RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: ANF-R04

Making Threat Intelligence Actionable: Recommending Responses with STIX

David McGrew

Fellow
Cisco Systems
@mcgrewAnalog

Jyoti Verma

Technical Leader
Cisco Systems

#RSAC

Introduction

Security process cycle

Poll

- What is the mean time to detect cyber threats in your organization ?
  - < 3 hours
  - < 3 days
  - < 3 weeks
  - < 3 months

https://pollev.com/mrti

Response

- Investigate
  - Obtain more information about a threat
- Mitigate
  - Block, but not eliminate, a threat
- Remediate
  - Fix or eliminate a threat

Poll

- What is the mean time to contain/remediate cyber threats in your organization ?
  - < 3 hours
  - < 3 days
  - < 3 weeks
  - < 3 months

https://pollev.com/mrti

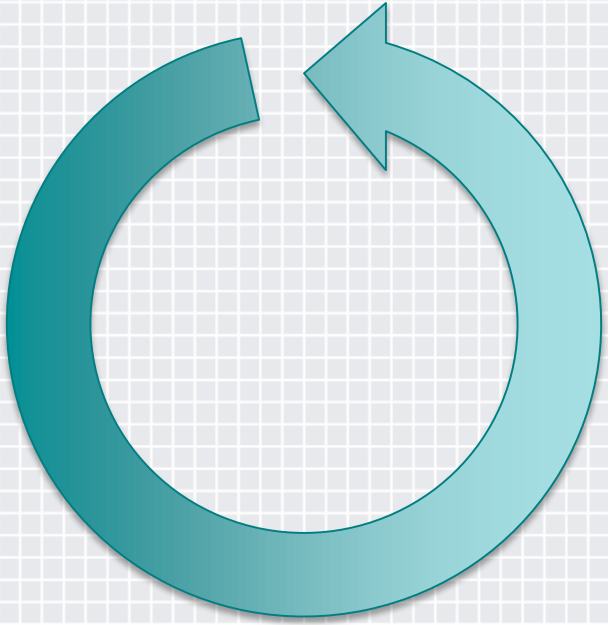
Connecting detection to response

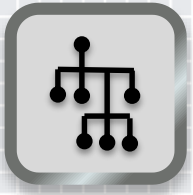
- There may be multiple detection sources
- There may be multiple response systems
- A human should be in the loop
  - Or have that option
- Processes should be automatable
  - One-click approval

