

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-W04

## Next Wave of Security Operationalization

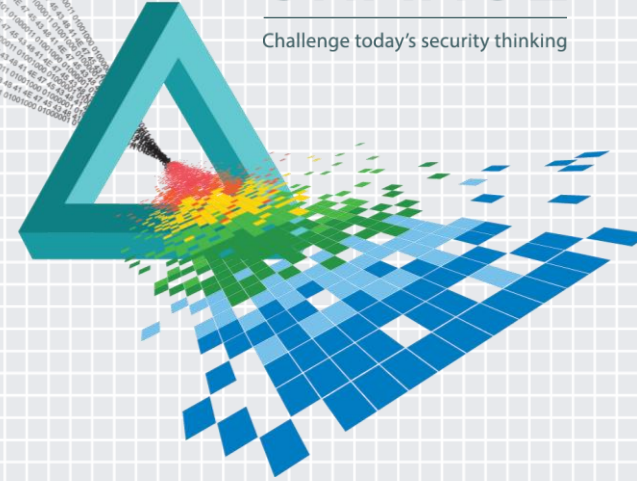
**Peter Lam**

---

A National Bank  
Security Analyst

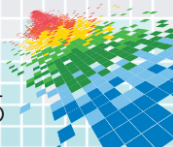
# CHANGE

Challenge today's security thinking



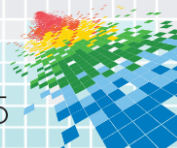
# Disclaimer

- ◆ The views and opinions expressed in this presentation are those of the authors and do not necessarily represent of position of RSA or the author's employer



# Speaker Bio

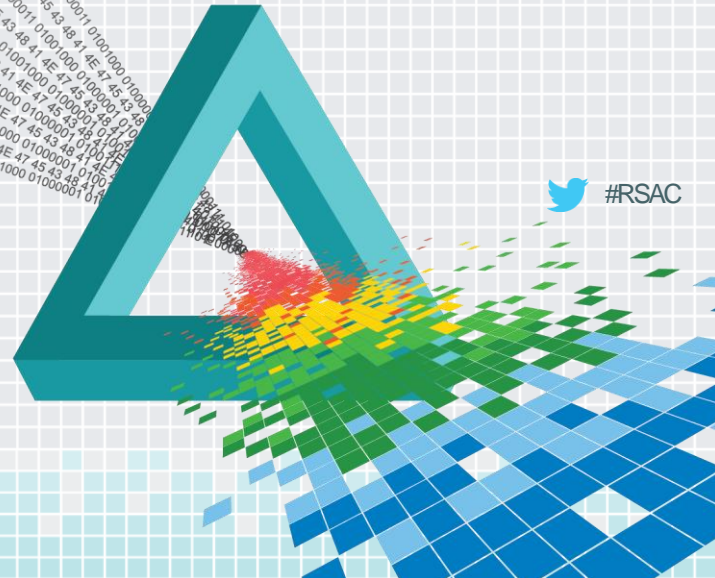
- ◆ Who am I?
  - ◆ Peter Lam
  - ◆ 1<sup>st</sup> Time Presenter at RSA
  - ◆ Information Security Staff in a national bank
  - ◆ 20+ Year of Professional IT Experience
    - ◆ Experience in:
      - ◆ System / Platform Engineering, Application Development, Security, Incident Response



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

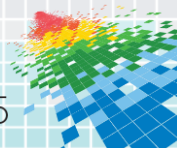
## Purpose & Audience



 #RSAC

# Purpose & Audience

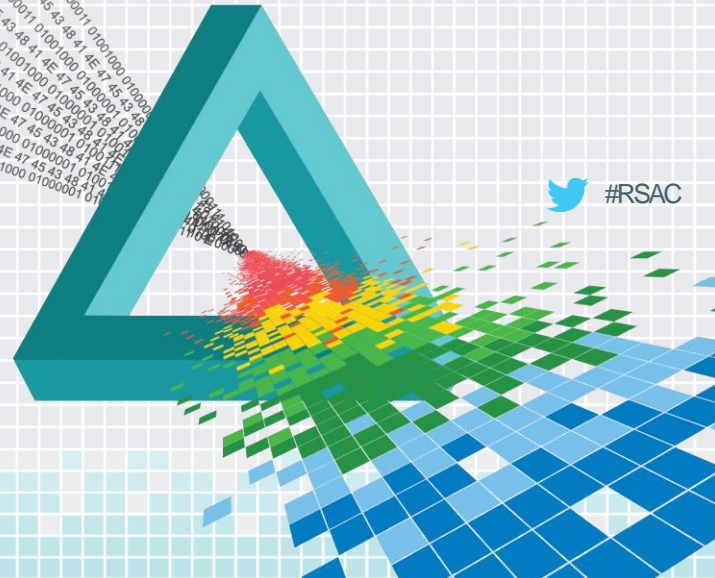
- ◆ Purpose
  - ◆ Help Drive Better Adoption of Technologies (Vendor & Us)
    - ◆ Demand Drives Supply
  - ◆ Definitely NOT to Repeat Presentations around STIX/TAXII by MITRE team
  - ◆ Introduce A Proof-of-Concept Threat Operationalization Platform
    - ◆ Explain Problems These Technologies Help Solve NOW
- ◆ Audience
  - ◆ Everyone who Wants to Learn about STIX & TAXII but Want Something that They Can Try Without Too Much Cost



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## What's the problem?



