

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: CXO-R03

## The Third Rail: New Stakeholders Tackle Security Threats and Solutions

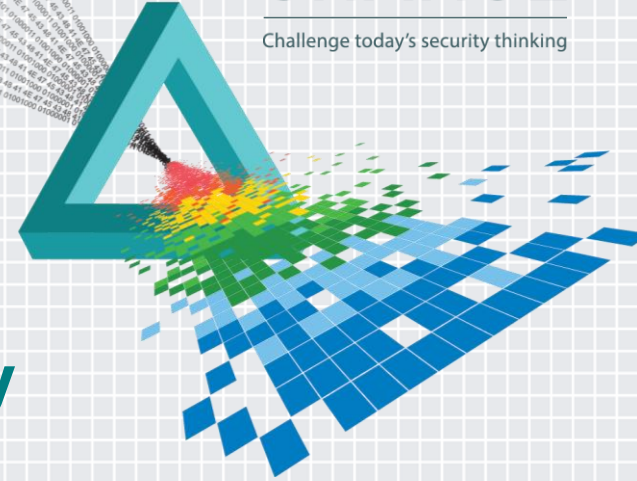
**Ted Ross**

---

Director, Threat Intelligence  
HP Security Research  
@tedross

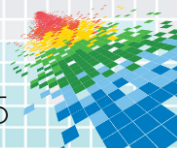
# CHANGE

Challenge today's security thinking



# Agenda

- ◆ My brief background
- ◆ An example of a successful collaboration
- ◆ Quick review of some basics
- ◆ Stakeholders
- ◆ “Next Gen” sharing
- ◆ Use cases



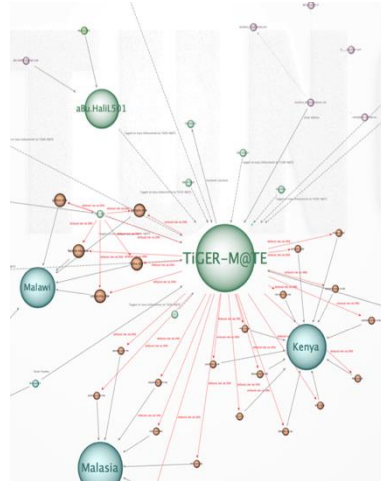
# HPSR Threat Intelligence

**Strategic**  
Human-to-human  
**Field Intelligence**

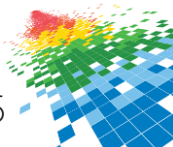
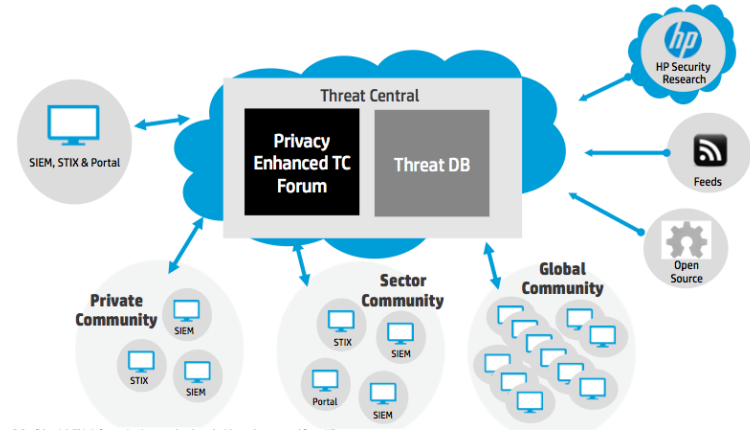
Monitor the Underground

Profile Threat Actors

Human Intel



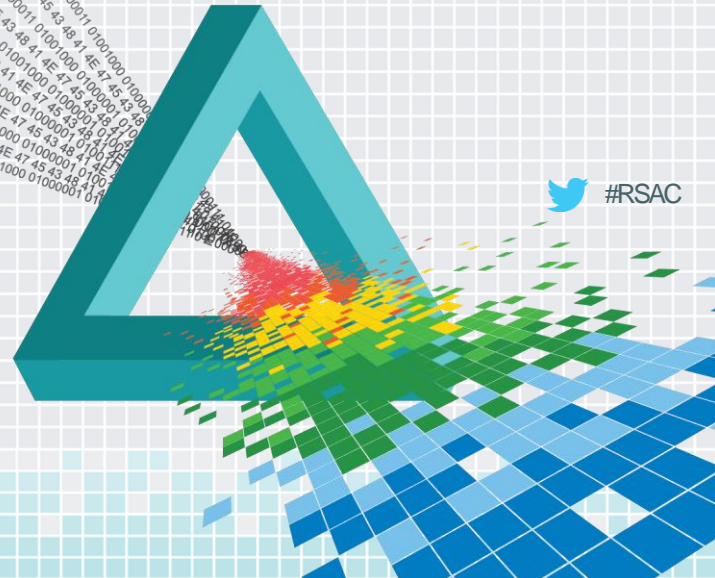
**Tactical**  
Machine-to-machine  
Facilitates **strategic** human-to-human interaction  
**Threat Central**



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## The Power of Collaboration: *A View from the Underground*



# The Adversary Collaborates Effectively

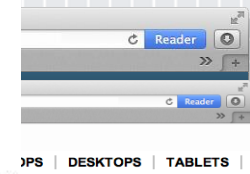
\$45-million in 10-hours: Cyber crime ring raids ATMs in 27 countries in one of the biggest ever bank heists



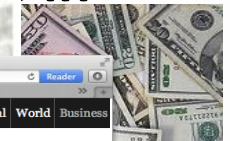
JESSICA DYE, JOSEPH AX AND JIM FINKLE, REUTERS | 09/05/13 | Last Updated: 10/05/13 2:02 PM ET  
[More from Reuters](#)



Expert  
How C  
Stole \$



ack  
s in



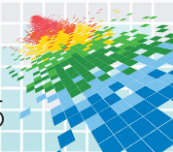
## The New York Times

In Hours, Thieves Took \$45 Million in A.T.M. Scheme



## BUSINESS

The Circuit: Hackers took \$45 million in ATM heist





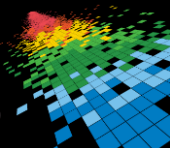
# Recruiting

[New thread]

Page 1 of 86 1 2 3 11 51 > Last

Threads In Forum: Search and Job Offer Forum Tools Search this Forum

Thread / Thread Starter	Rating	Last Post	Replies	Views
Sticky: Market Place for Offer/Request a Job (p 1 2 3 ... Last Page)		5:37 PM	207	11,014
BULGARAIN needed asap		Today 06:56 AM	2	75
looking for partner for new projects! serious work!		Yesterday 11:55 PM	0	33
Need USA cashiers ASAP!!! (p 1 2 3)		Yesterday 06:36 AM	26	1,188
Searching German Bank Logins I		7:07 PM	1	42
Westernunion drop needed in usa		11:08 PM	2	123
uk bank drop needed		4:27 PM	7	164
Can you cashout cc (any country but your specific bin)? (p 1 2 3 ... Last Page)		3:17 PM	274	8,024
Looking for : Logins urgent		5:53 AM	0	15
Need In-store workers! (p 1 2 3 ... Last Page)		2:39 AM	37	1,394
I have 8 Drop, we can do everything with their names		6:26 PM	1	70



# But... they don't trust each other

[Reply] Page 1 of 313 1 2 3 11 51 101 > Last »

View First Unread Thread Tools Search this Thread Rating: [Progress Bar]

Senior Member

Posts: 511

Reputation: 127 +/-



- We are not responsible for cards balanse
- Invalid cards replace time - 60 min for US, 20 min for EU.
- We can deny an access to our service with no any explanation
- WE do NOT provide any Moneyback, only replace.
- Once You buy cards at our shop, You automatically agree with all the rules and terms.
- We are NOT responsible for AVS mismatch

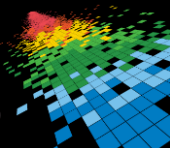
Contact us:

[Reply]



























# Collaboration

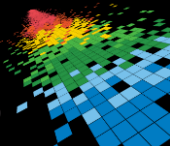
<p>Senior Member</p>  <p>Posts: 324</p> <p>Reputation: 81 +/-</p>	<p>I have orders that are processed.</p> <p>I hear that Instore pickup is hott and should not try it.</p> <p>What do you guys think? Are the feds all over this?</p> <p>[Reply]</p>
<p>Member</p>  <p>Posts: 69</p> <p>Reputation: 0 +/-</p>	<p>Nah, they still work... I've been picking up 5+ orders daily all around the USA.</p> <p>Contact me if you need people to pick-up for you...I can resell your products and send your cut the same/next day.</p> <p>Thanks for your time.</p> <p>[Reply]</p>





