In the first three months following this presentation you should
  - Identify LOCAL companies to cooperate with
    - Meeting in person == good!
  - Work with Legal/C-suite to gain approval to cooperate and share CTI
  - Identify how STIX/TAXII can help you get better at info sharing
  - Identify integration gaps and start hammering on your vendors
    - Don’t underestimate the value of “when we make our next purchasing decision for $category; we are really looking for $feature”

Apply what you learned today – cont.

- Within six months you should
  - Integrate threat intelligence in to your security playbook
  - Require STIX and TAXII compliance on all RFIs and RFPs
  - Be meeting regularly with peers from local companies
    - Deploy a CTI sharing strategy within that ecosystem
  - Think outside the box! “trade indicators for sightings”

RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-F01

STIX, TAXII, CISA: The impact of the US Cybersecurity Information Sharing Act of 2015

Bret Jordan CISSP

Director of Security Architecture
Blue Coat Systems

Mark Davidson

Director of Software Development
Soltra

#RSAC