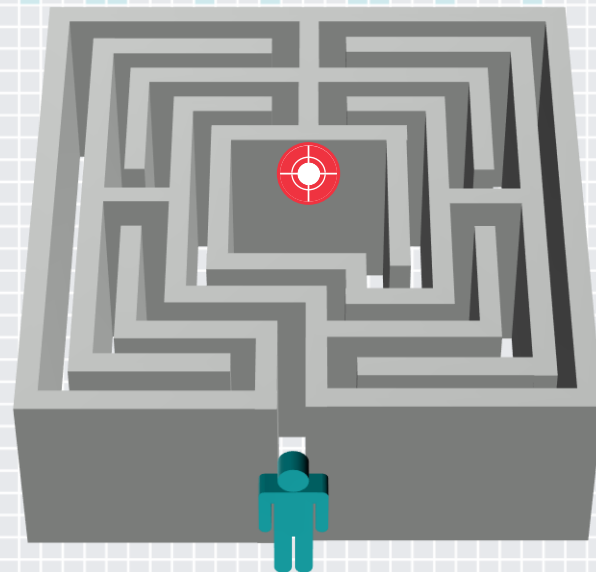
# Intelligence Sources

price	Paid		Free		
	type	<b>Control System</b>	<b>Private Vendor</b>	<b>Open Source</b>	<b>Government</b>
format	<b>Proprietary / System Specific</b>	<b>Portal / Secured Email</b>	<b>CSV / CIF / RSS</b>	<b>PDF / RSS</b>	<b>PDF</b>
touch needed	<b>No</b>	<b>Maybe</b>	<b>Maybe</b>	<b>Yes</b>	<b>Yes</b>
e.g.	<b>Firewall</b>	<b>ISAC / Boutique Security Firm</b>	<b>OSINT</b>	<b>CISCP</b>	<b>Any (Teaser News)</b>

CIF – Collective Intelligence Framework  
 ISAC – Information Sharing and Analysis Center  
 OSINT – Open Source Intelligence  
 CISCP – Cyber Information Sharing and Collaboration Program

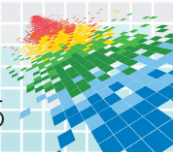
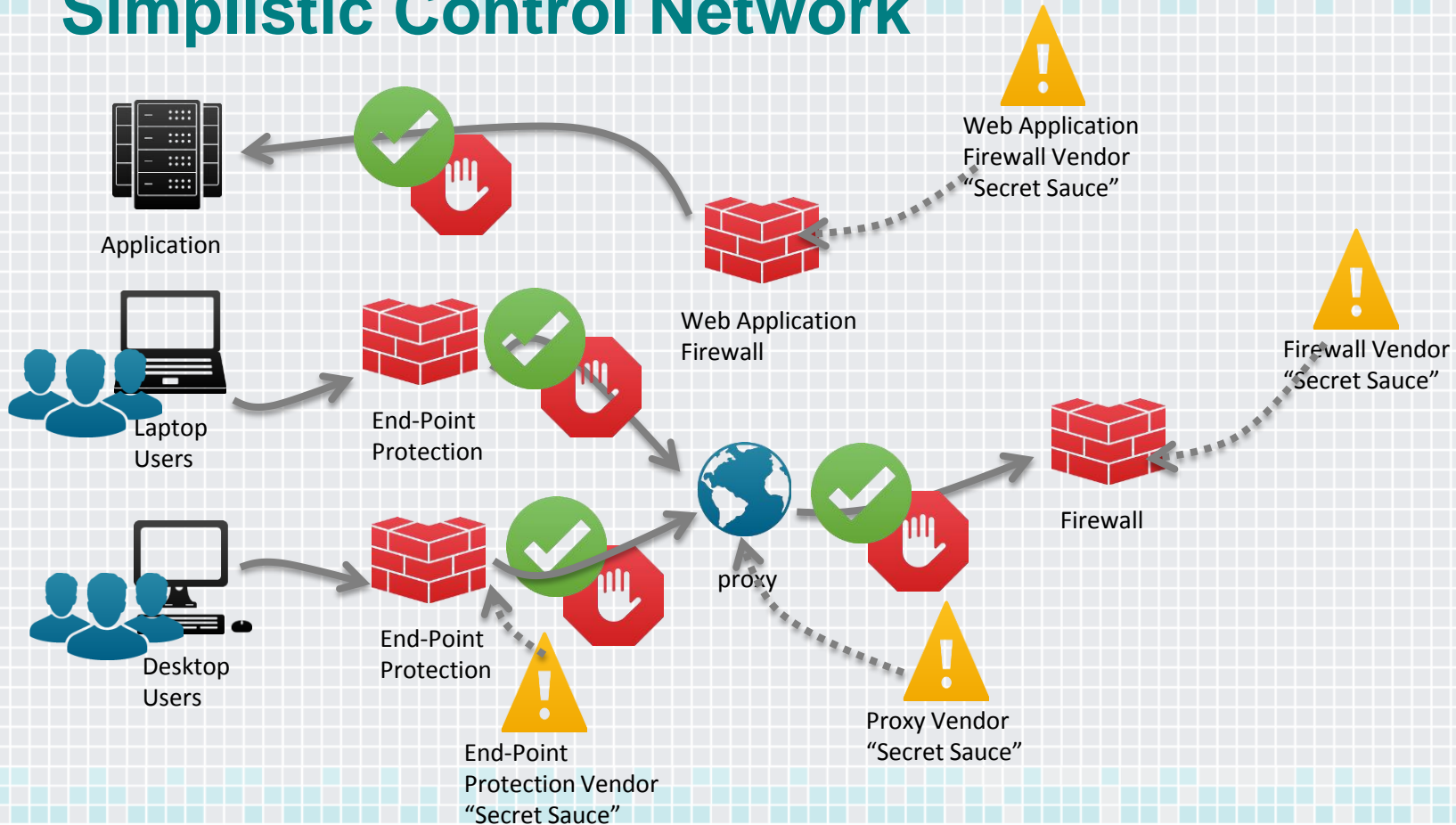
# Challenge One