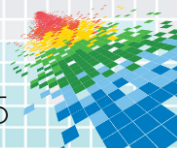
# Payment Options – Escrow, Laundering, Assets

		my perfect money account is blocked (B 1 2 3)		13 11:29 PM	21	606
		exchanger from PM to WU		13 03:06 PM	7	132
		Where to buy verified WebMoney Accs?		13 07:58 PM	0	18
		bitcoin issue (B 1 2)		13 07:00 PM	11	365
		Selling PerfectMoney 2000 or half and 30 btc, need wmz Rate 1 PM/btc: wmz. One Time deal		13 12:54 PM	0	70
		Does PM allow multiple accounts with same IP and Mac address?		13 01:52 AM	2	41
		ALTERNATIVE PAYMENT METHODS?! BESIDE LR/PM/WMZ? (B 1 2 3 ... La		13 12:30 AM	62	1,663
		Perfect Money Payment problem(Money sent but not recieved)		13 08:03 AM	7	231
		<b>TAX REFUND TUT. (B 1 2)</b>		13 08:59 AM	12	476
		SWEDEN UKASH TO PM		13 11:23 PM	1	48
		Need Who Can Pickup MoneyGram Anyname		13 12:02 AM	0	66
		Who Can Load Western Union Pre-paid Card...		13 12:00 AM	1	84



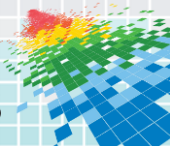
# Lessons Learned from the Adversary

- ◆ **Sharing is social - social rules apply**
- ◆ **Protect your identity**
- ◆ **Credibility is key**
- ◆ **Reuse what others have learned**
- ◆ **Leverage each others strengths**



# Challenges that We Must Overcome

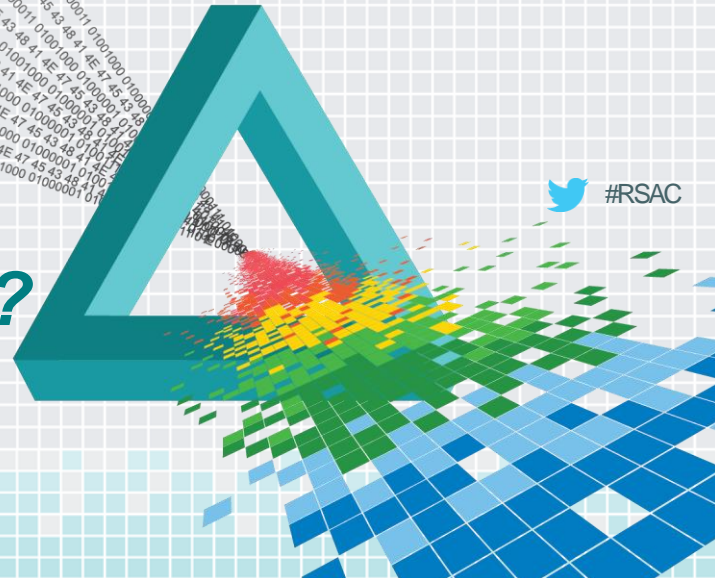
- **Limited participation**
  - Not comfortable sharing (social issues)
  - No time
  - No trust
- **Data is not actionable – lacks context and relevance**
- **Overly manual – not timely**



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

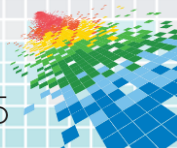
## The Power Of Collaboration: *What are the Good Guys doing?*





# ISACs (*Information Sharing & Analysis Centers*)

- Created from Presidential Directive in 1998 (updated in 2003).
  - Public and private sector to **create a partnership to share information** about threats, vulnerabilities, and events to **help protect the critical infrastructure**.
- U.S. Treasury, DHS and other relevant **government agencies / entities use ISACs to disseminate critical information**.
- Last count there are **18 different ISACs** (i.e. Financial Services, Energy, Water, National Health, Surface Transportation, etc).
- **FS-ISAC** (launched in 1999) is the most advanced and leading the way for others
  - In early 2013, FS-ISAC extended their charter to include information sharing for financial services entities **world-wide**.





## STIX / TAXII

 The logo for STIX (Structured Threat Information eXpression) features the word "STIX" in a bold, black, sans-serif font. The letter "X" is uniquely styled with a red diagonal slash through it. A small "TM" trademark symbol is positioned to the upper right of the "X".

**Structured Threat Information eXpression**

*A Structured Language for Cyber Threat Intelligence Information*

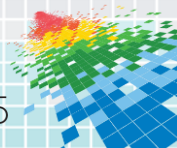
**Source - <https://stix.mitre.org>**

 The logo for TAXII (Trusted Automated eXchange of Indicator Information) features the word "TAXII" in a bold, yellow, sans-serif font. The letter "X" is uniquely styled with a black diagonal slash through it. A small "TM" trademark symbol is positioned to the upper right of the "I". Below the text is a horizontal bar with a black and yellow checkerboard pattern.

**Trusted Automated eXchange of Indicator Information**

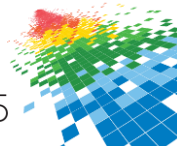
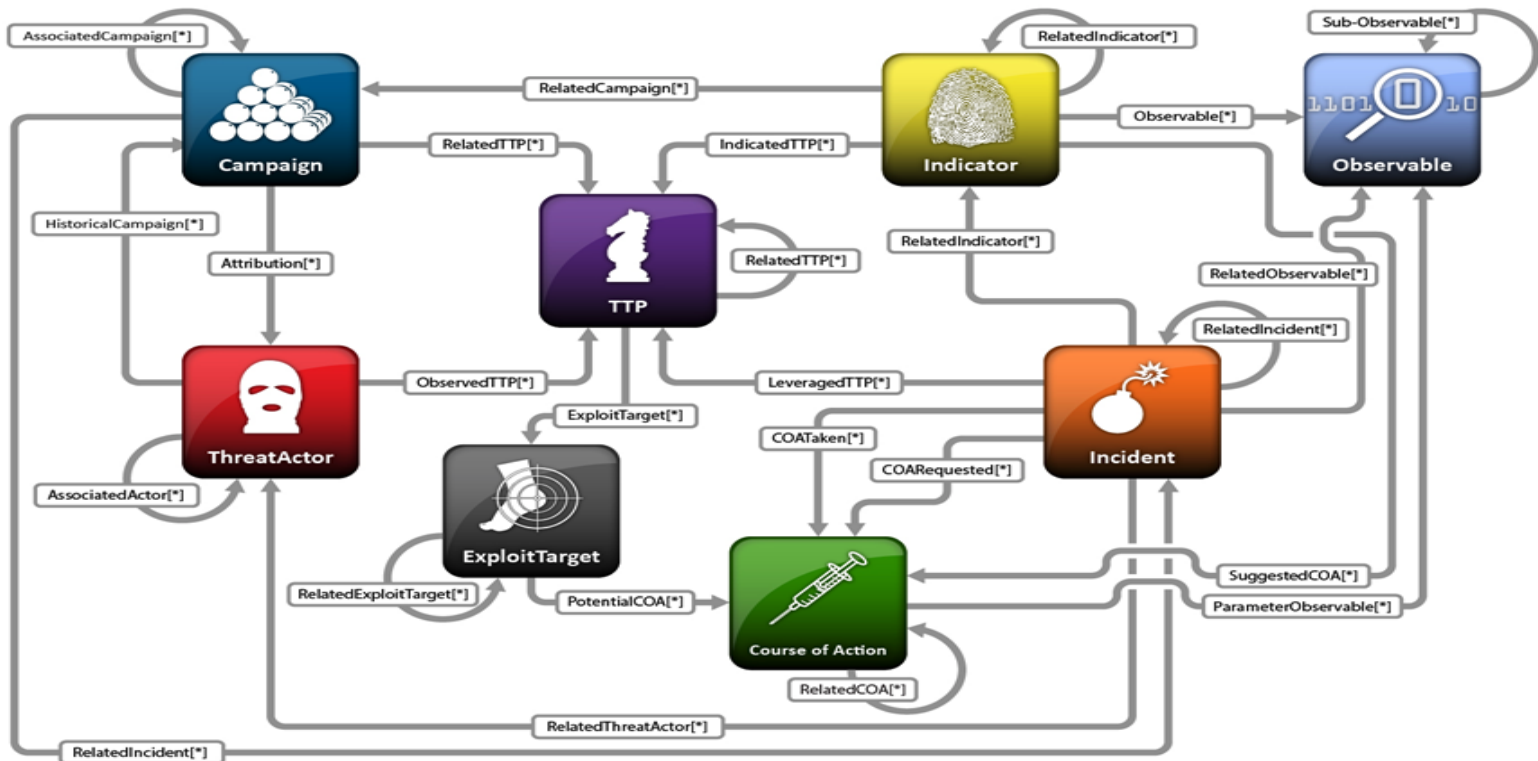
*Enabling Cyber Threat Information Exchange*