Connecting detection to response

Cloud Threat Analytics

Local Threat Analytics





Network Controller

Endpoint Protection

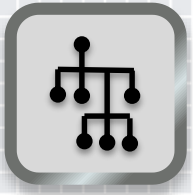
Threat Intelligence Aggregator

Cloud Threat Analytics

Local Threat Analytics

TIA

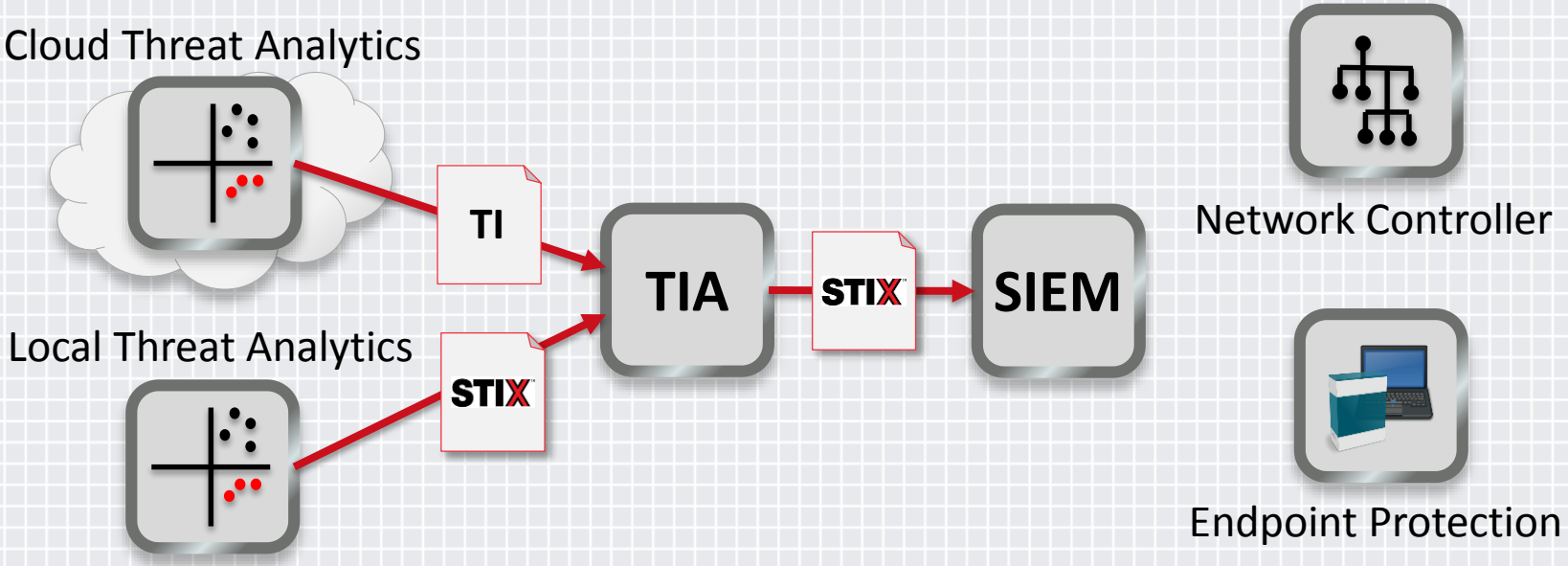
SIEM



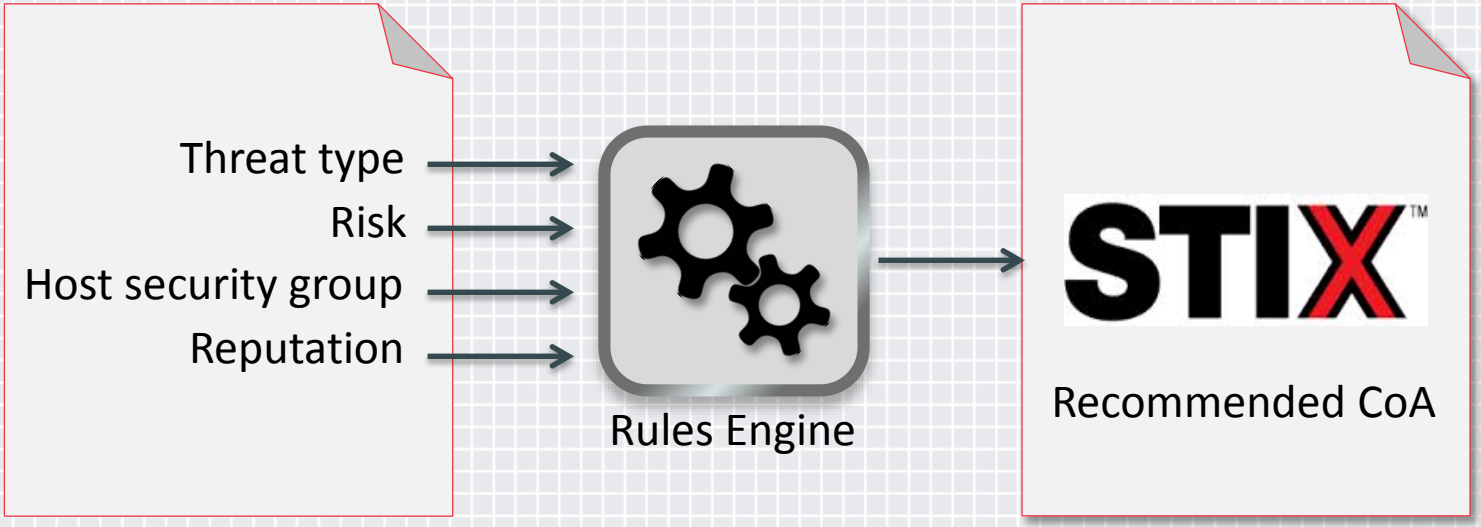
Network Controller

Endpoint Protection

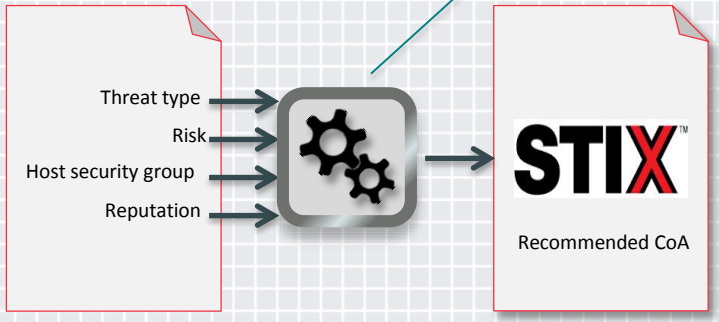
Threat Intelligence Aggregator

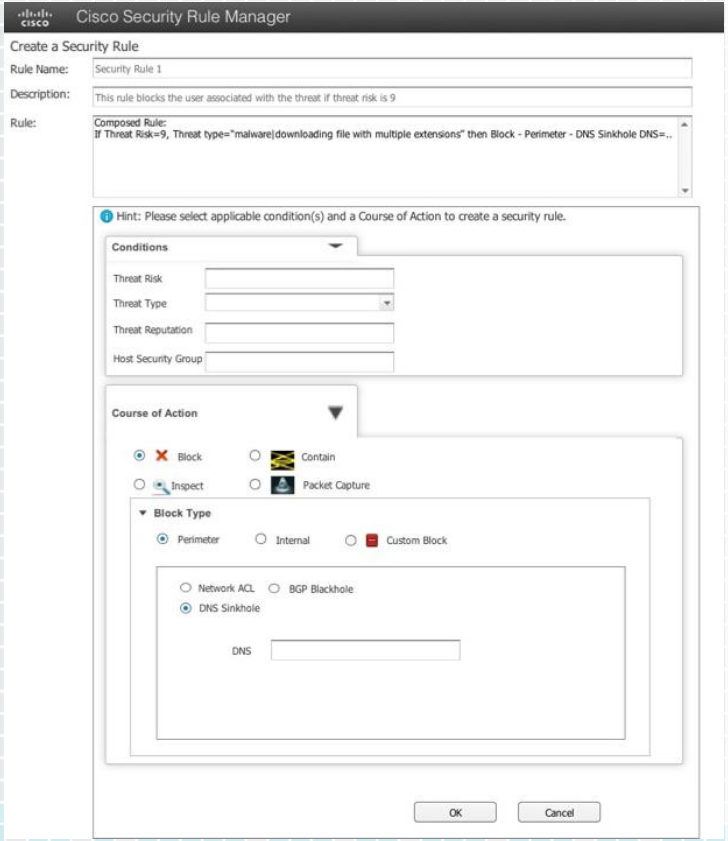


Threat Intelligence Aggregator



Threat Intelligence Aggregator

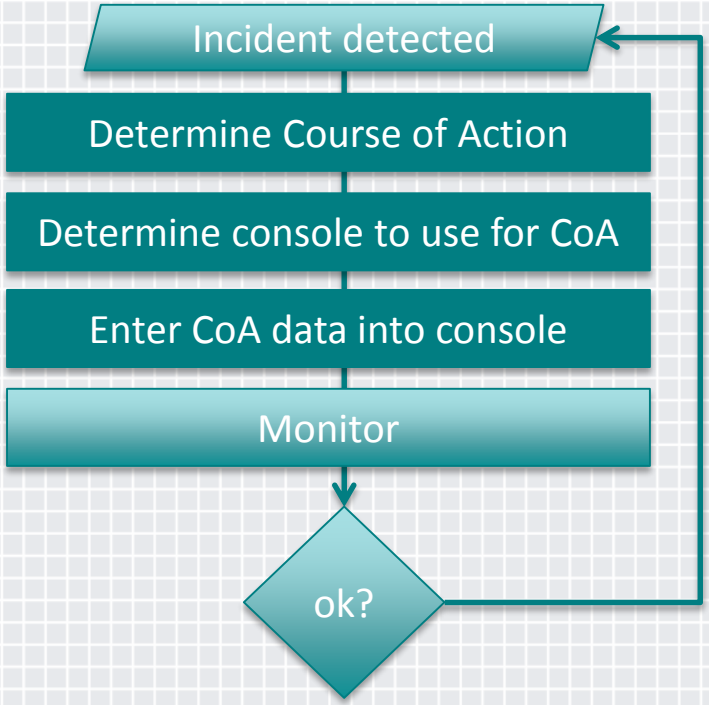




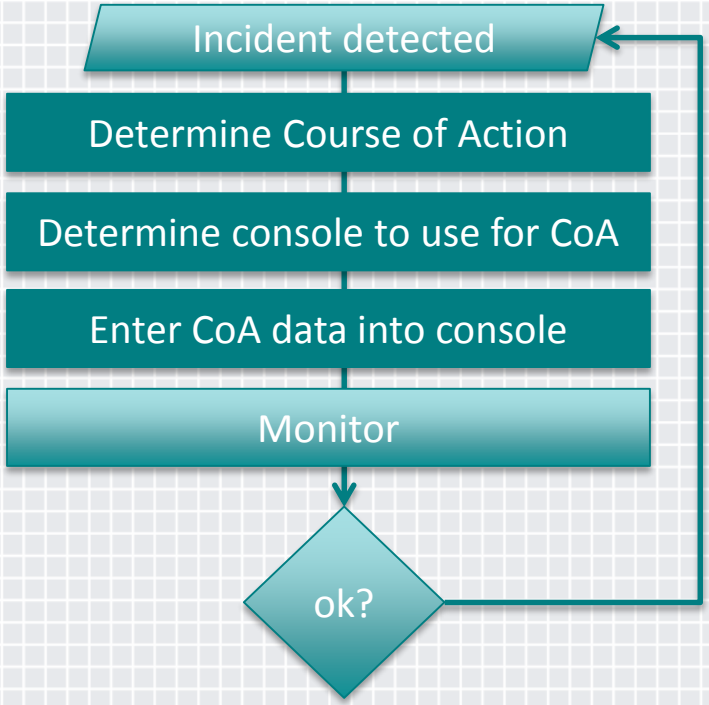
Rules

Risk	Threat Type	Default Suggested Course of Action
8-9	malware using automatically generated domain (DGA)	Block compromised host
8-9	malware using url-string as communication channel (C&C)	Block compromised host
8-9	malware using https communication channel	Block compromised host
8-9	malware downloading suspicious file	Block compromised host
7-8	malware using repetitive requests	Contain compromised host
7	malware downloading malicious file	Contain compromised host
6-7	misuse of web proxy auto discovery protocol (WPAD)	Tag host as suspicious and inspect through IPS
6	anonymization software (TOR)	Tag host as suspicious and inspect through IPS
5	remote desktop connection	Inspect host traffic through IPS
3	Skype	Inspect host traffic through IPS

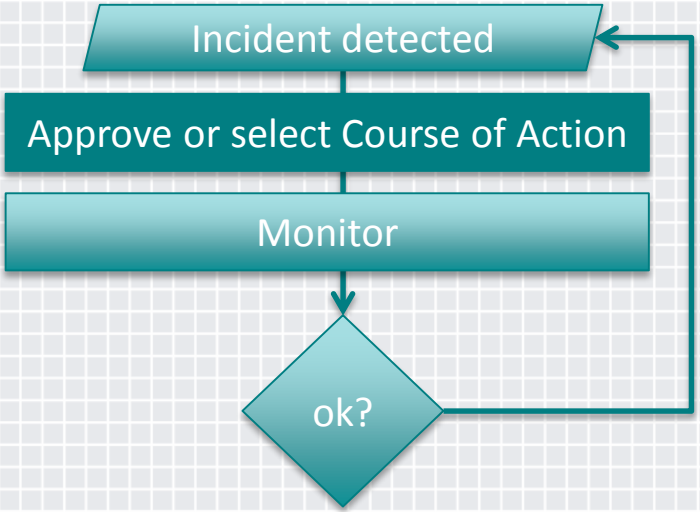
Manual



Manual



Semiautomated



Network actions

- Investigate
  - Inspect with IPS: SPAN, TAP, SDN copying or redirection
  - Netflow/IPFIX monitoring
  - Packet capture
- Mitigate
  - Perimeter blocking: BGP black hole, DNS sinkhole, ACL
  - Interior blocking: 802.1X Change of Authorization, ACL
  - Containment: VLAN tagging, SGT tagging
- Remediate
  - Containment to remediation server or service

Endpoint actions

- Investigate
  - Scan endpoint
- Mitigate
  - Kill process, Delete file
- Remediate
  - Reimage host, Remove software, Reinstall software

STIX™

Poll

What is STIX?

- Structured Threat Information eXchange
- Structured Threat Information eXpression
- Some Thing In XML

https://pollev.com/mrti

Poll

What is STIX?

- Structured Threat Information eXchange
- Structured Threat Information eXpression
- Some Thing In XML

https://pollev.com/mrti

What is STIX?