- ◆ Ineffective and Labor Intensive, because
  - ◆ Multiple delivery channels
    - ◆ Mostly manual effort
      - ◆ Missed email; Staff on vacation, etc.
  - ◆ Format varies greatly among vendor
    - ◆ Comma Separated Value (CSV), Extensible Markup Language (XML), Unformatted text
      - ◆ Needs multiple parsers for different sources
      - ◆ Human error; copy & paste, field extraction
  - ◆ Huge amount of Intelligence

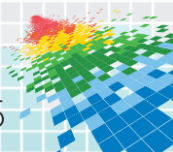
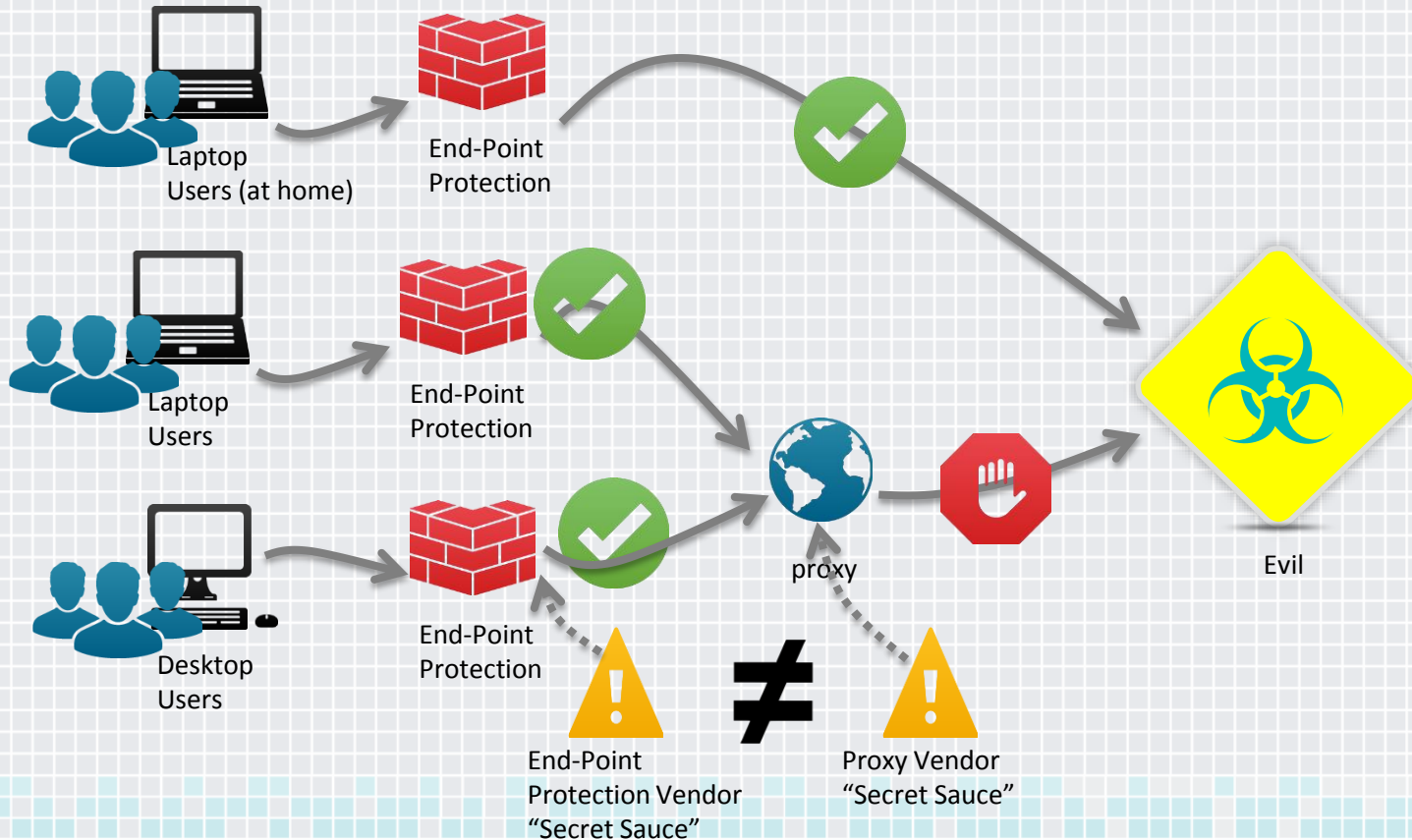




# Simplistic Control Network



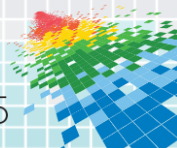
# Simplistic Control Network



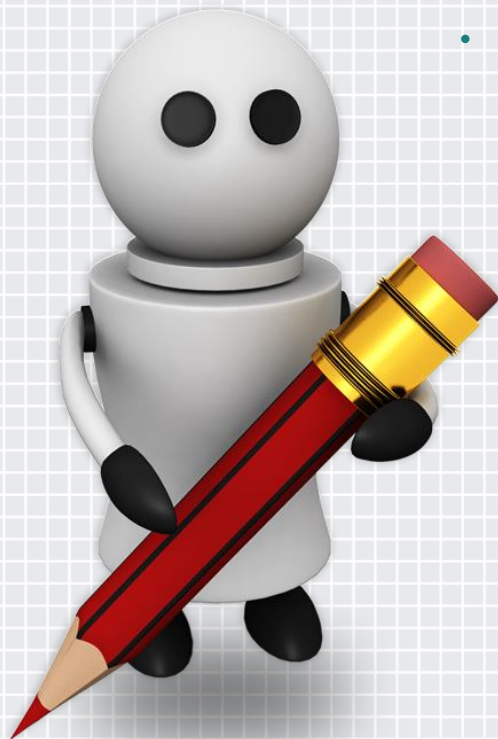
# Challenge Two



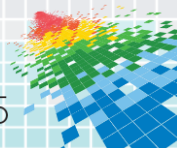
- ◆ Vendors Most Likely Won't Share Their "Secret Sauce", or indicators
  - ◆ Unless Part of the Sharing Ring
  - ◆ Not Hard to Understand "Why"
- ◆ Same Indicator Not Replicated Across Multiple Controls
  - ◆ Multi-Layer Security Control But Single-Layer Security Intelligence?