**Source - <http://taxii.mitre.org>**

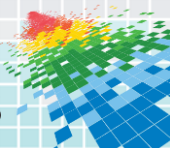
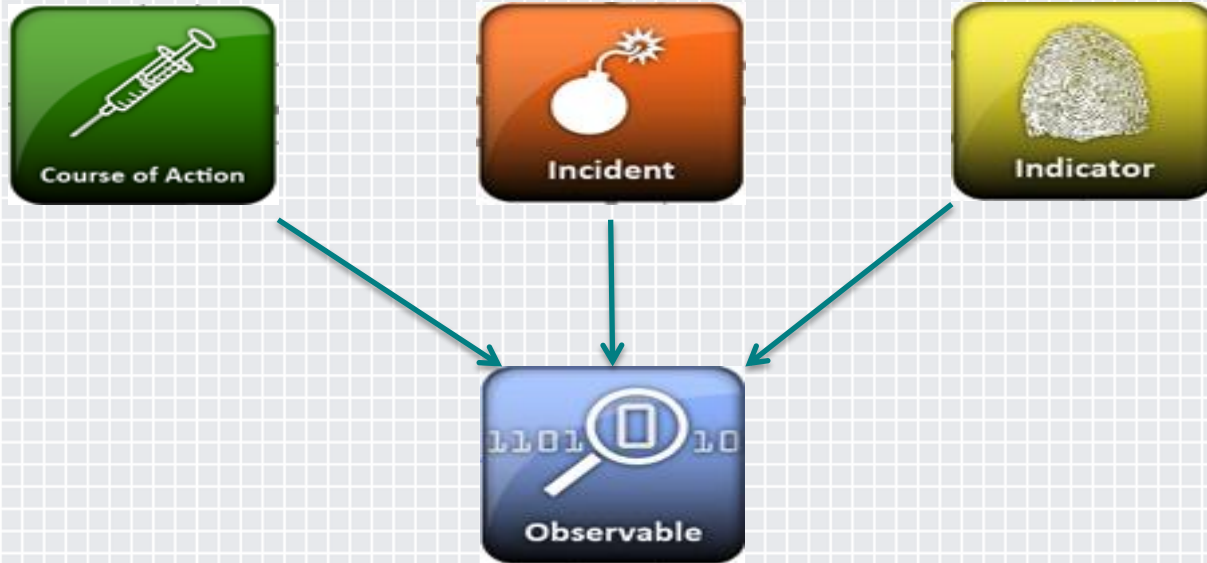


# STIX Data Model

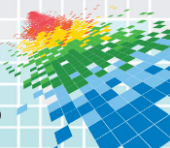
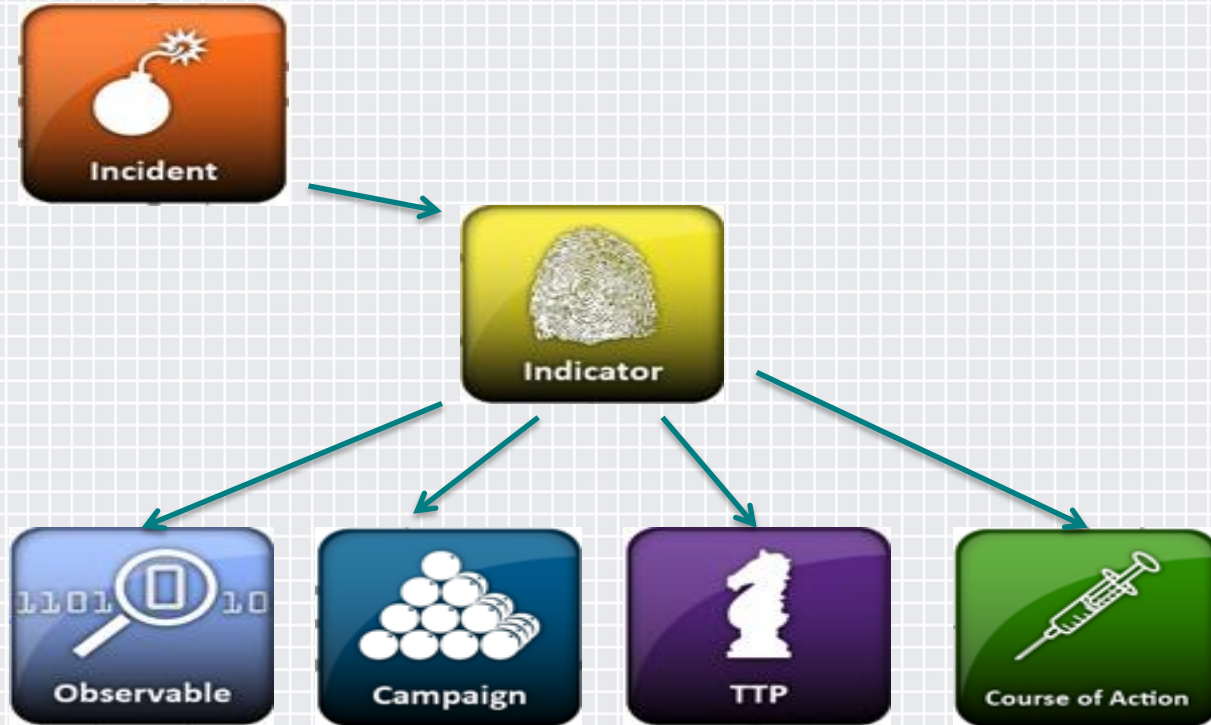
<https://stix.mitre.org>



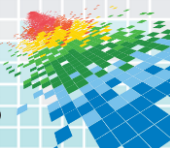
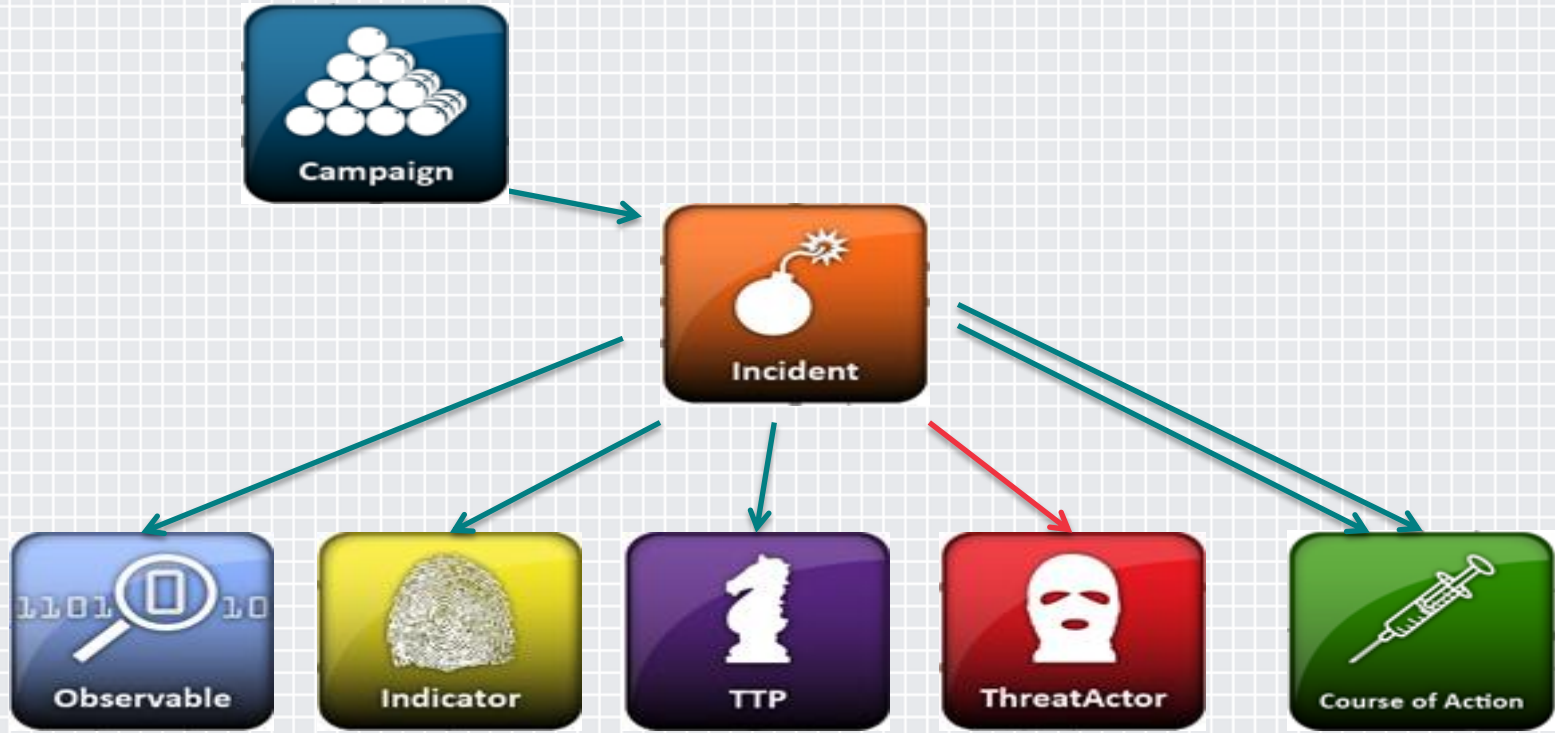
# Observable (lowest level)