Incident

Indicator

Observable

Course of Action

Tactics, Techniques, Procedures

Campaign

Exploit Target

Threat Actor

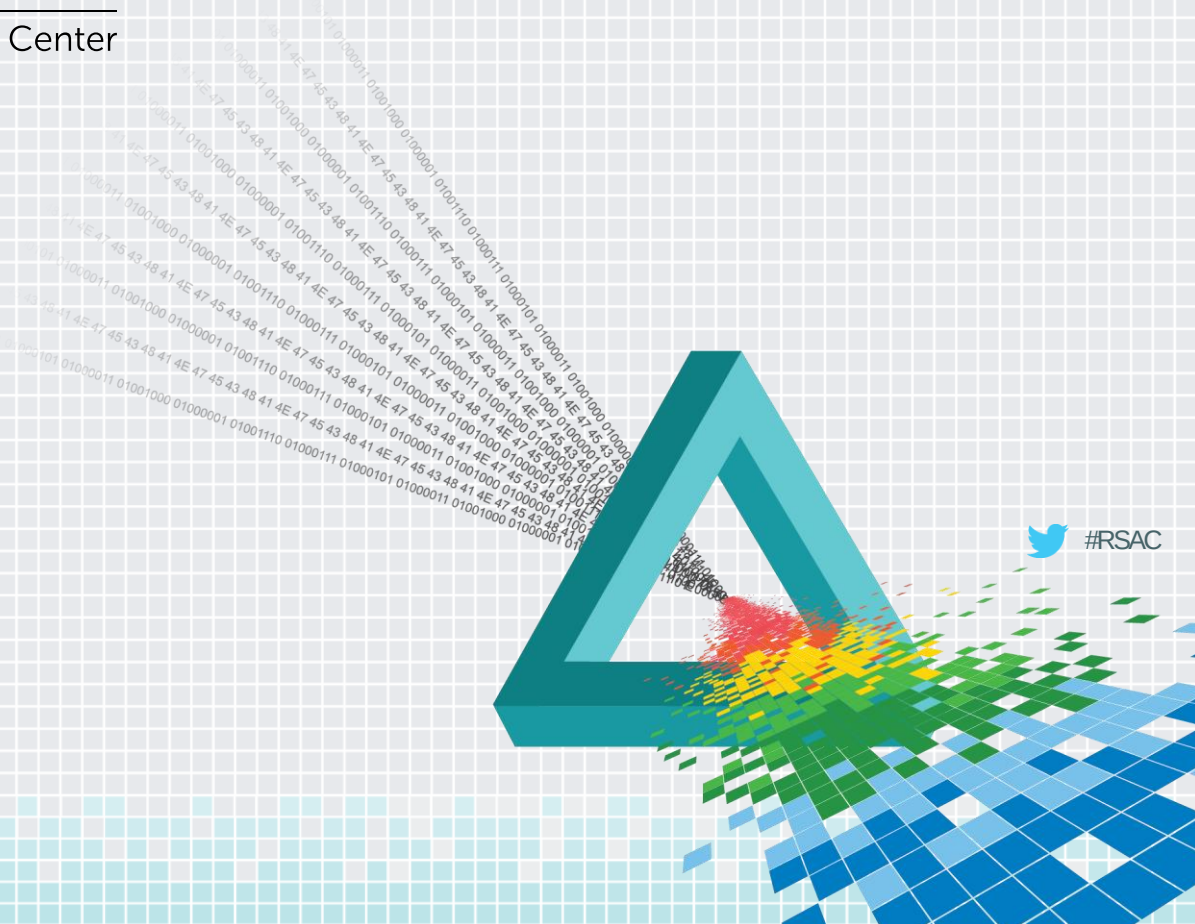
Why use STIX between detection & response?

- Standard for communicating threat info between elements
- Human and machine readable
- Standard definitions
- Normalized measures of risk and likelihood

Pros and Cons of STIX

PROS	CONS
Very comprehensive list of elements to build IoCs	Limited commercial adoption
Support for “free text” and comments	Fairly verbose and complex schema
Integration with CAPEC and MAEC for robust IoCs	Course of Actions needs further definition to be useful
Vendor neutral	

STIX Extensions



Extending CourseOfActionType

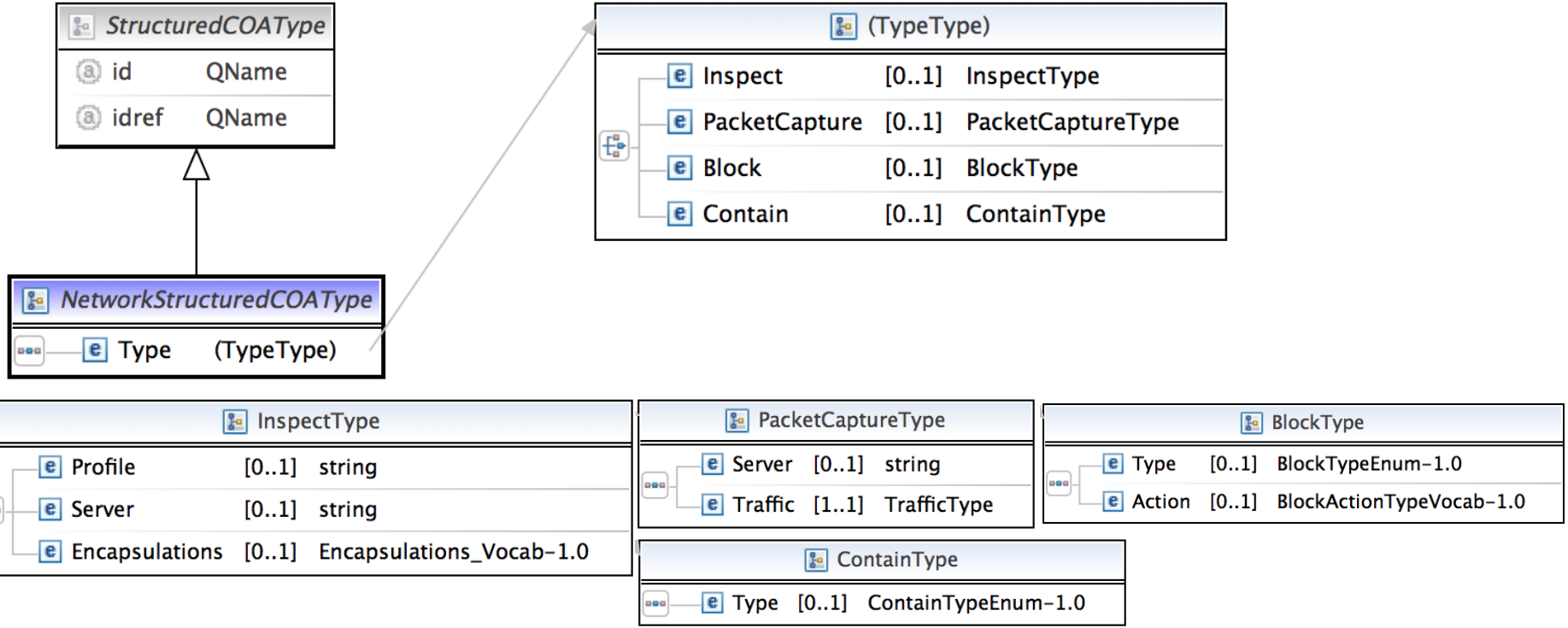
1. Expanded vocabulary with specific network action types
   - Block
   - Contain
   - Inspect
   - Packet Capture

2. Added priority for the actions

Course of Actions along the attack continuum

	BEFORE	DURING	AFTER
STIX Course Of Action	Indicator - SuggestedCOA	Incident - RequestedCOA	Incident - COATaken
Action target	Cybox Observable tied to Indicator • URL • Email addresses, subjects • Files • DNS domain names • IP addresses	1. Cybox Observable tied to Incident 2. Incident Victim • IP address • MAC address	1. Cybox Observable tied to Incident 2. Incident Victim
	External threats	Internal threats	

NetworkStructuredCOAType



BLOCK

Types:

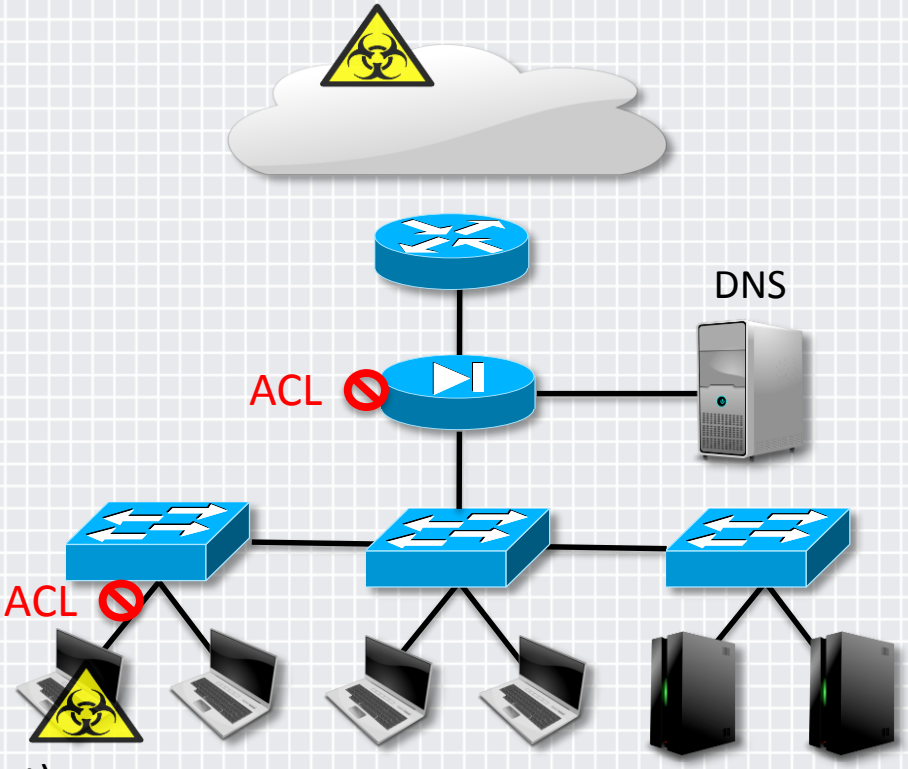
1. Perimeter block
2. Internal block

Actions:

1. Network ACL
2. BGP black-hole
3. DNS sink-hole

What is needed to apply this rule?