# What?



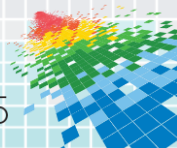
- Operationalization of Threat Intelligence Handling around Indicators
  - Automatically:
    - Collect
      - Receive Threat Intelligence
    - Dissect
      - Extract Crucial Indicators
    - Detect
      - Search for Realized Threat
    - Distribute
      - Intelligence across All Layers of Controls
    - Prevent
      - Deploy Prevention Control



# Why?



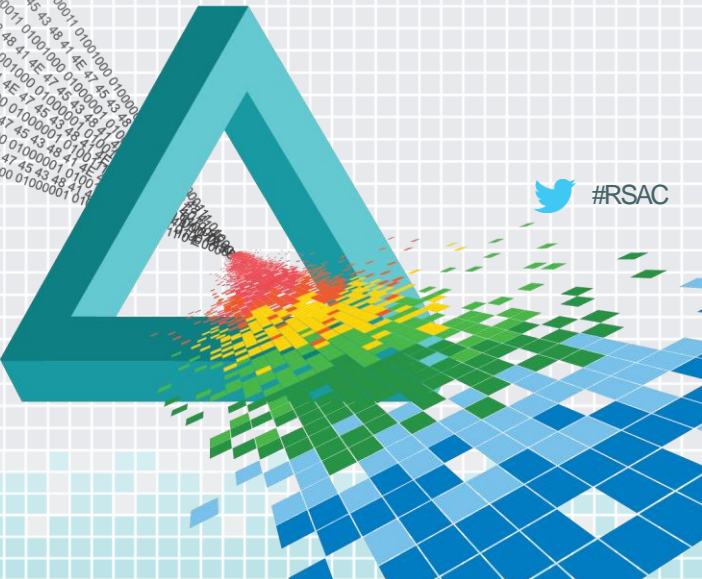
- Bad Guys have Malware Supply Chain
  - Commercialization of Crime Ware
    - Operationalize of Malware Development
- Highly Time Sensitive Response Needed
  - Exponentially Expensive to Recover
- Machines Should do the Heavy Lifting, NOT HUMAN, ESPECIALLY NOT the ANALYSTS



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## How?

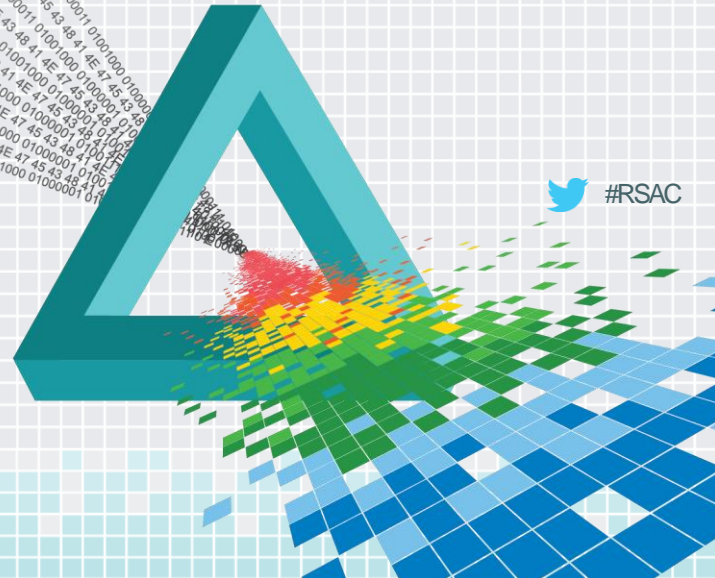


 #RSAC

# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

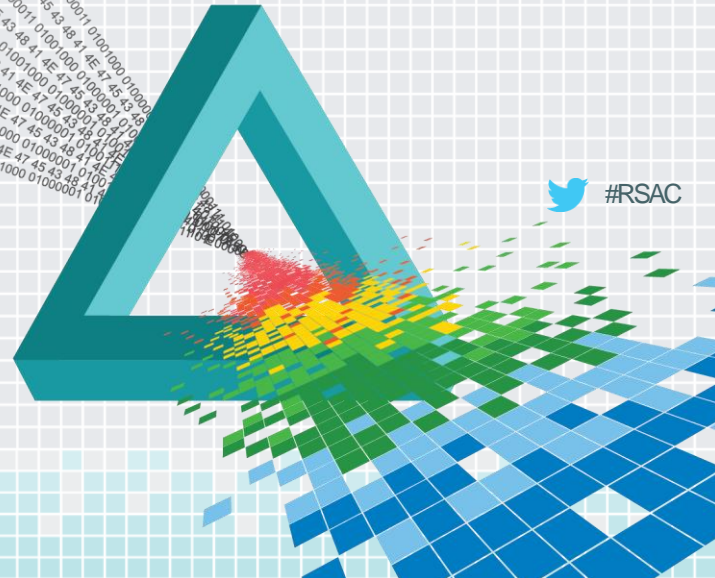
## High Level Understanding of the Enabling Technologies



