

SESSION ID: ANF-R04

Making Threat Intelligence Actionable: Recommending Responses with STIX

David McGrew

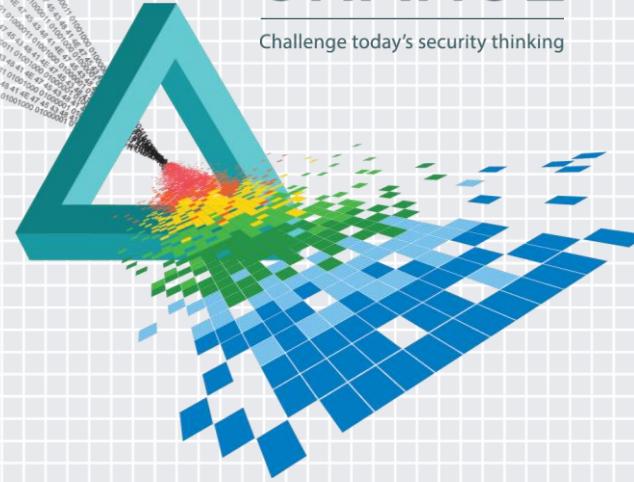
Fellow
Cisco Systems
@mcgrewAnalog

Jyoti Verma

Technical Leader
Cisco Systems

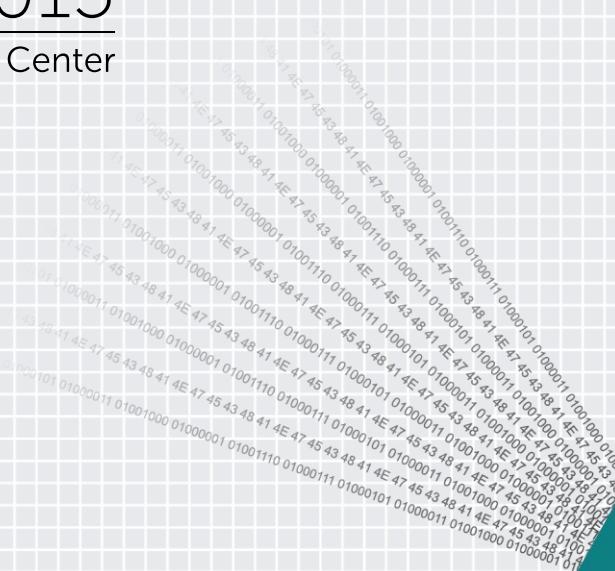
CHANGE

Challenge today's security thinking



RSA® Conference 2015

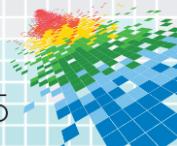
San Francisco | April 20-24 | Moscone Center



Introduction

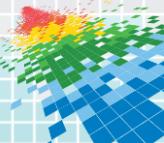


Security process cycle



Poll

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



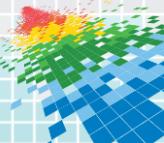
Response

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



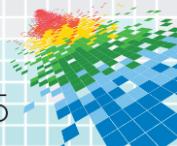
Poll

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



Connecting analytics 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

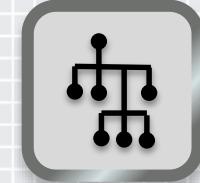
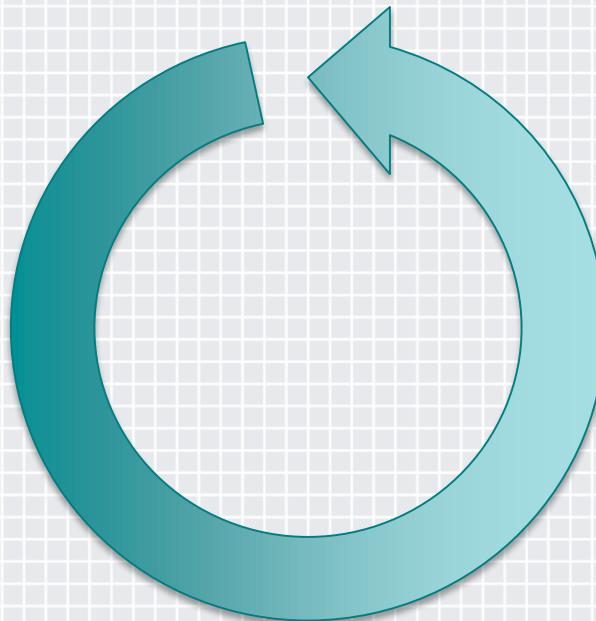