- Matching traffic (5 tuple)
- Action (Alert, Drop, Deny, Log, Pass, Reject)



NetworkStructuredCOAType - Block Type

BlockType

Type	[0..1]	BlockTypeEnum-1.0
Action	[0..1]	BlockActionTypeVocab-1.0

BlockTypeEnum-1.0

BlockActionTypeVocab-1.0

NetworkACL	[0..1]	BlockNetworkACL
BGPBlackhole		BlockBGPBlackhole
DNSSinkhole		BlockDNSSinkhole

BlockNetworkACL

Traffic	[1..1]	Rule_Action

BlockBGPBlackhole

Host	string

BlockDNSSinkhole

DNSSinkhole	[1..1]	string

BLOCK

Types:

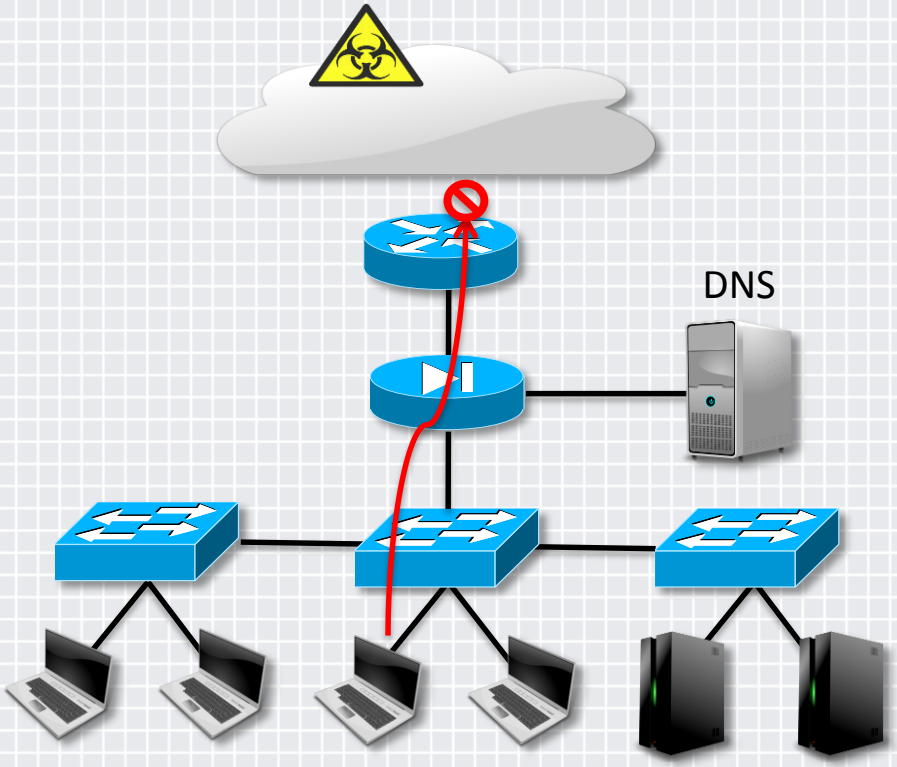
1. Perimeter block
2. Internal block

Actions:

1. Network ACL
2. BGP black-hole
3. DNS sink-hole

What is needed to apply this rule?

- Reflect router on which the static route will be applied



BLOCK

Types:

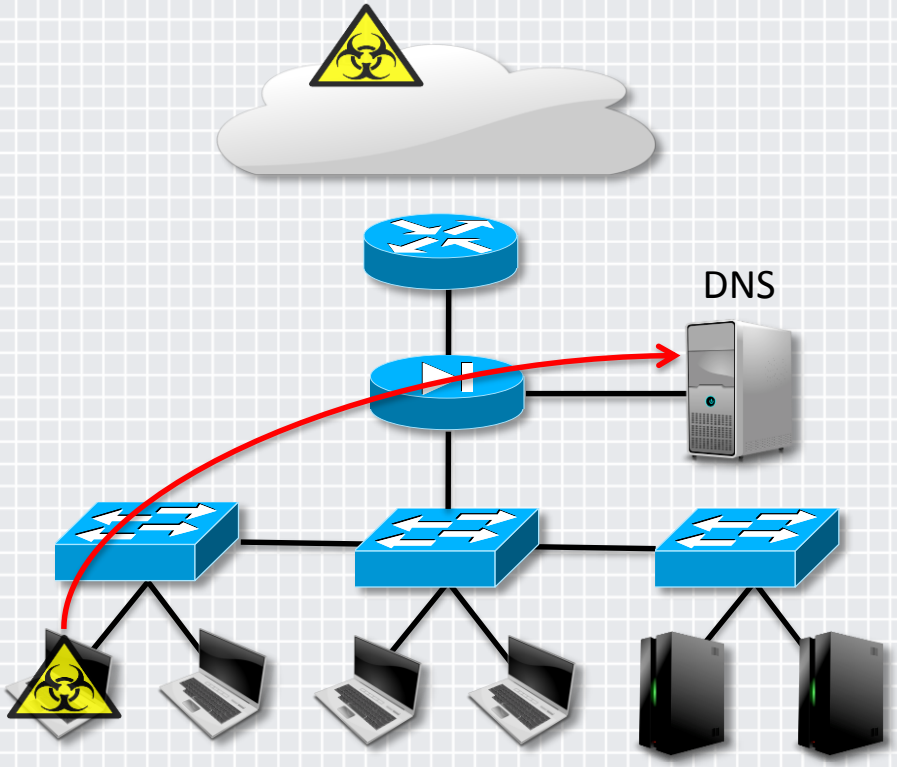
1. Perimeter block
2. Internal block

Actions:

1. Network ACL
2. BGP black-hole
3. DNS sink-hole

What is needed to apply this rule?

- Custom DNS server



CONTAIN

Remediation:

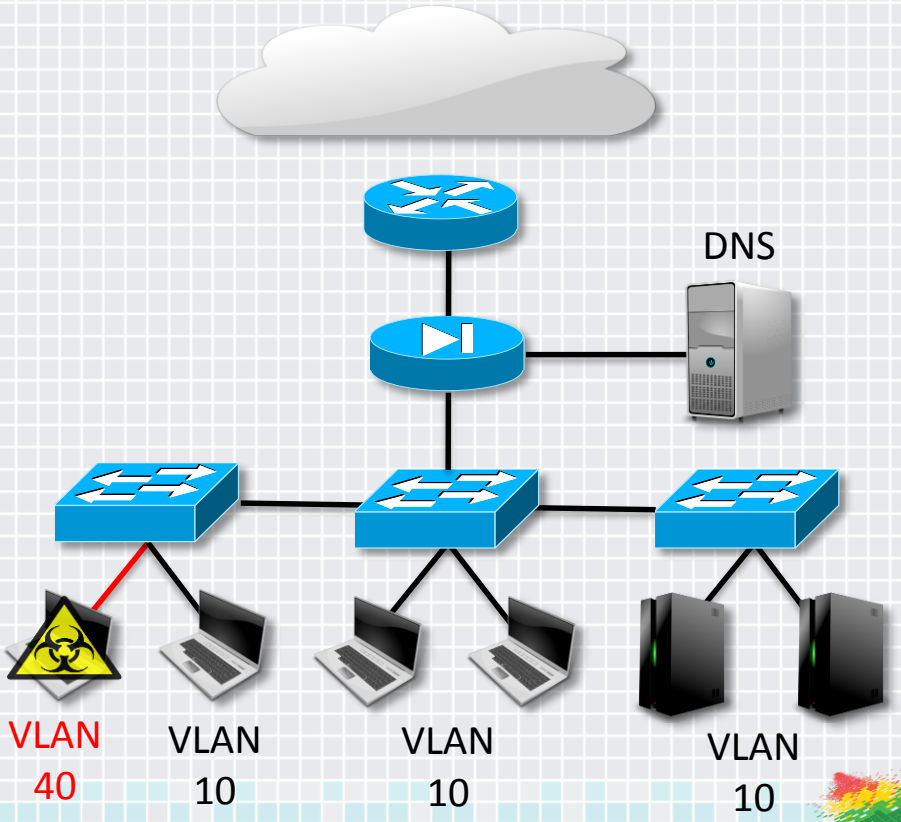
1. VLAN Containment
2. Security Group Tagging

What is needed to apply this rule?