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

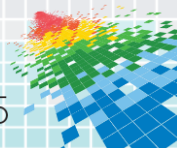
## Protocol Technologies





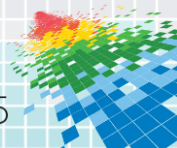
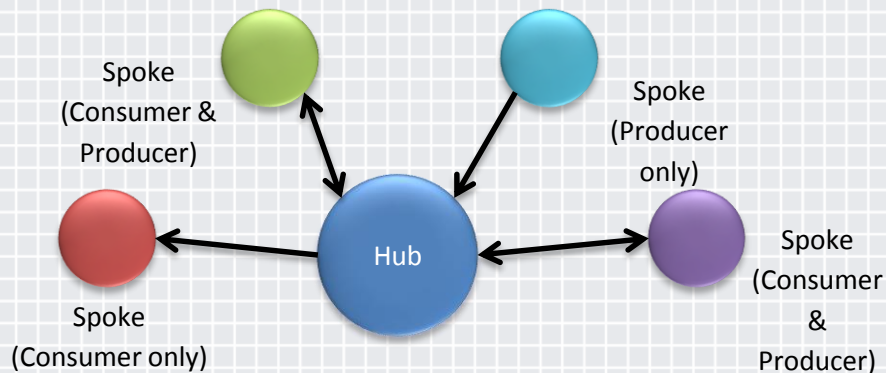
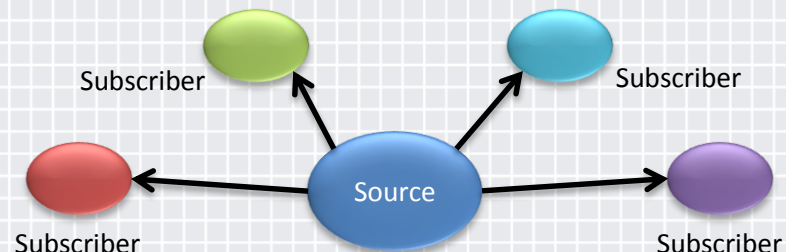
# TAXII

- ◆ Stands for
  - ◆ Trusted Automated eXchange of Indicator Information
- ◆ Threat Intelligence Exchange Agreements
  - ◆ How messages are expressed and transported
  - ◆ Exchange Models
    - ◆ Source-Subscriber / Hub & Spoke / Peer-to-Peer Models
  - ◆ Role Models
    - ◆ Data Producers / Consumers
  - ◆ Service Models



# Exchange Model

- ◆ Source-Subscriber Model
  - ◆ Typical for Current Threat Intelligence (TI) Vendor / Customer Relationship Model
- ◆ Hub & Spoke Model
  - ◆ Suitable for used in Large Organizations
    - ◆ Various Contract Owners with TI vendors and become a Spoke (Consumer & Producer)
    - ◆ Play Attention to Sharing Agreement



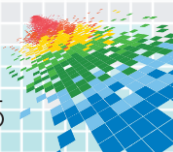
# Role & Service Models

## ◆ Role Models

- ◆ Producer Only
- ◆ Consumer Only
- ◆ Producer & Consumer

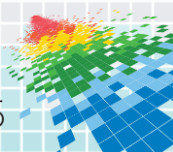
## ◆ Service Models

- ◆ Discovery Service
- ◆ Collection Management Service
- ◆ Inbox Service
- ◆ Poll Service



# STIX

- ◆ Stands for
  - ◆ Structured Threat Information eXpression
- ◆ Structured Way of Describing Cyber Threat
  - ◆ Eight Main Constructs



# STIX Eight Constructs



## Observable

- ◆ What activity was observed



## Indicator

- ◆ What should be looked for



## Incident

- ◆ Where was it seen



## Tactics, Techniques & Procedures (TTP)

- ◆ What does it do

## ◆ ExploitTarget

- ◆ What weakness does it exploit

## ◆ Campaign

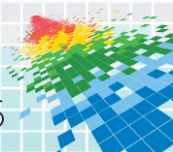
- ◆ Why

## ◆ ThreatActor

- ◆ Who

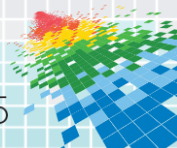
## ◆ Course of Action

- ◆ Suggested Action



# Profiles

- ◆ Contracts between Sharing Parties (Producers to Consumers)
- ◆ Define In-Scope / Out-of-Scope
  - ◆ Which Constructs / Elements Required
- ◆ More on This



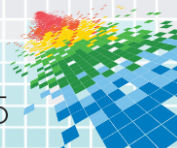
# Related Standards

- ◆ STIX's Observable Indicators leverage CybOX to precisely describe the details
- ◆ CybOX
  - ◆ Cyber Observable eXpression
  - ◆ About 80 Objects

## B2. Which objects currently have representations defined in CybOX?

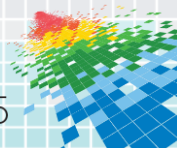
The following list identifies the current objects with CybOX-defined representations:

Account	Network Route Entry	Win Event
Address	Network Subnet	Win Executable File
API	PDF File	Win File
Artifact	Pipe	Win Handle
Code	Port	Win Kernel Hook
Custom	Process	Win Kernel
DNS Cache	Product	Win Mailslot
DNS Query	Semaphore	Win Memory Page Region
DNS Record	Socket	Win Mutex
Device	Socket Address	Win Network Route Entry
Disk	System	Win Network Share
Disk Partition	URI	Win Pipe
Email Message	UNIX File	Win Prefetch
File	UNIX Network Route Entry	Win Process
GUI Dialogbox	UNIX Pipe	Win Registry Key
GUI	UNIX Process	Win Semaphore
GUI Window	UNIX User Account	Win Service
HTTP Session	UNIX Volume	Win System
Library	User Account	Win System Restore
Link	User Session	Win Task
Linux Package	Volume	Win Thread
Memory	WhoIS	Win User Account
Mutex	Win Computer Account	Win Volume
Network Route	Wind Critical Selection	Win Waitable Timer
Network Connection	Win Driver	X509 Certificate
Network Flow	Win Event Log	
Network Packet		