Connecting detection to response

Cloud Threat Analytics



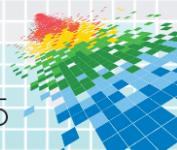
Local Threat Analytics



Network Controller



Endpoint Protection

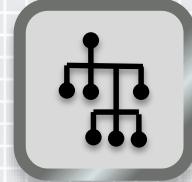


Threat Intelligence Aggregator

Cloud Threat Analytics



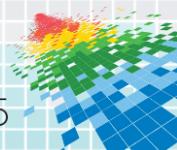
Local Threat Analytics



Network Controller

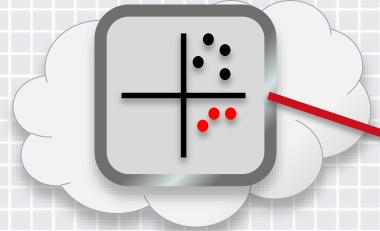


Endpoint Protection



Threat Intelligence Aggregator

Cloud Threat Analytics



TI

TIA

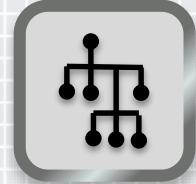
STIX™

SIEM

Local Threat Analytics



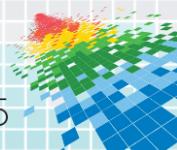
STIX™



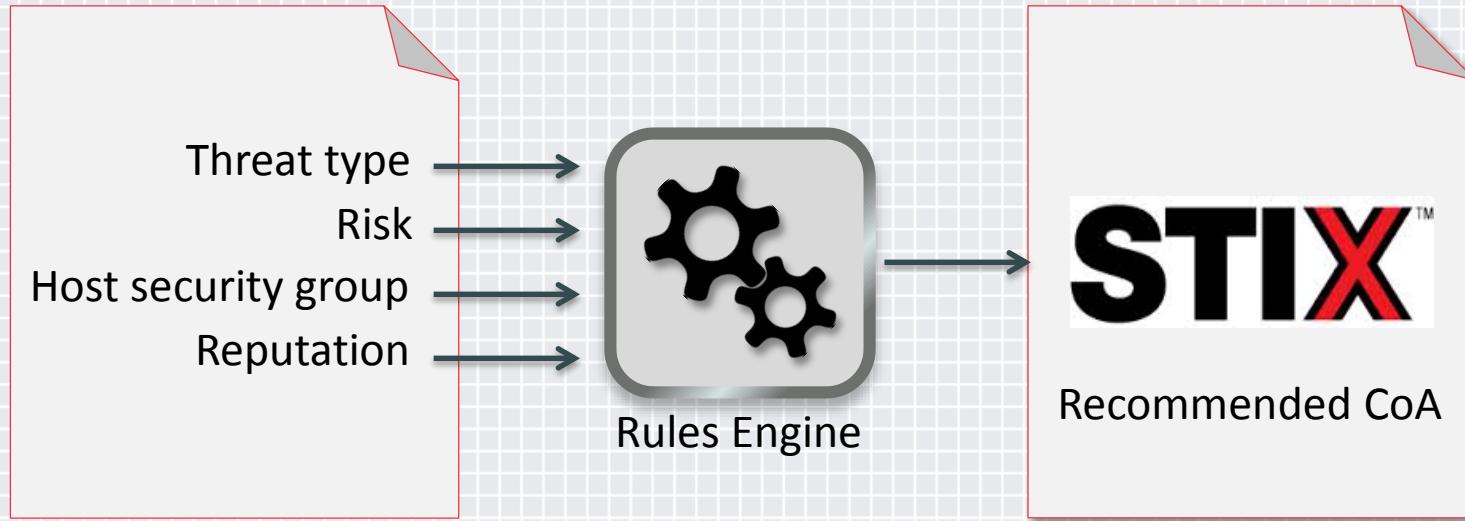
Network Controller



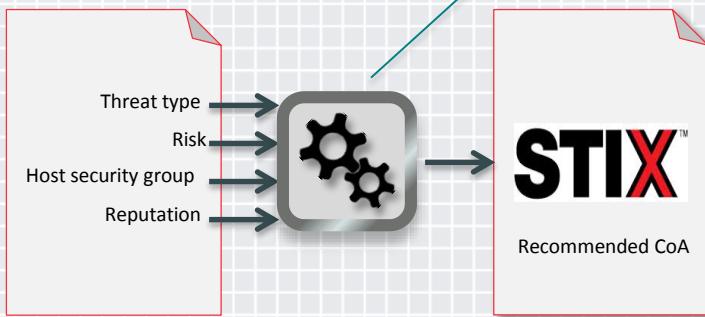
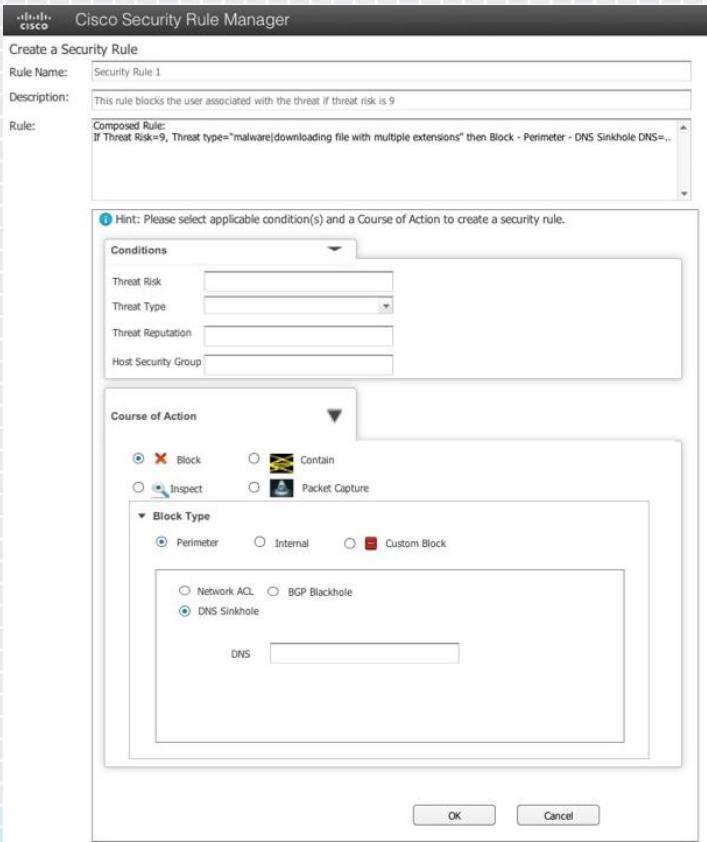
Endpoint Protection