- VLAN Profile
  VLAN Tag

Other requirements

- Network infrastructure to handle VLANs



NetworkStructuredCOAType - ContainType

ContainType

Type	[0..1]	ContainTypeEnum-1.0

ContainTypeEnum-1.0

Type	(TypeType)

(TypeType)

Remediation	[0..1]	Remediation
NonSensitive	[0..1]	NonSensitive
Honeypot	[0..1]	HoneyPot

Remediation

Server	[0..1]	string
ContainmentProfile		RemediationContainmentProfile
Traffic	[1..1]	Rule_Action

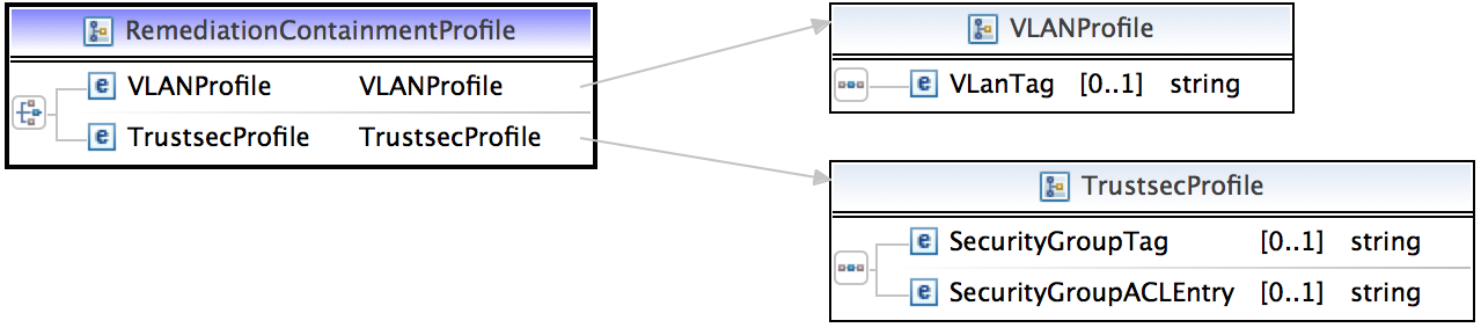
NonSensitive

PermissibleIps	[0..1]	IPAddressList
Traffic	[0..1]	TrafficType

HoneyPot

PermissibleIps	[0..1]	IPAddressList
Traffic	[1..1]	TrafficType
Routes	[0..1]	Routes

ContainType - Remediation



CONTAIN

Remediation:

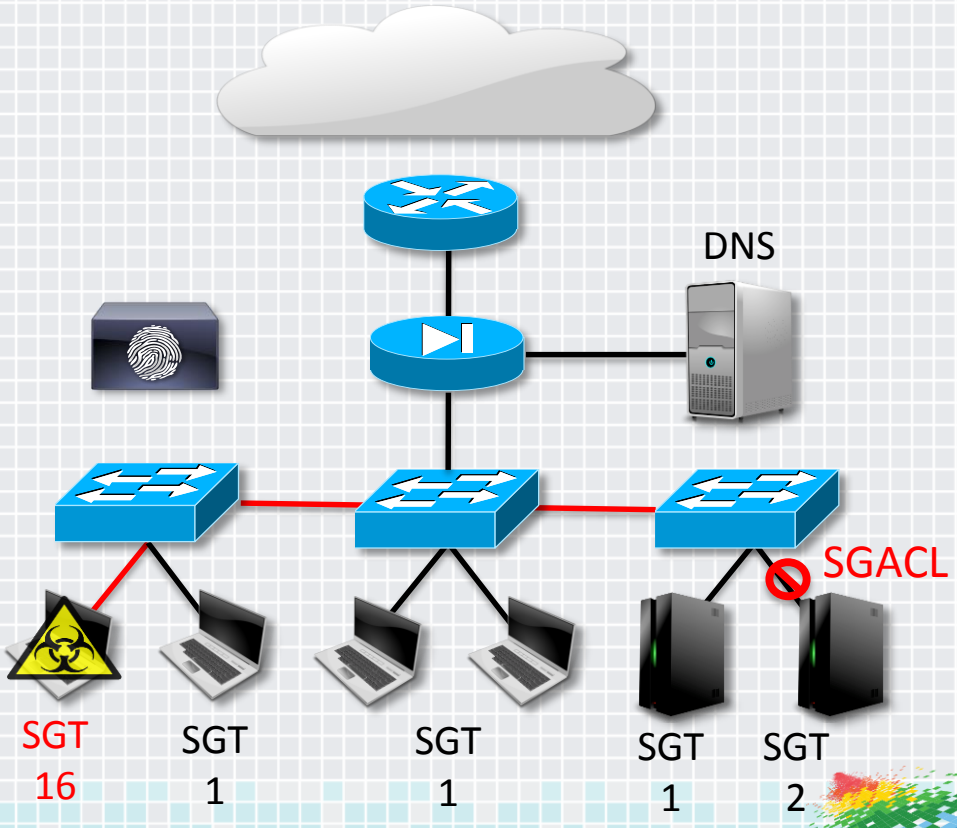
1. VLAN Containment
2. Security Group Tagging

What is needed to apply
This rule?

- Security Group Profile
  - Security Group Tag
  - Security Group ACL

Other requirements

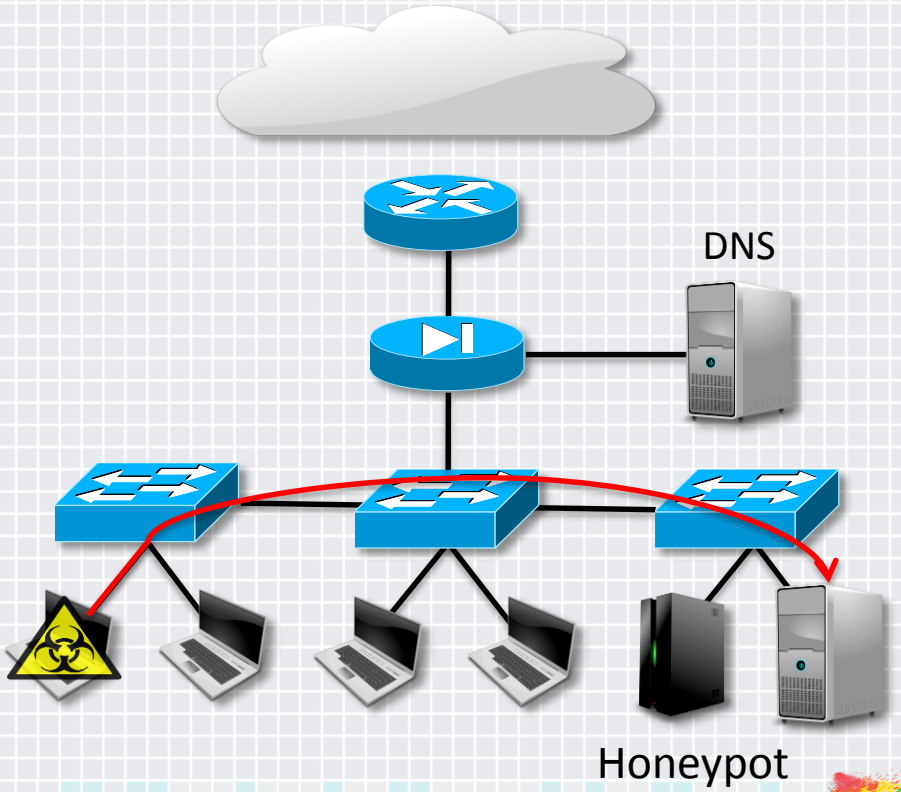
- Security Group Policy enforcer
- Network devices that can handle tags



CONTAINMENT TO HONEYNET

What is needed to apply this rule?

- Permissible IP list
- Traffic description (5 tuple)
  - Source port, Destination port, Source IP, Destination IP, Protocol
- Routes
  - Prefix, next hop, next hop type



ContainType - HoneyPot

HoneyPot

PermissibleIps	[0..1]	IPAddressList
Traffic	[1..1]	TrafficType
Routes	[0..1]	Routes

IPAddressList

TrafficType

id		QName
Protocol	[0..1]	TrafficTypeProtocol-1.0
SourceAddress	[0..1]	string
SourcePort	[0..1]	string
DestinationAddress	[0..1]	string
DestinationPort	[0..1]	string

TCP, UDP, ICMP, ANY

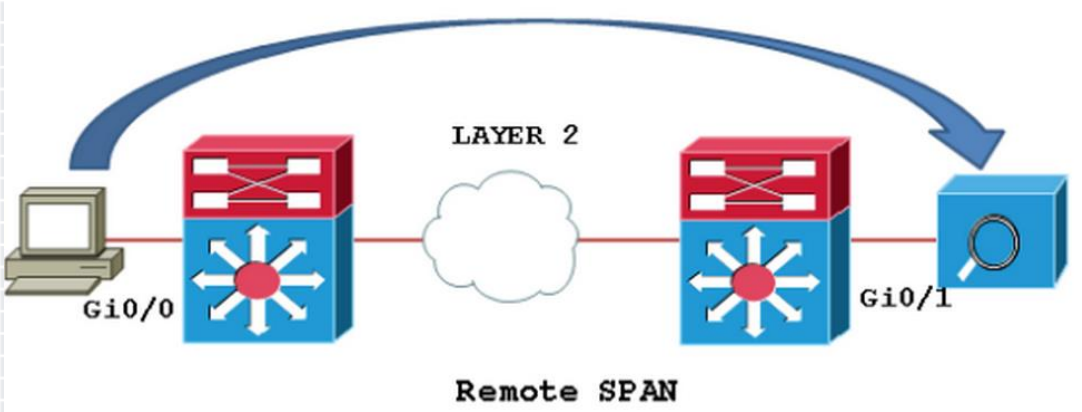
Routes

prefix	[0..1]	string
NextHop	[0..1]	string
NextHopType	[0..1]	string

INSPECTION ON DEMAND

What is needed to achieve this?

- Inspection profile
- Inspection Server
- Encapsulations – GRE, VXLAN etc.