# Which Fundamental Problems Were Solved

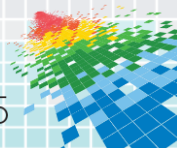
- ◆ TAXII
  - ◆ Solves Transport / Channel Problem
    - ◆ No more secured emails, RSS, portal access to obtain intelligence
- ◆ STIX / CyBox
  - ◆ Solves Intelligence Format Problem
    - ◆ No more free form text, or CSV
      - ◆ No more copy and paste
      - ◆ No more extracting searchable terms from emails, or portal
    - ◆ Precisely Describe
- ◆ Allow Machine Extraction without Human Interaction





# Now What?

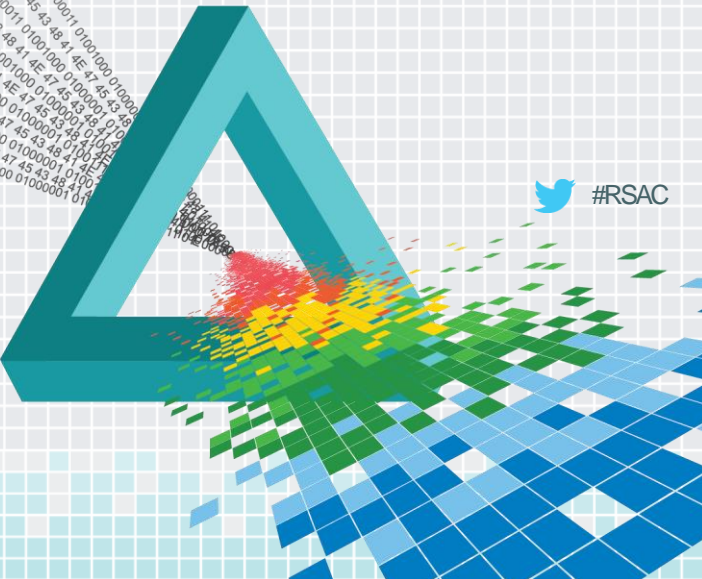
- ◆ Read the XML encoded intelligence manually?
- ◆ Have a way to precisely describe and share intelligence between parties
  - ◆ Of course NOT
    - ◆ At the minimum
      - ◆ Search for indicators like IPs / URLs
      - ◆ Add IPs / URLs to “Block” list
        - ◆ Propagate intelligence across control layers



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

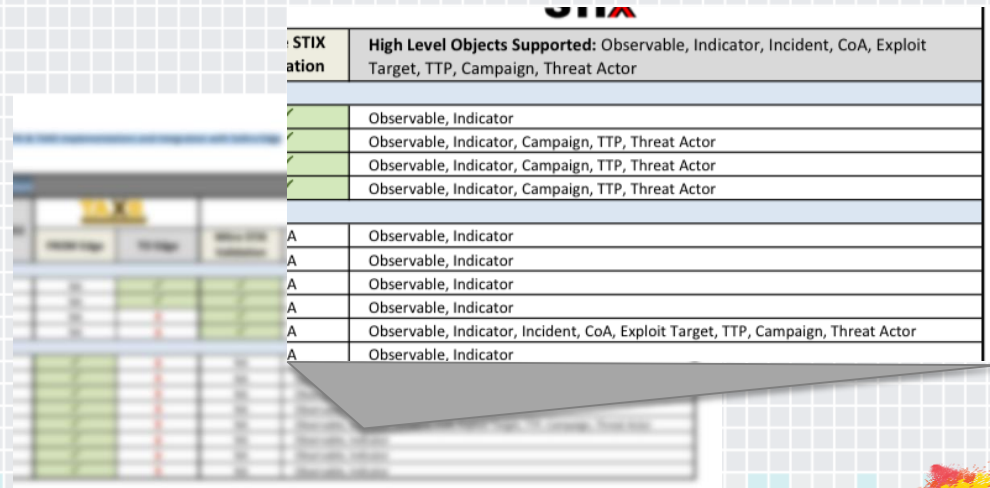
## Platform Technologies



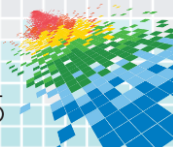
 #RSAC

# Feeds

- ◆ Compliant with Standards
- ◆ Confirm Which Constructs are Supported with Vendors
- ◆ Standards Vary Board By Design
  - ◆ Data Fields Mostly Not Required
- ◆ At least, Observable / Indicators



STIX ation	High Level Objects Supported: Observable, Indicator, Incident, CoA, Exploit Target, TTP, Campaign, Threat Actor
✓	Observable, Indicator
✓	Observable, Indicator, Campaign, TTP, Threat Actor
✓	Observable, Indicator, Campaign, TTP, Threat Actor
✓	Observable, Indicator, Campaign, TTP, Threat Actor
A	Observable, Indicator
A	Observable, Indicator
A	Observable, Indicator
A	Observable, Indicator
A	Observable, Indicator, Incident, CoA, Exploit Target, TTP, Campaign, Threat Actor
A	Observable, Indicator



# STIX Profile

- ◆ Without Profile
  - ◆ Feed Still Compliant, but Not As Rich
    - ◆ Time Reference
    - ◆ Confidence Level

Valid\_Time\_Position 0..n

ValidTimeType

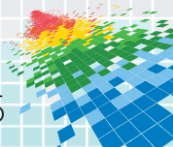
Specifies the time window for which this Indicator is valid.