# Indicator



# Incident

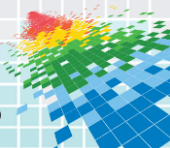




# Evolution

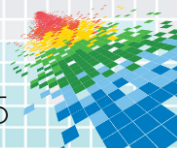
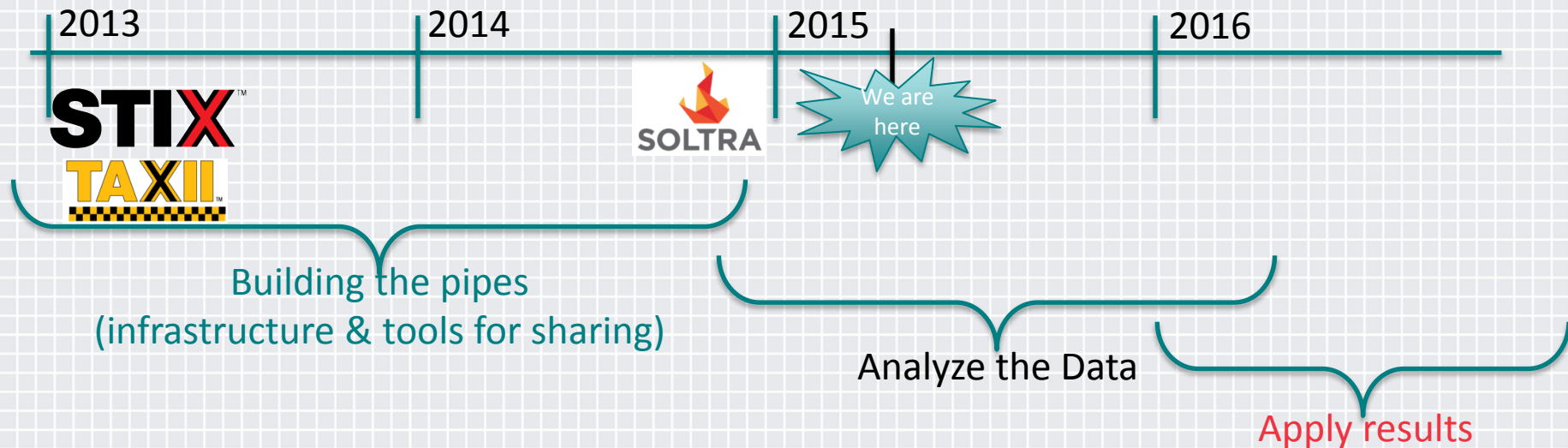
## *2015 Embedded Human Threats*

Video Removed for security purposes



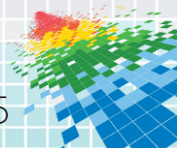
# Evolution

*Props to Chris Blask (ICS-ISAC)*

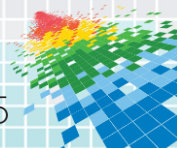
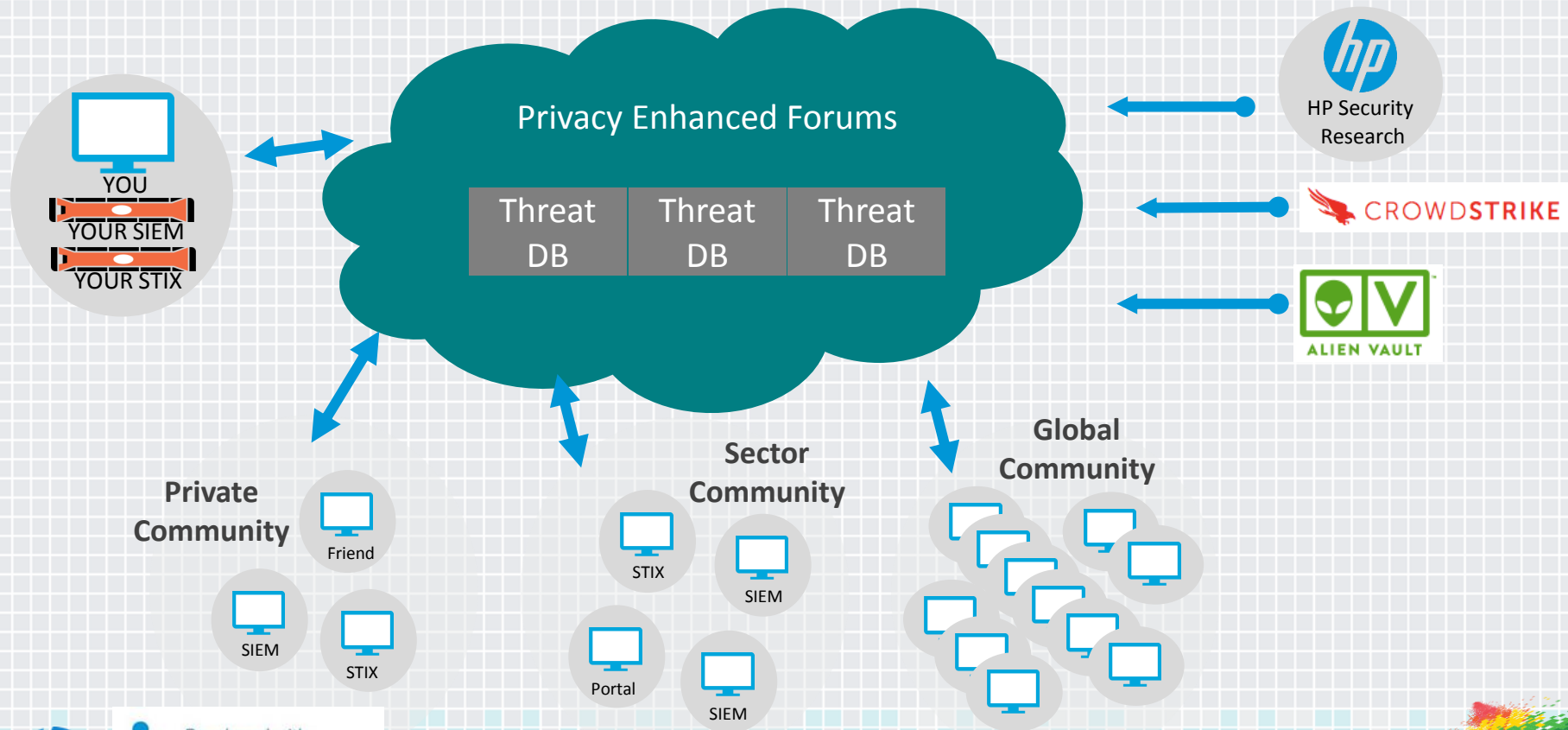