NetworkStructuredCOAType - InspectType

InspectType		
Profile	[0..1]	string
Server	[0..1]	string
Encapsulations	[0..1]	Encapsulations_Vocab-1.0

GRE, VXLAN

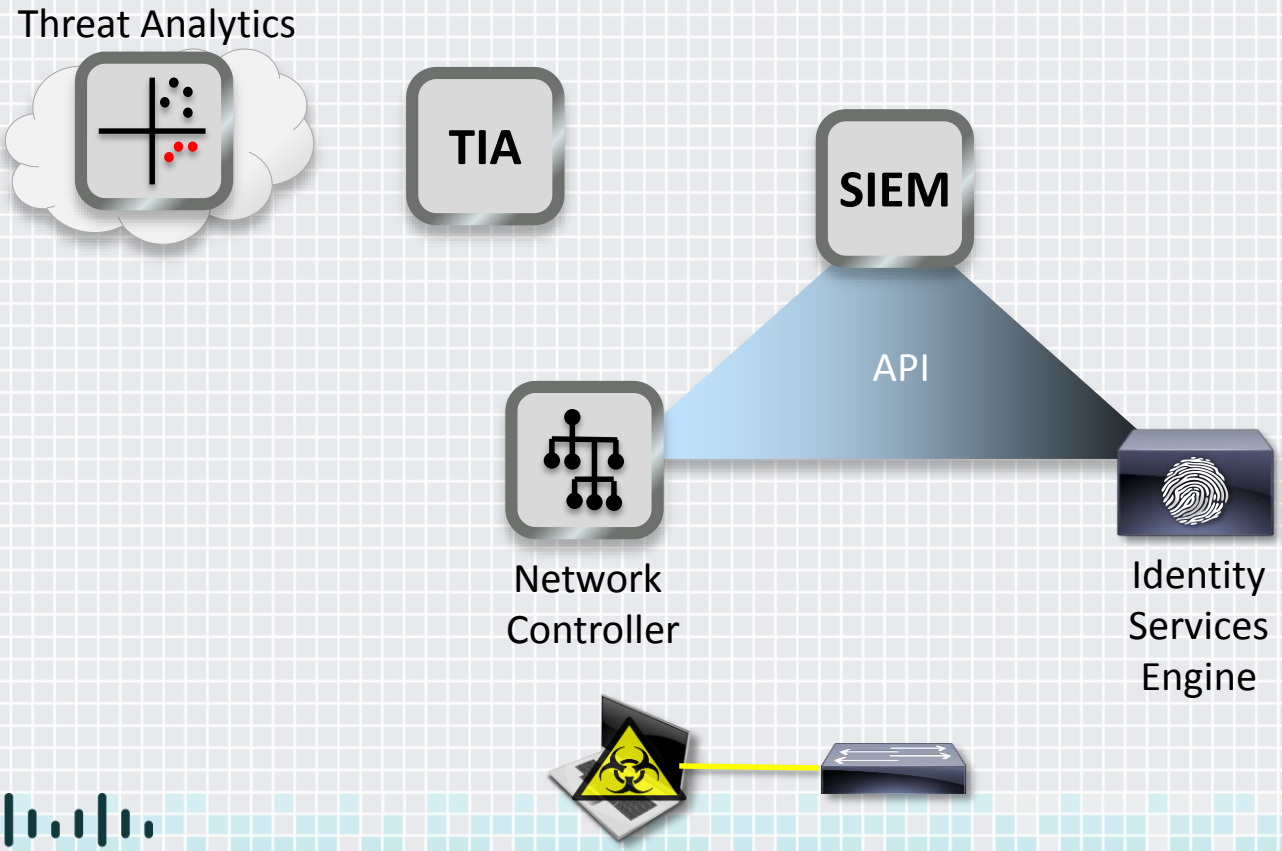
PacketCaptureType

PacketCaptureType		
Server	[0..1]	string
Traffic	[1..1]	TrafficType

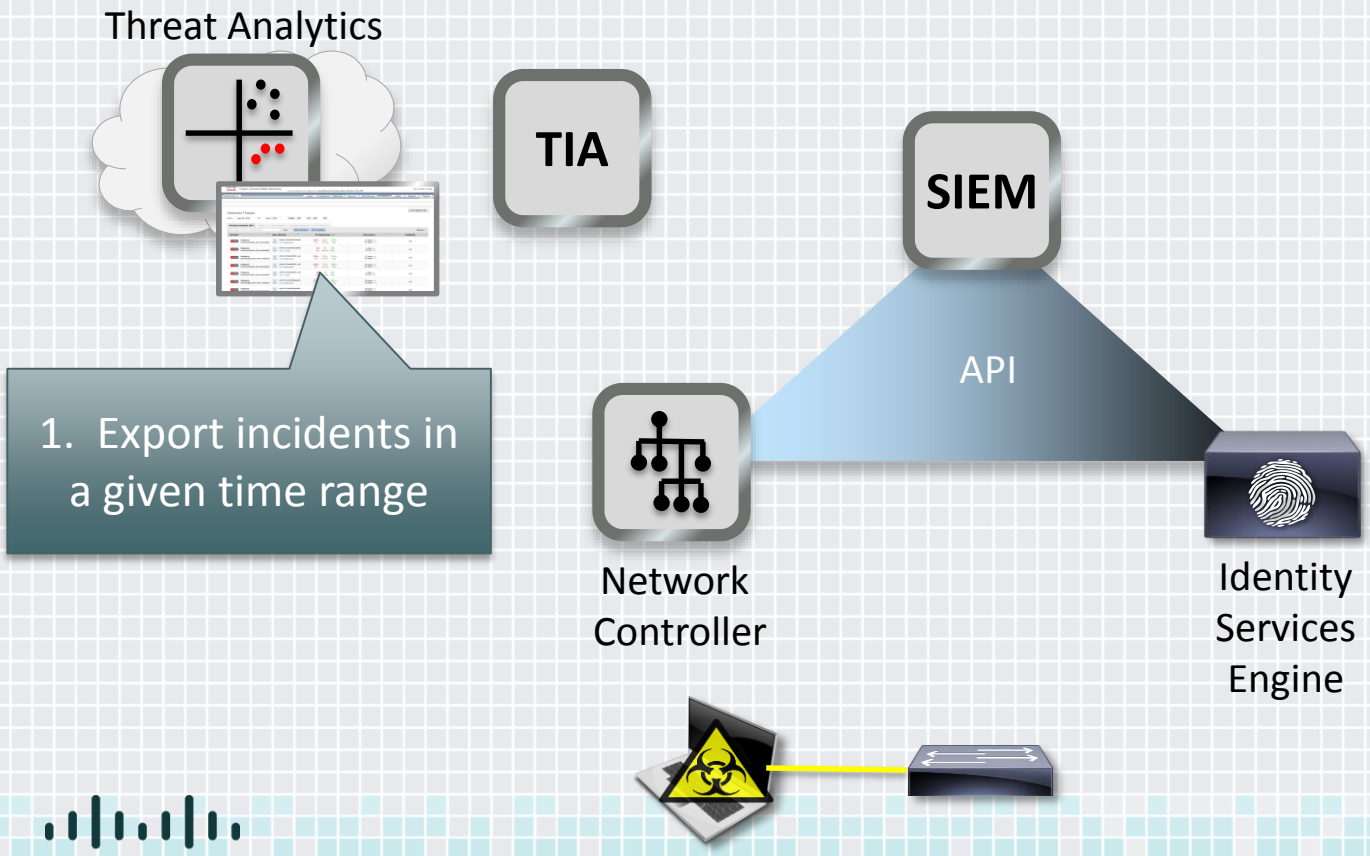
TrafficType		
id		QName
Protocol	[0..1]	TrafficTypeProtocol-1.0
SourceAddress	[0..1]	string
SourcePort	[0..1]	string
DestinationAddress	[0..1]	string
DestinationPort	[0..1]	string