Observable 0..1	ObservableType	Specifies a relevant cyber observable for this Indicator.
Composite_Indicator_Expression 0..1	CompositeIndicatorExpressionType	Specifies a multipartite composite Indicator.
Related_TTP 0..n	RelatedTTPType	Specifies the relevant TTP indicated by this Indicator.
Kill_Chain_Phases 0..1	KillChainPhaseReferenceType	Specifies relevant kill chain phases indicated by this Indicator.
Test_Mechanisms 0..1	TestMechanismsType	The TestMechanisms field specifies Test Mechanisms effective at identifying the cyber Observable specified in this cyber threat Indicator.
Likely_Impact 0..1	StatementType	Specifies the likely potential impact within the relevant context of this Indicator were to occur. This is typically local to an Indicator consumer and not typically shared. This field includes a Description of the likely potential impact within the relevant context of this Indicator were to occur and a Confidence held in the accuracy of this assertion. NOTE: This structure potentially still needs to be fleshed out more for structured characterization of impact.
Suggested_COAs 0..1	SuggestedCOAType	The Suggested_COAs field specifies suggested Courses of Action for this cyber threat Indicator.
Handling 0..1	MarkingType	Specifies the relevant handling guidance for this Indicator. The valid marking scope is the nearest indicatorBaseType ancestor of this Handling element and all its descendants.
Confidence 0..1	ConfidenceType	Specifies a level of confidence held in the accuracy of this Indicator.
Related_Indicators 0..n	RelatedIndicatorType	The Related_Indicators field is optional and enables content producers to express a relationship between the enclosing Indicator (i.e., the subject of the relationship) and a disparate Indicator (i.e., the object of the relationship).
Related_Campaigns 0..1	RelatedCampaignReferenceType	The Related_Campaigns field captures references to related campaigns. Note that unlike most other relationships, this Related_Campaigns relationship is not reciprocal.

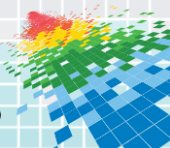
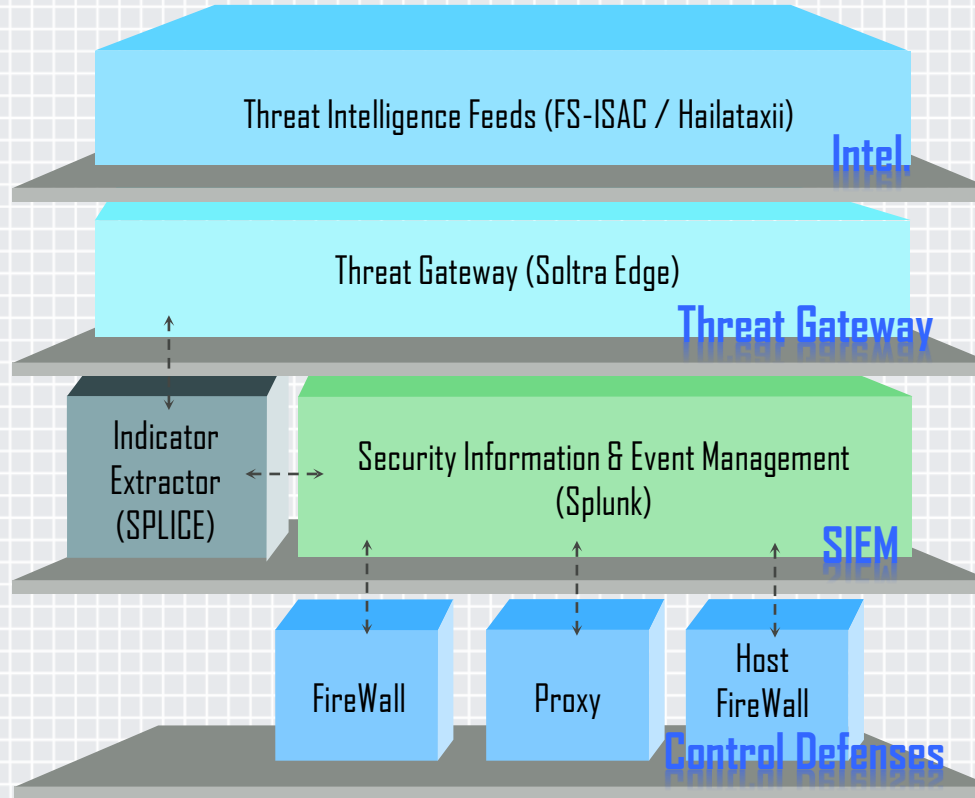
Confidence 0..1

ConfidenceType

Specifies a level of confidence held in the accuracy of this Indicator.