# The Next Phase- Analyze the Data

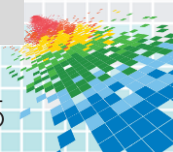
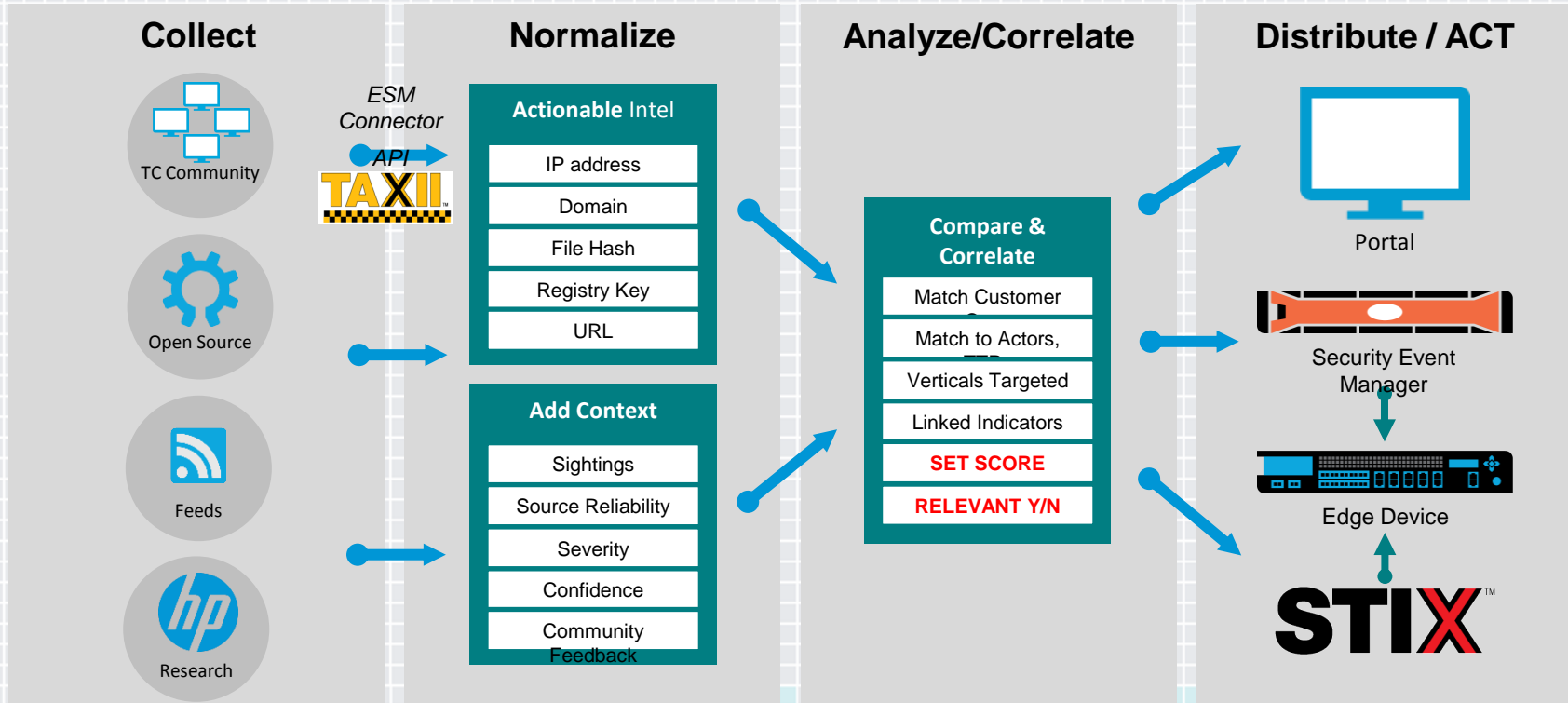
- ◆ Indicators come from multiple sources, each with a unique view on the threat
- ◆ Collaboration allows us to **LINK artifacts**
- ◆ **Interacting** with an intelligent system allows us to determine which threats are important to you – **RELEVANCE**
- ◆ Using the context to score the indicators makes them **ACTIONABLE**



# Key Stakeholders



# Automated Action Influenced by Context



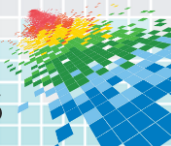


# Results & Actions

	First Sighting	Second Sighting	Vote Down Effect	Third Sighting	Fourth Sighting	Highest Possible
Reliability	Normal	Normal	Normal	Normal	Normal	HIGH
Severity	M	M	M	M	M	H
Confidence	M	M	M	M	M	H
Sightings	1	2	4	3	4	4
Votes	0	0	-4	0	0	4
SCORE	35	47	52	59	73	100

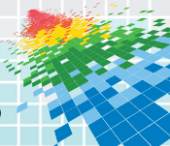
Monitor Activity

Take Action



# Results & Actions

	First Sighting	Second Sighting	Vote Down Effect	Third Sighting	Fourth Sighting	Highest Possible
Reliability	Normal	Normal	Normal	Normal	Normal	HIGH
Severity	M	M	M	M	M	H
Confidence	M	M	M	M	M	H
Sightings	1	2	4	3	4	4
Votes	0	0	-4	0	0	4
SCORE	35	47	52	59	73	100

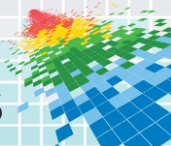


# Results & Actions

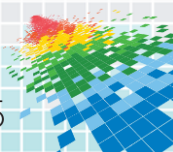
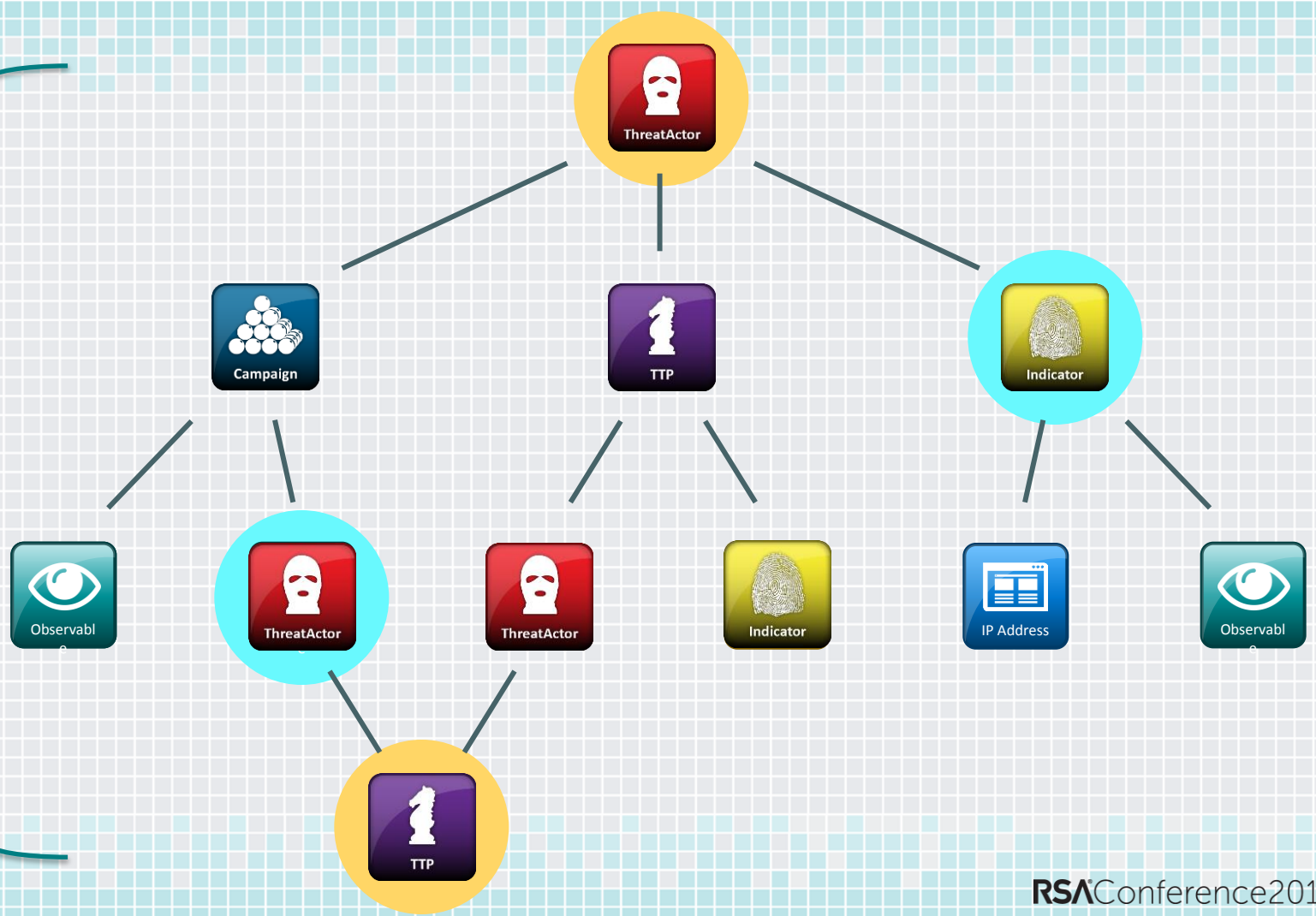
	First Sighting	Second Sighting	Vote Down Effect	Third Sighting	Fourth Sighting	Highest Possible
Reliability	Normal	Normal	Normal	Normal	Normal	HIGH
Severity	M	M	M	M	M	H
Confidence	M	M	M	M	M	H
Sightings	1	2	4	3	4	4
Votes	0	0	-4	0	0	4
SCORE	35	47	52	59	73	100