Threat Intelligence Aggregator



Threat Intelligence Aggregator

Screenshot of the Cisco Security Rule Manager interface, showing a "Create a Security Rule" dialog:

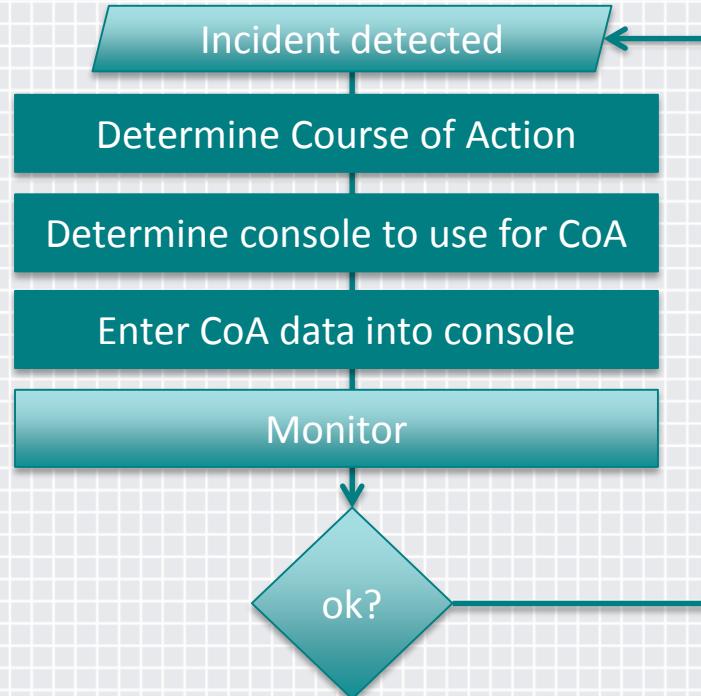
- Rule Name:** Security Rule 1
- Description:** This rule blocks the user associated with the threat if threat risk is 9
- Rule:** Composed Rule:
If Threat Risk=9, Threat type="malware|downloading file with multiple extensions" then Block - Perimeter - DNS Sinkhole DNS=..
- Hint:** Please select applicable condition(s) and a Course of Action to create a security rule.
- Conditions:**
 - Threat Risk
 - Threat Type
 - Threat Reputation
 - Host Security Group
- Course of Action:**
 - Block
 - Contain
 - Inspect
 - Packet Capture
- Block Type:**
 - Perimeter
 - Internal
 - Custom Block
- DNS:**