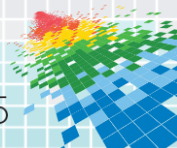


# POC Platform

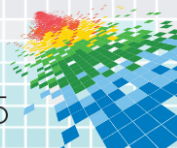
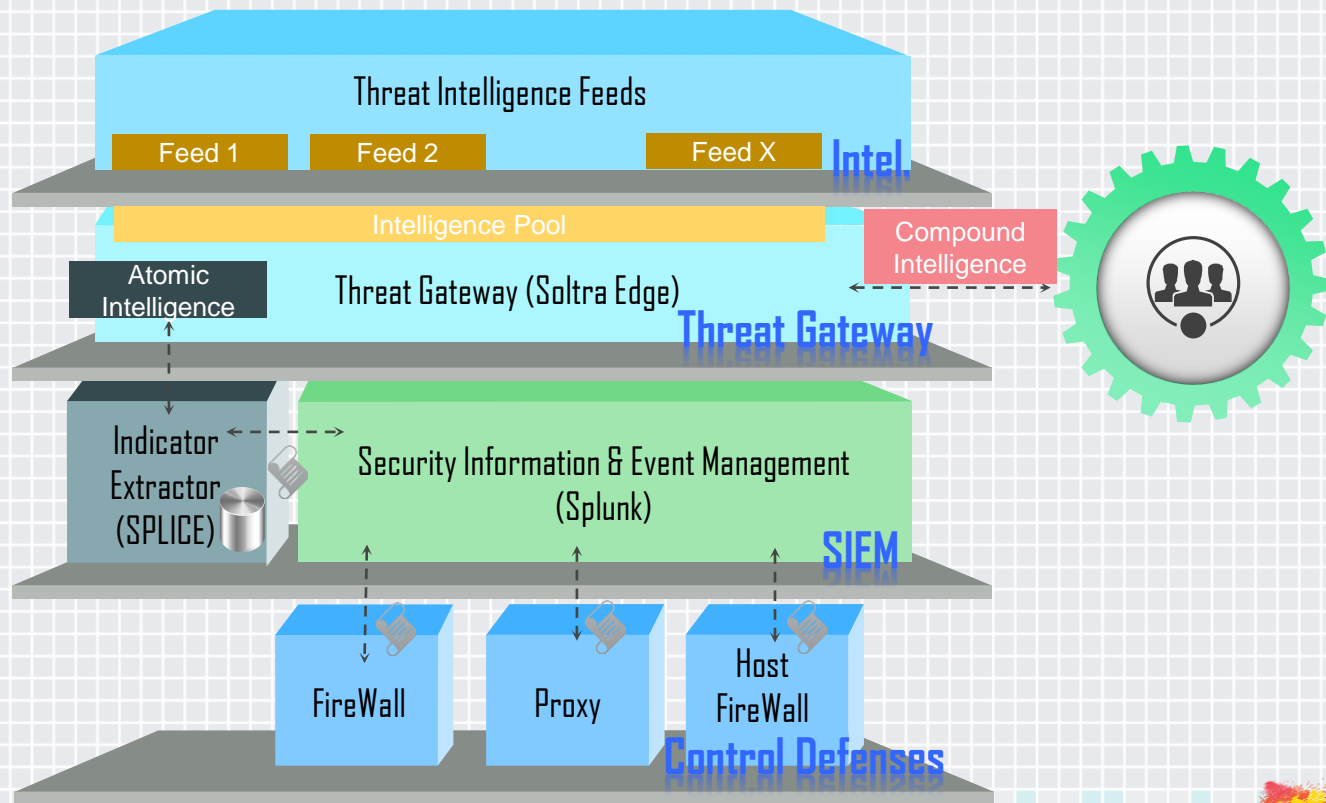


# Platform

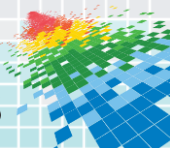
- ◆ Threat Intelligence Gateway
  - ◆ Receive Threat Intelligence
    - ◆ Talk TAXII
    - ◆ Decompose STIX
- ◆ Indicator Extractor
  - ◆ Extract Indicator of Compromise from STIX
  - ◆ Search for Realized Threat against SIEM
- ◆ Security Information and Event Management (SIEM)
  - ◆ Initiate Incident Response Upon Match
  - ◆ Initiate First Response
    - ◆ Block IP/URL at perimeter
- ◆ Scripts
  - ◆ Add Indicators to “Block” list



# POC Platform



# Demo Screen

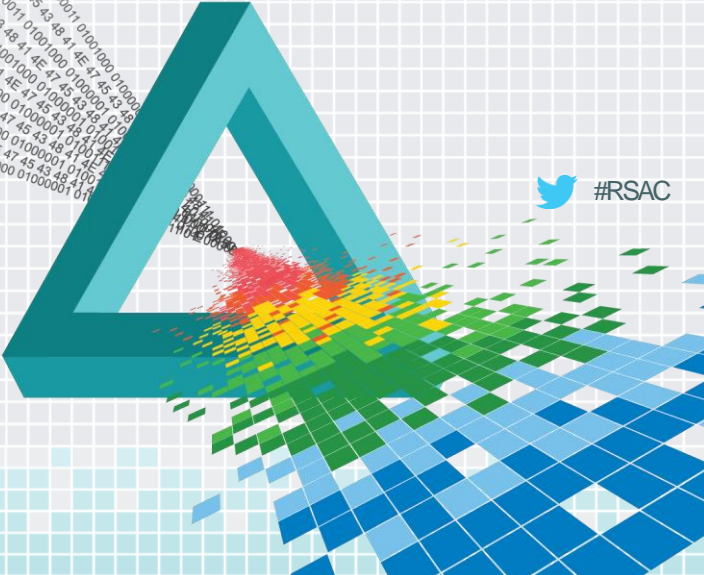




# RSA<sup>®</sup>Conference2015

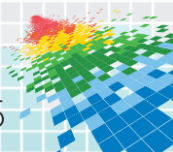
San Francisco | April 20-24 | Moscone Center

Apply



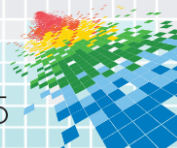
# Summary

- ◆ Threat Intelligence Sharing Technologies are Maturing
- ◆ Feed Readily Available (Hailataxii & FS-ISAC if member)
- ◆ POC Platform can be Created with Minimum Cost
- ◆ Automatic
  - ◆ Detect Indicator for Realized Threat
  - ◆ Deploy Indicator to “Block” list



# Apply

- ◆ Obtain Quality Vendor Feed
- ◆ Deploy POC Platform
- ◆ Create Automatic Mechanism



# Reference & Tool

- ◆ Feed
  - ◆ Hailataxii.com (Open Source)
  - ◆ FS-ISAC
- ◆ Soltra EDGE ([www.soltra.com](http://www.soltra.com))
- ◆ Splunk SA-Splice ([splunkbase.splunk.com/app/2637](http://splunkbase.splunk.com/app/2637))
- ◆ Script to Extract All Atomic Indicators