Monitor Activity

Take Action



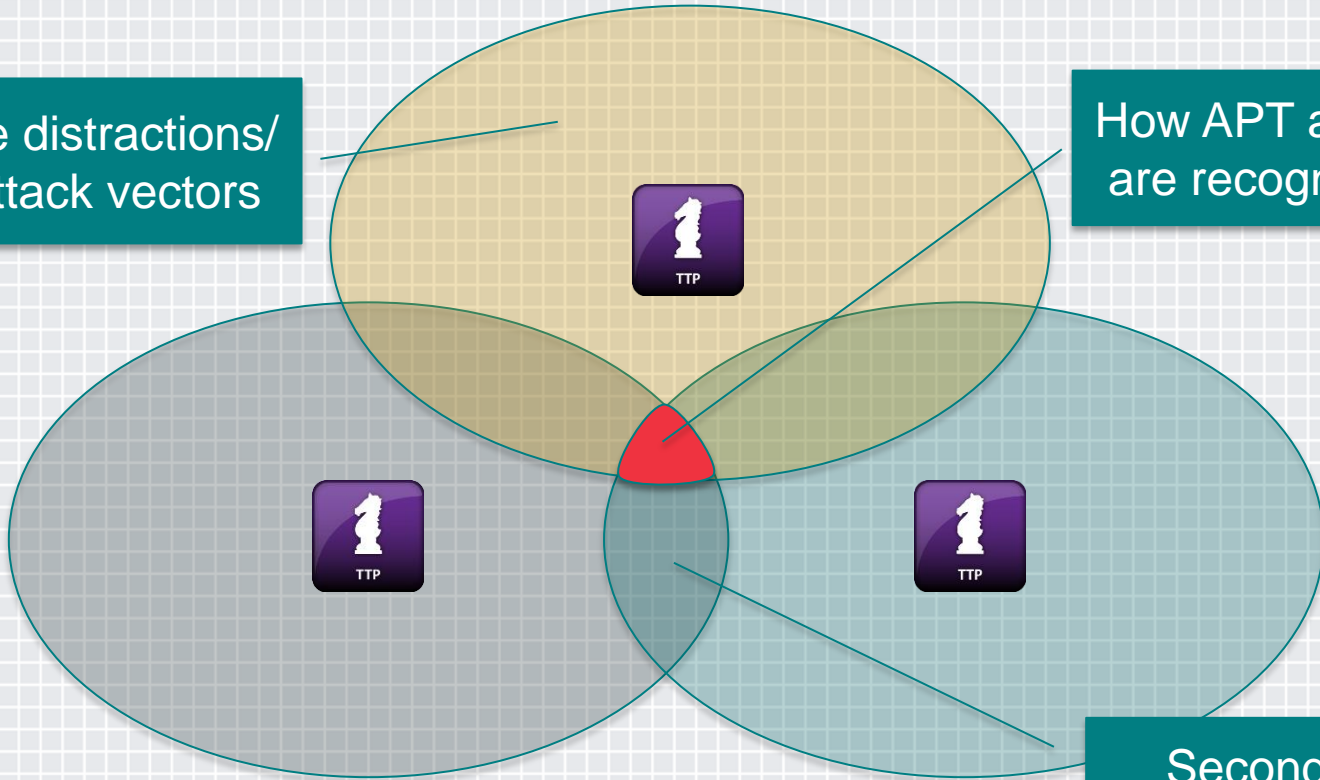
Query Depth = 3



# Automated APT Actor Recognition

Possible distractions/  
Easy attack vectors

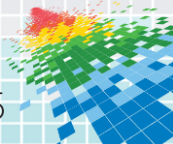
How APT actors  
are recognized



Secondary  
recognition



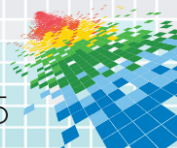
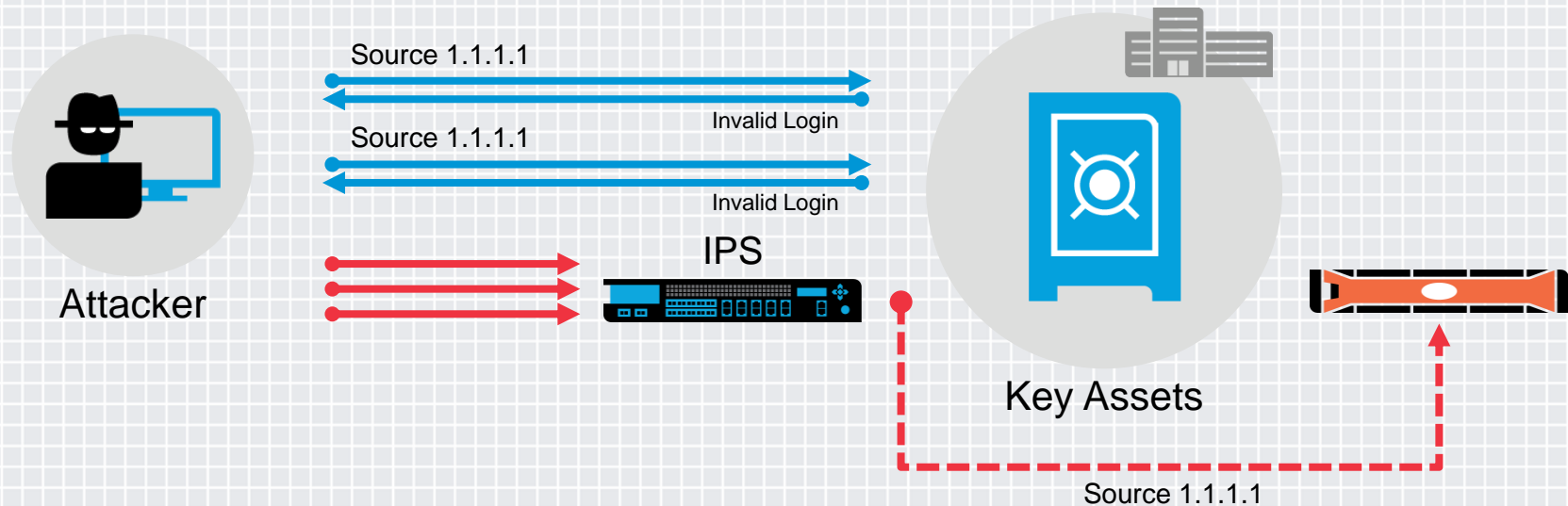
The power of linking Actors (courtesy of CERT-EU)