TCP, UDP, ICMP, ANY

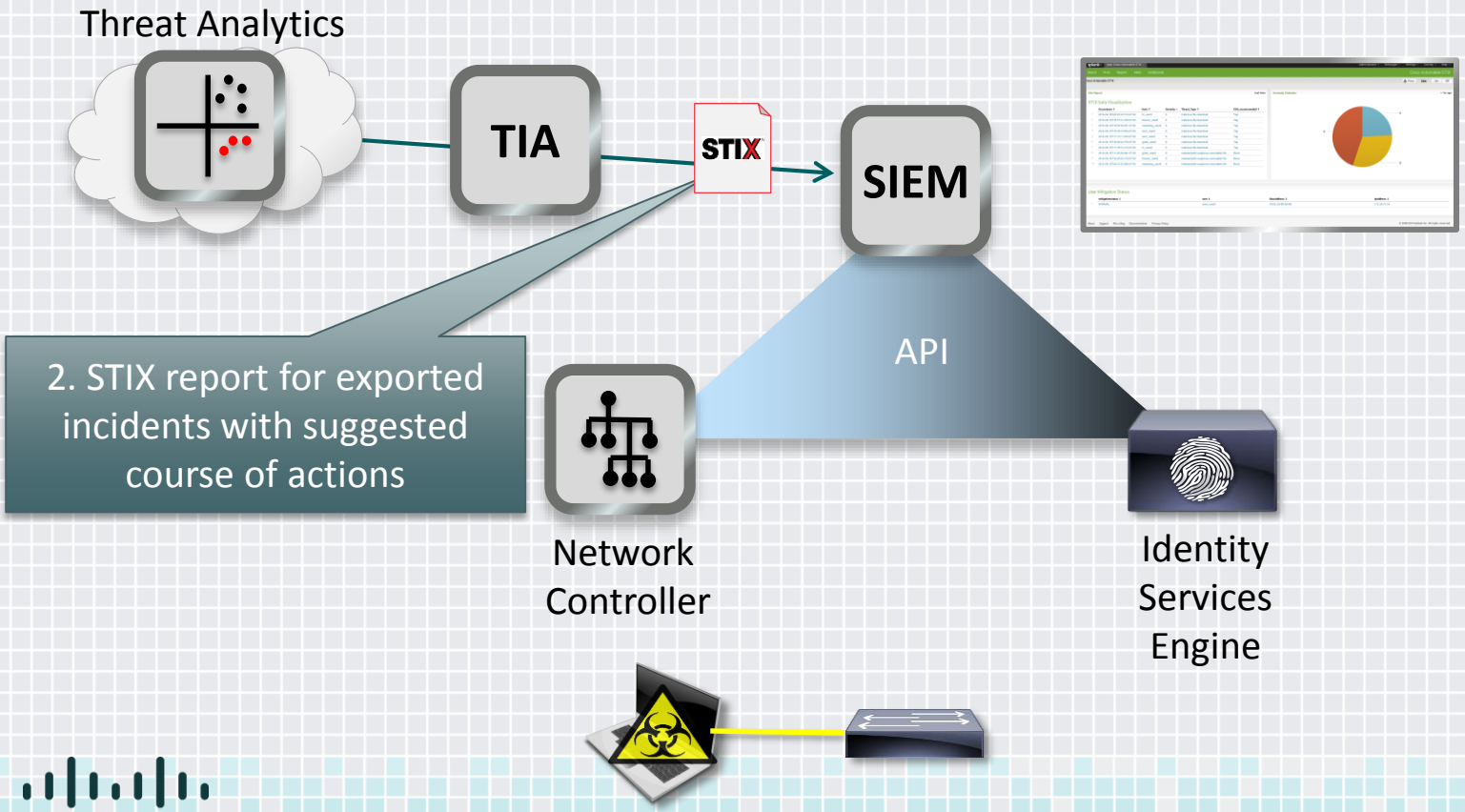
Workflow



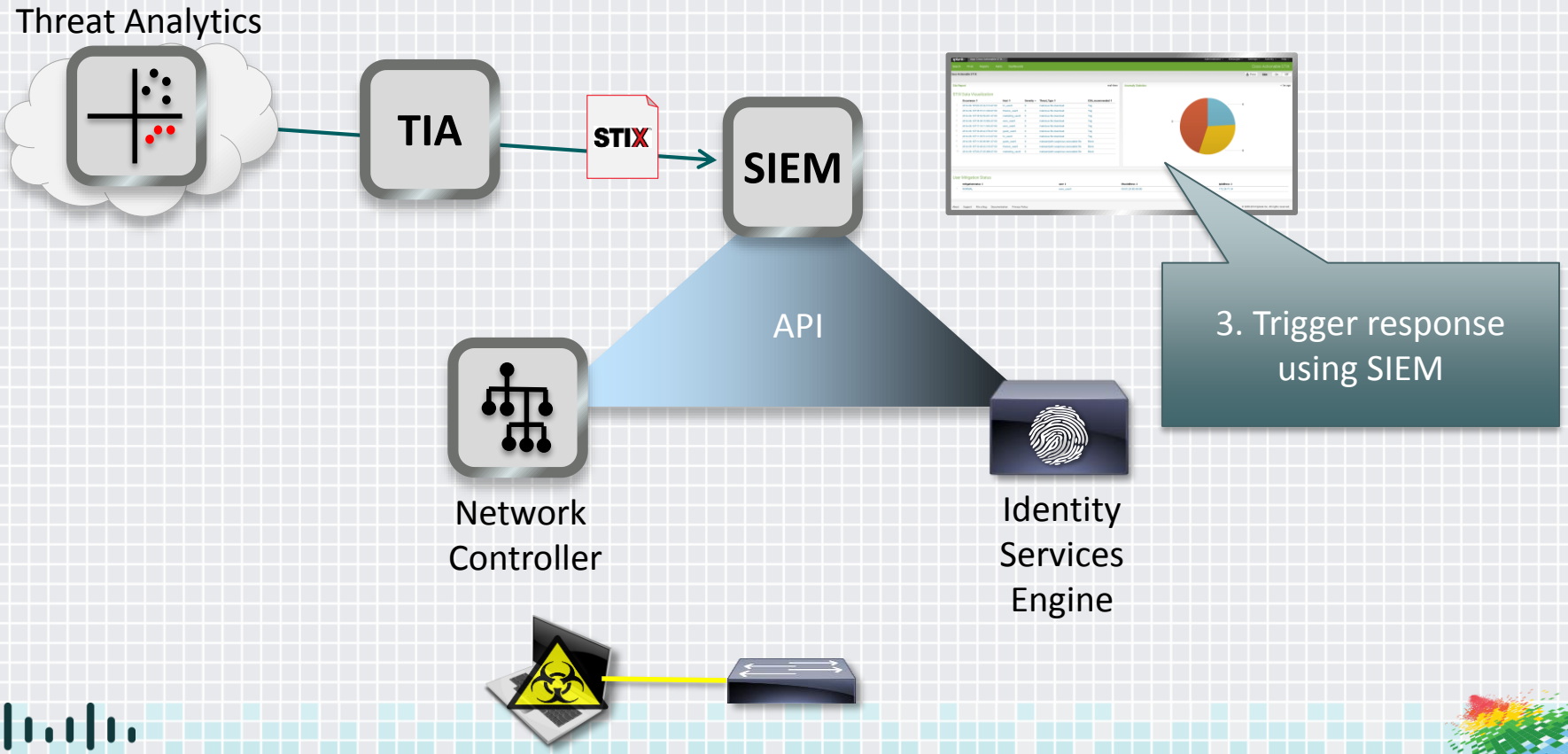
Workflow



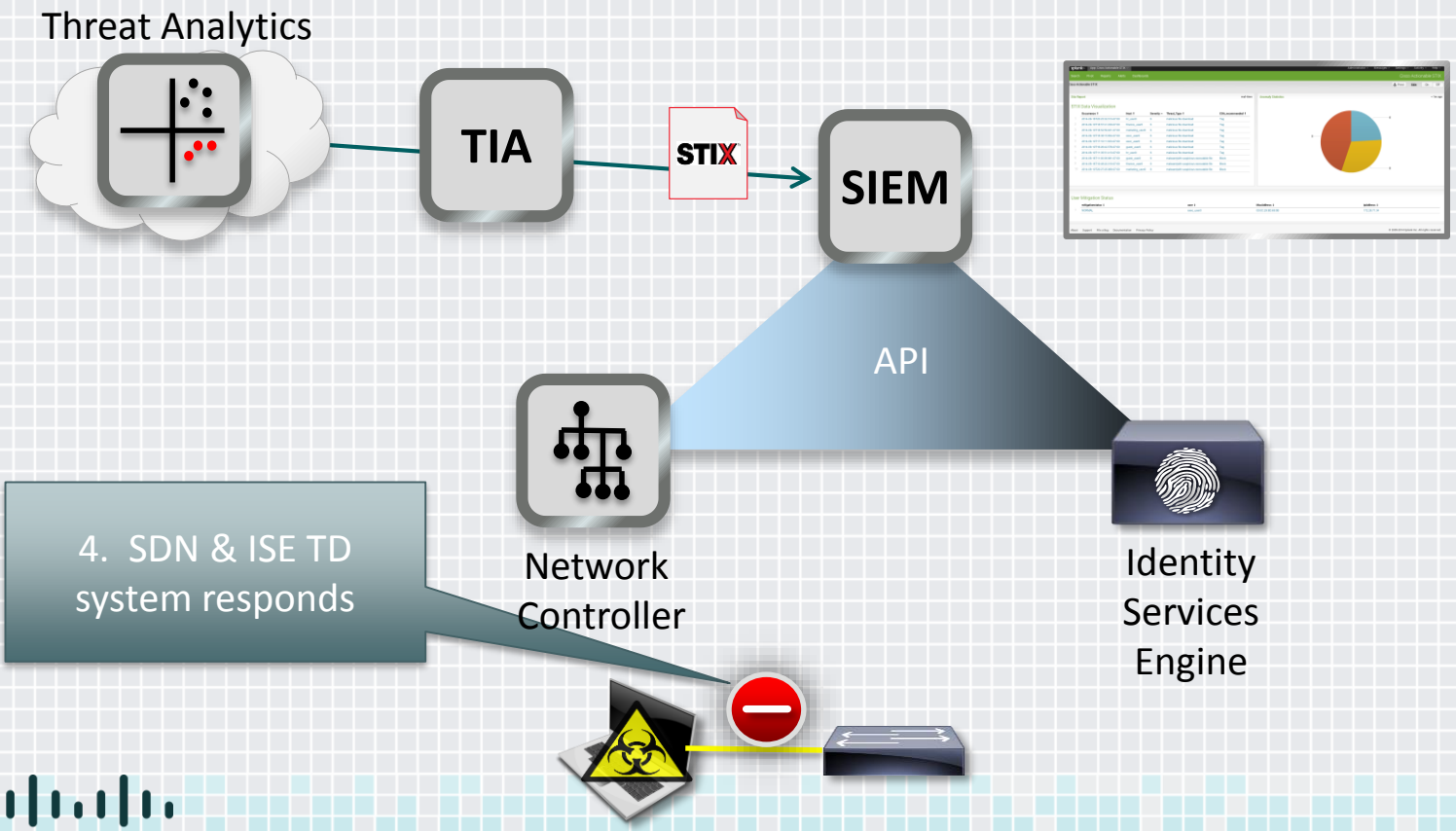
Workflow



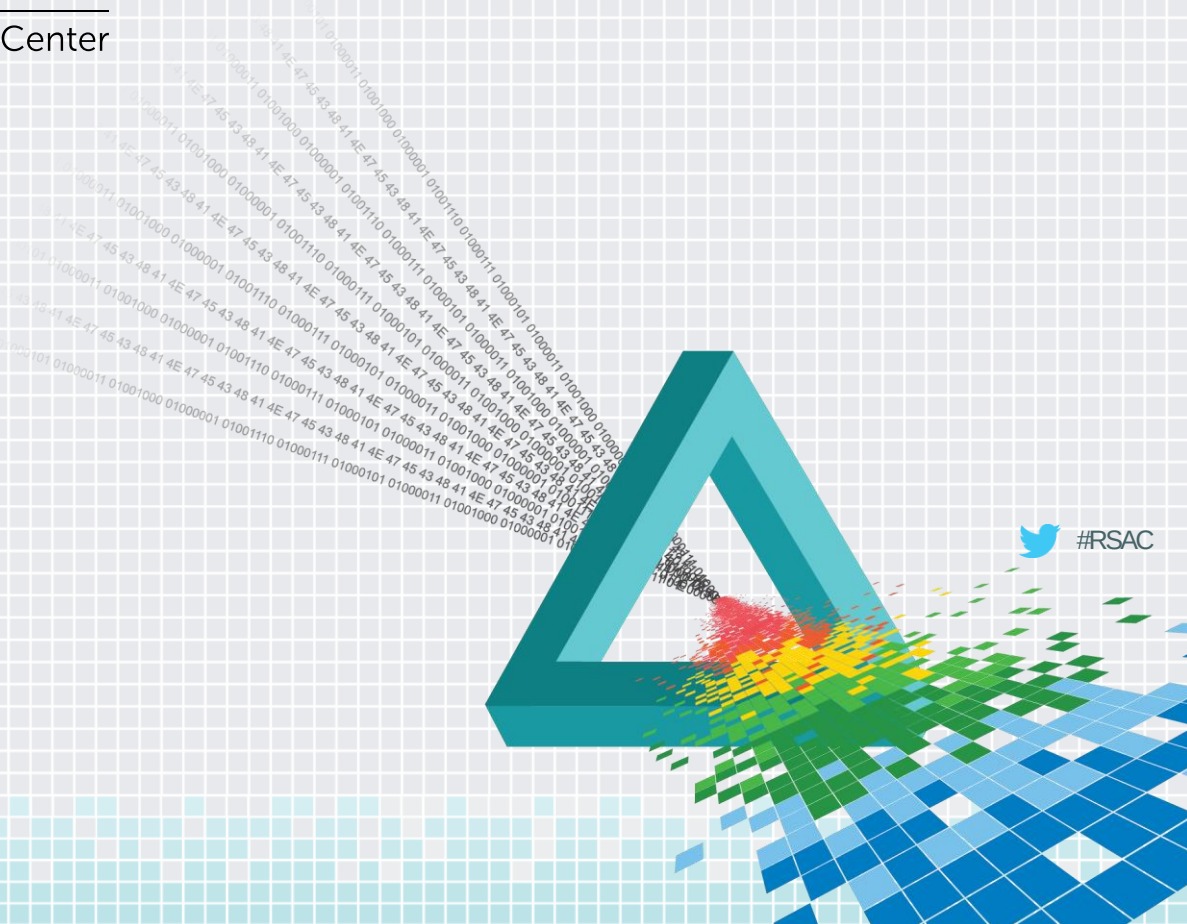
Workflow



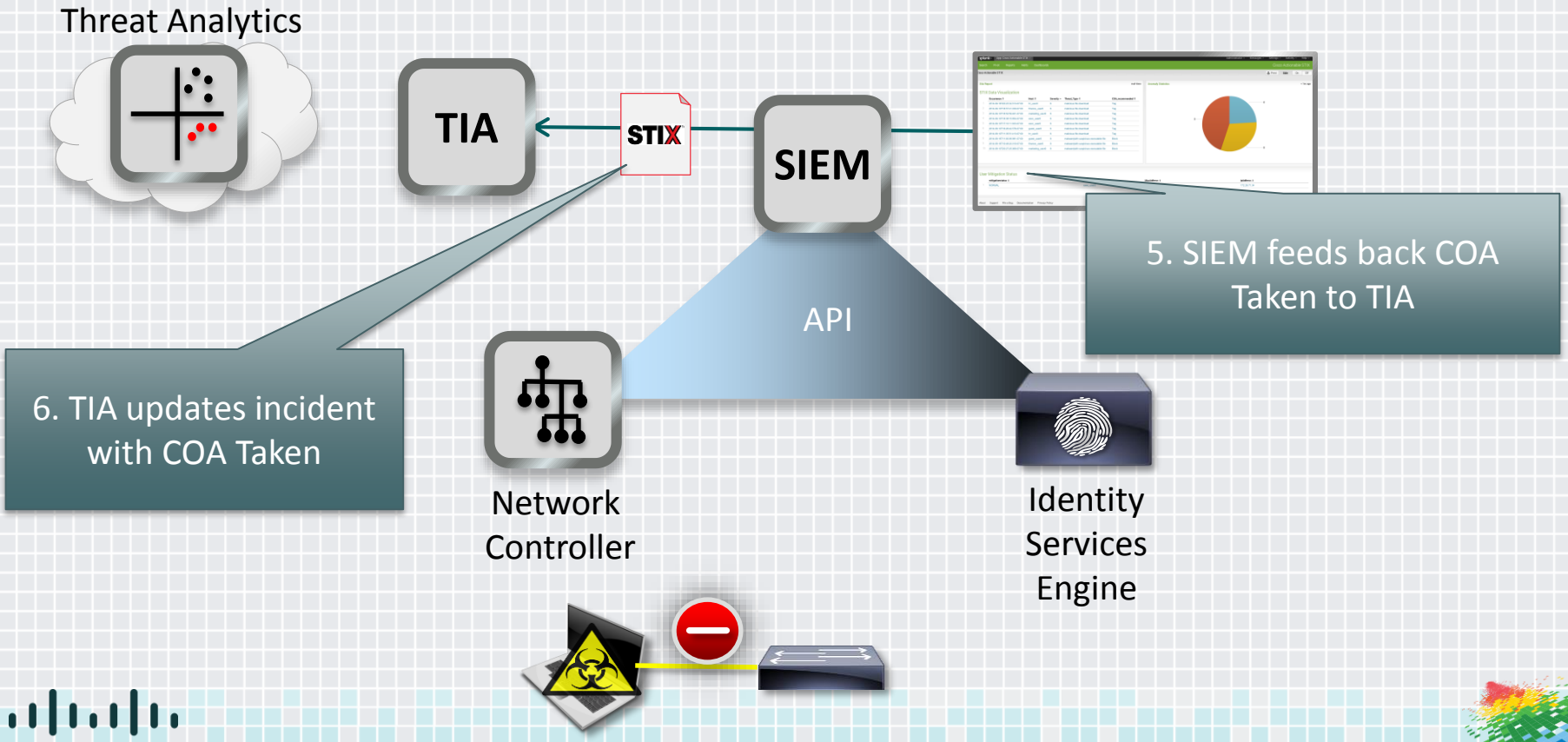
Workflow



Demonstration



Future work



Summary

- STIX can be used to recommend actionable responses
- Machine readable: actionable
- NetworkStructuredCOA used for investigation, mitigation, and remediation

Apply what you have learned

- In the next week
  - Identify detection and response systems within your organization that could use an actionable CoA
  - Determine if those elements are using STIX
- Over the next three months
  - Provide feedback to the STIX community
  - Experiment with STIX CoA definition and software

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thanks for your attention

#RSAC

STIX extensions

```
<xs:complexType name="NetworkStructuredCOAType" abstract="true”>
  <xs:extension base="coa:StructuredCOAType">
    <xs:choice>
      <xs:element name="Inspect" type="network_coa:InspectType" minOccurs="0"/>
      <xs:element name="PacketCapture" type="network_coa:PacketCaptureType" minOccurs="0"/>
      <xs:element name="Block" type="network_coa:BlockType" minOccurs="0"/>
      <xs:element name="Contain" type="network_coa:ContainType" minOccurs="0"/>
    </xs:choice>
  </xs:extension>
</xs:complexType>
```