Rules

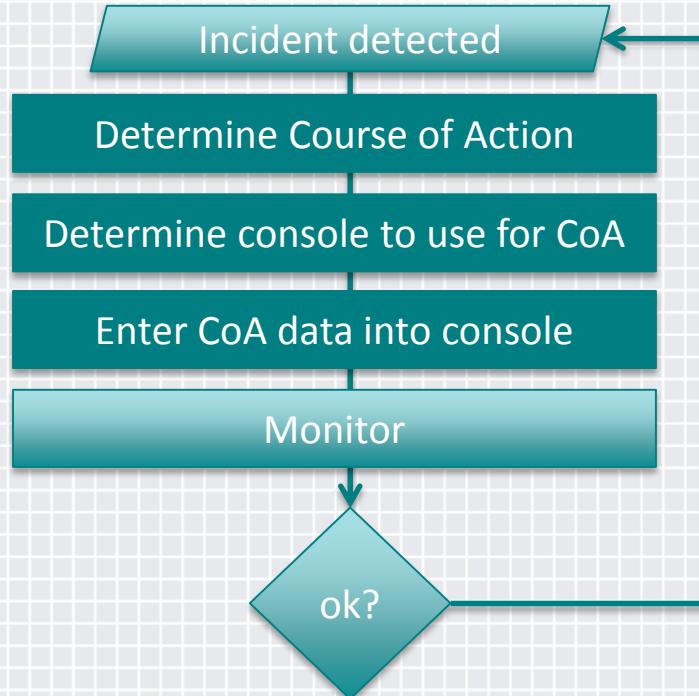
Risk	Threat Type	Default Suggested Course of Action
8-9	malware using automatically generated domain (DGA)	Block compromised host
8-9	malware using url-string as communication channel (C&C)	Block compromised host
8-9	malware using https communication channel	Block compromised host
8-9	malware downloading suspicious file	Block compromised host
7-8	malware using repetitive requests	Quarantine compromised host
7	malware downloading malicious file	Quarantine 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



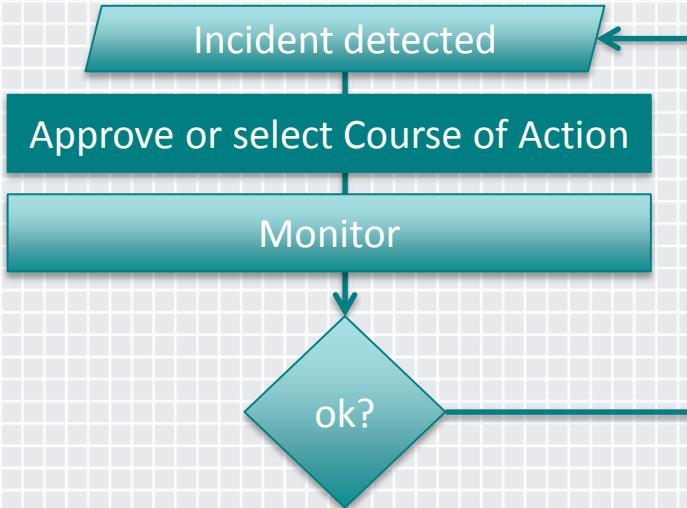
Manual



Manual

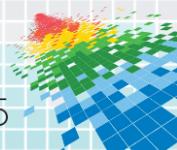


Semiautomated



Network actions

- ◆ Investigate
 - ◆ Inspect with IPS: SPAN, TAP, SDN copying or redirection
 - ◆ Netflow/IPFIX monitoring
- ◆ 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



Poll

- ◆ What response mechanisms do you use?





Poll

What is STIX?

- ◆ Structured Threat Information eXchange
- ◆ Structured Threat Information eXpression
- ◆ Some Think In XML



What is STIX?



Incident



Tactics, Techniques, Procedures



Indicator



Campaign



Observable



Exploit Target



Course of Action



Threat Actor

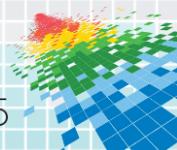
Why use STIX between detection & response?