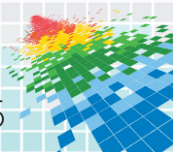
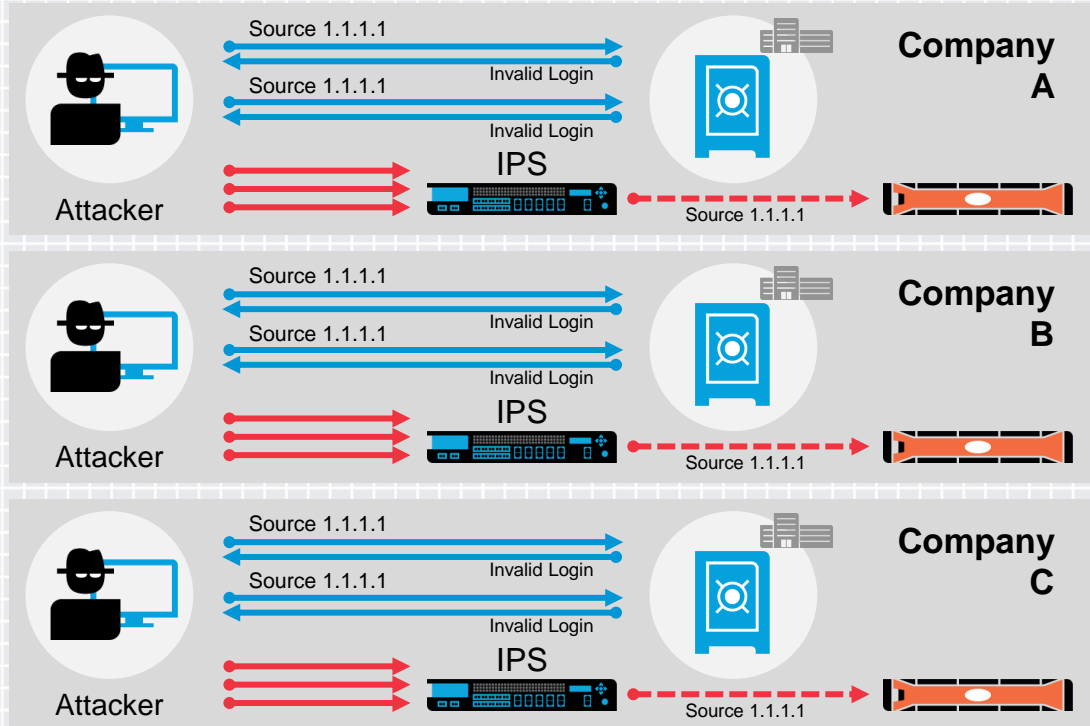
# Use Case: Automated Actions

## Brute force login



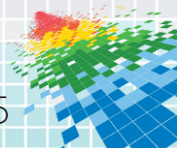
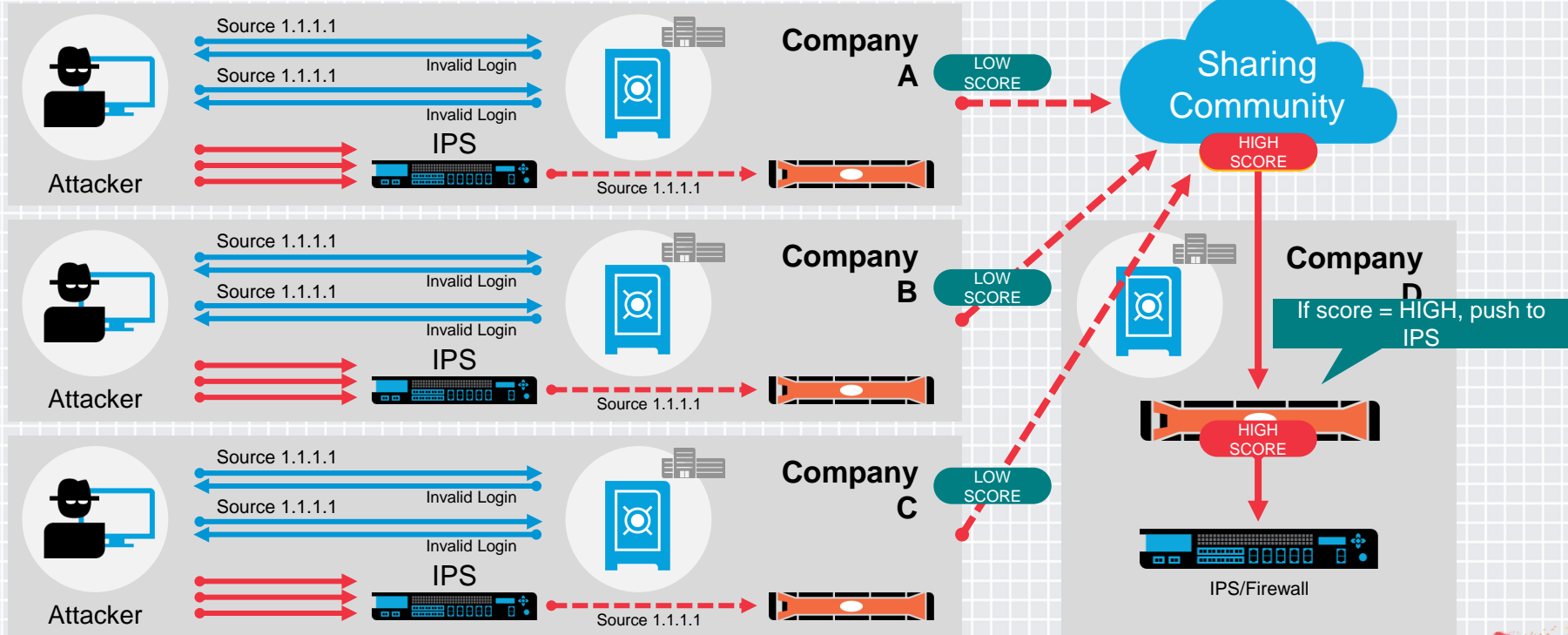
# Use Case: Automated Actions

## Current approach



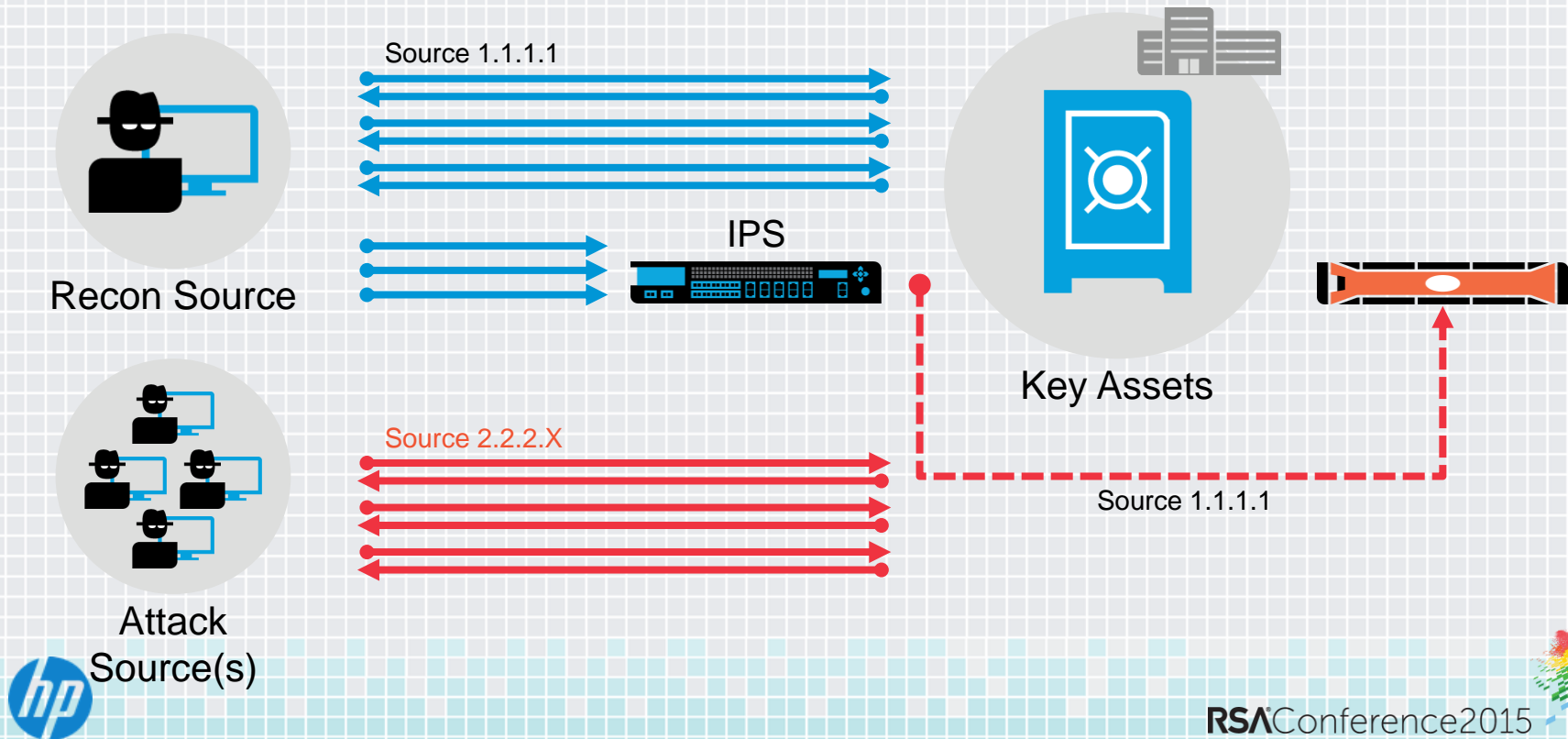
# Use Case: Automated Actions

## New approach



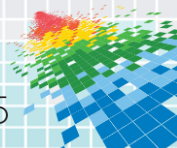
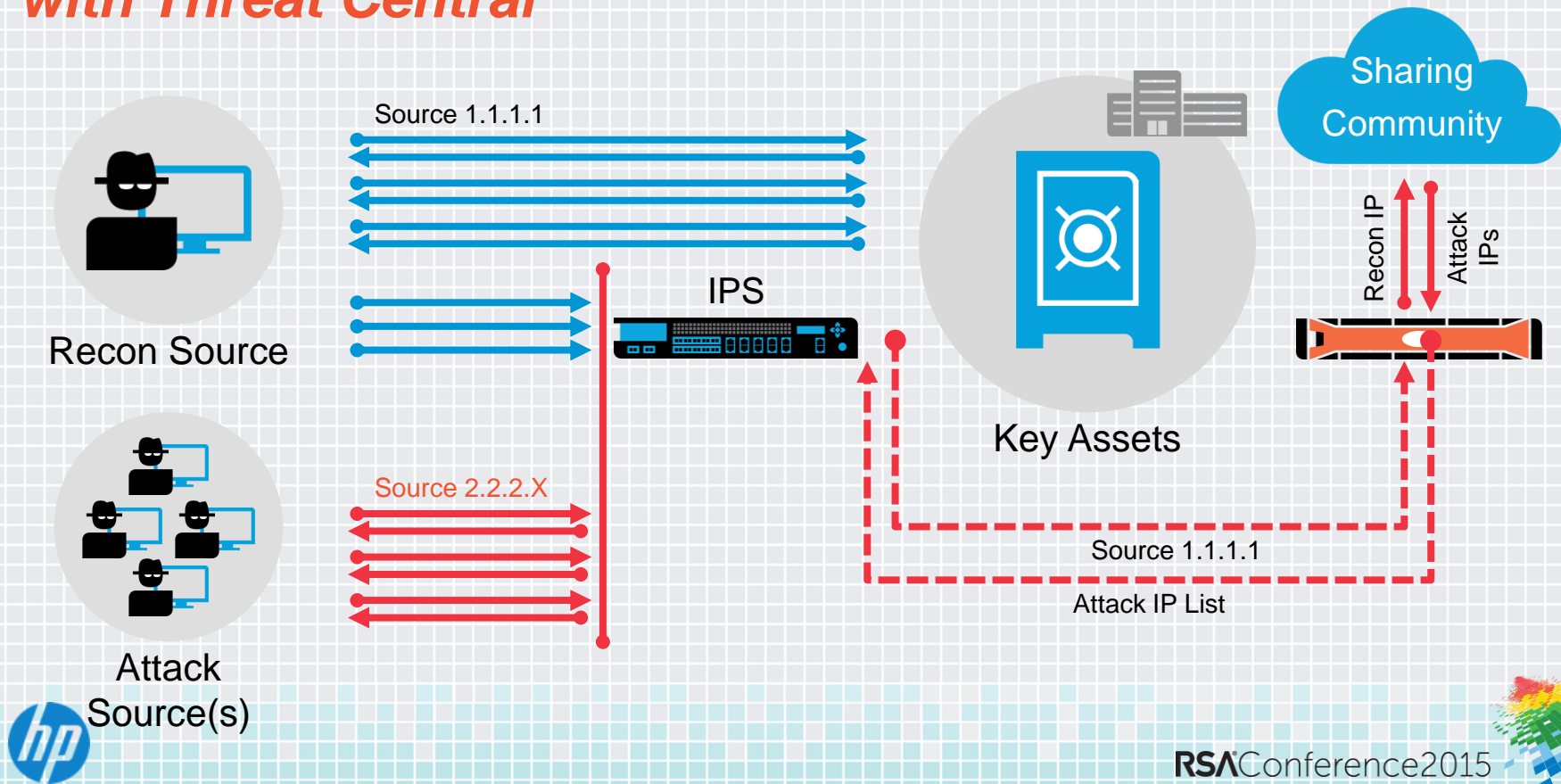
# Use Case: Proactive Block Lists - RECON

## Current approach

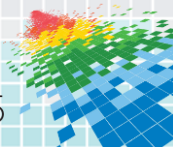
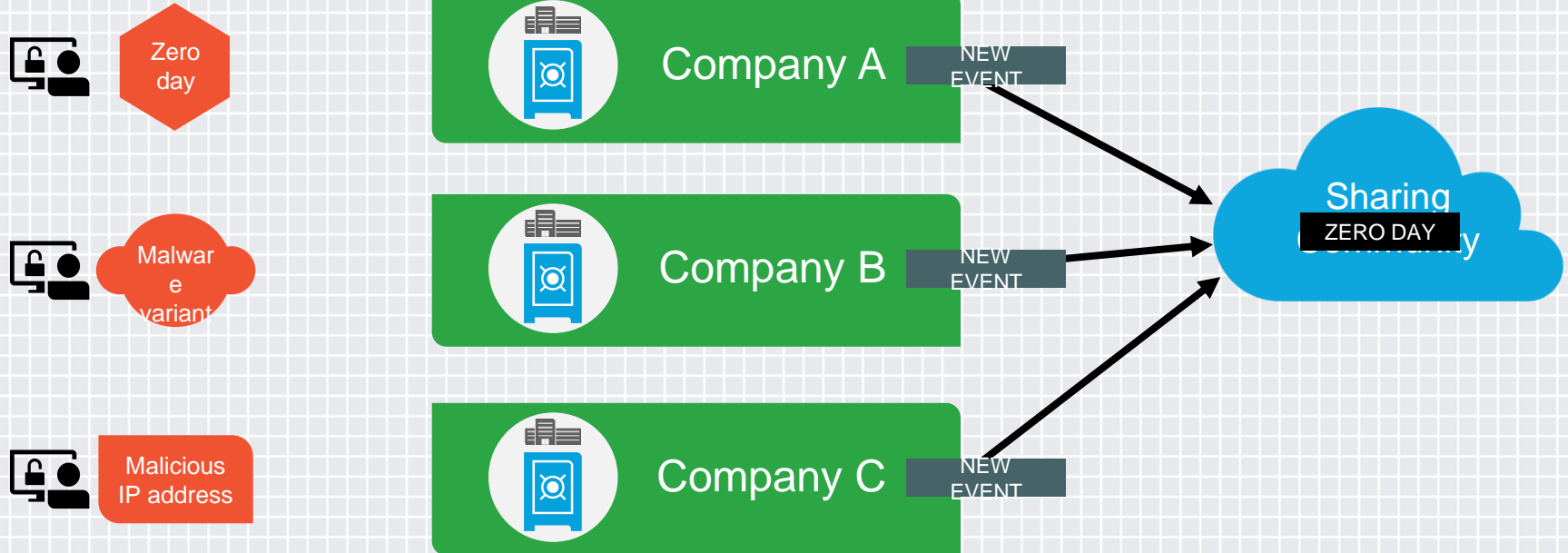


# Use Case: Proactive Block Lists - RECON

## with Threat Central



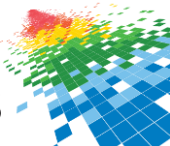
# Summarizing: Leveraging the Community





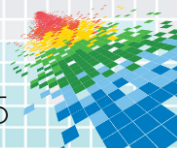
# What to Look for in Threat Sharing Systems

- ◆ Automated bi-directional sharing
- ◆ Analysis of the data
- ◆ Actionable derived results
- ◆ Tap into the existing community of security experts
- ◆ Product agnostic sharing is a must



# How to Apply

- ◆ Within three months, select a collaboration system that produces
  - A- Actionable results
  - B- Indicators that are relevant to you
- ◆ Start collaborating with both human-human and machine-machine using a system that will send indicators automatically as a result of the collaboration.
- ◆ Leverage strategic intelligence (context) to better defend – defend with purpose



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

# Thank You