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



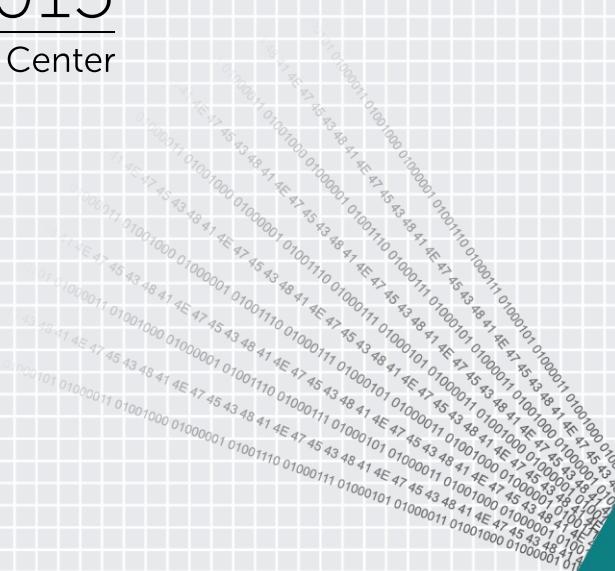
Pros and Cons of STIX

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	



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

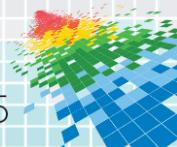


STIX Extensions

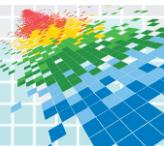
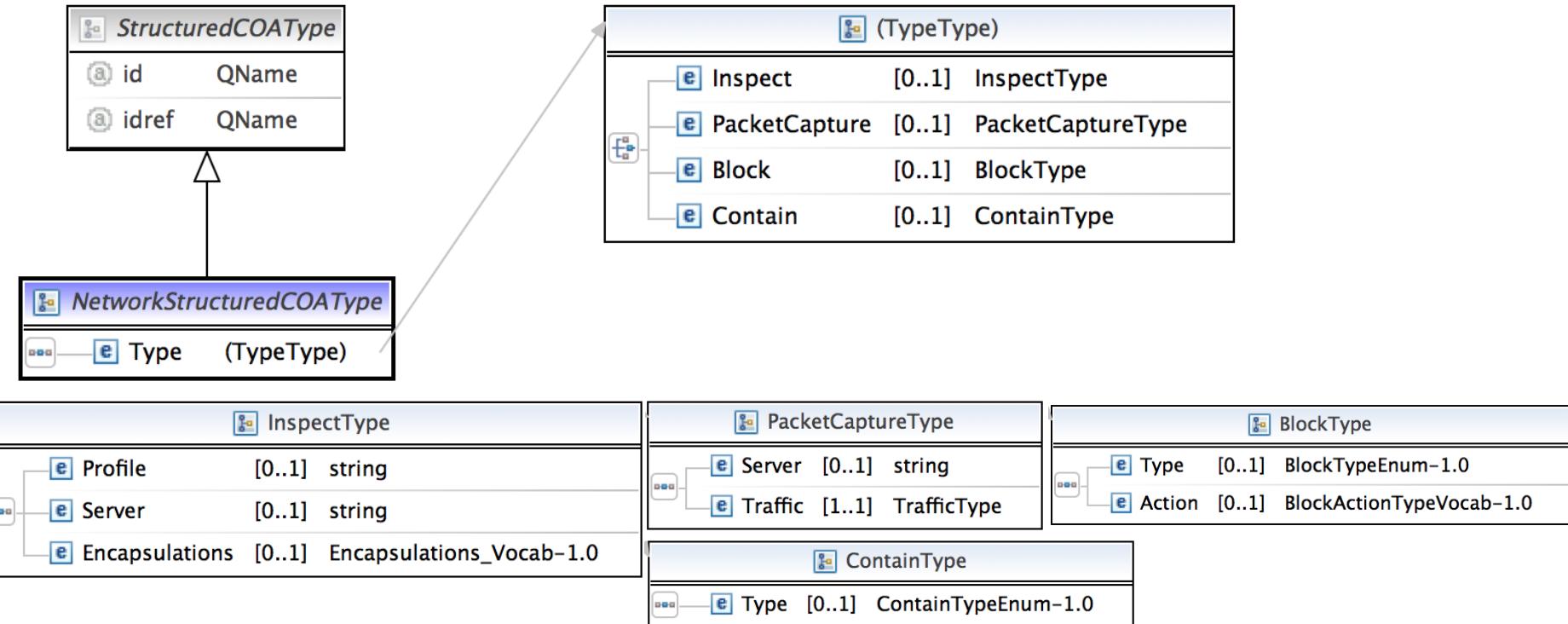


Extending CourseOfActionType

1. Expanded vocabulary with specific network action types
 - Block
 - Contain
 - Inspect
 - Packet Capture
2. Added priority for the actions



NetworkStructuredCOAType



BLOCK

Types:

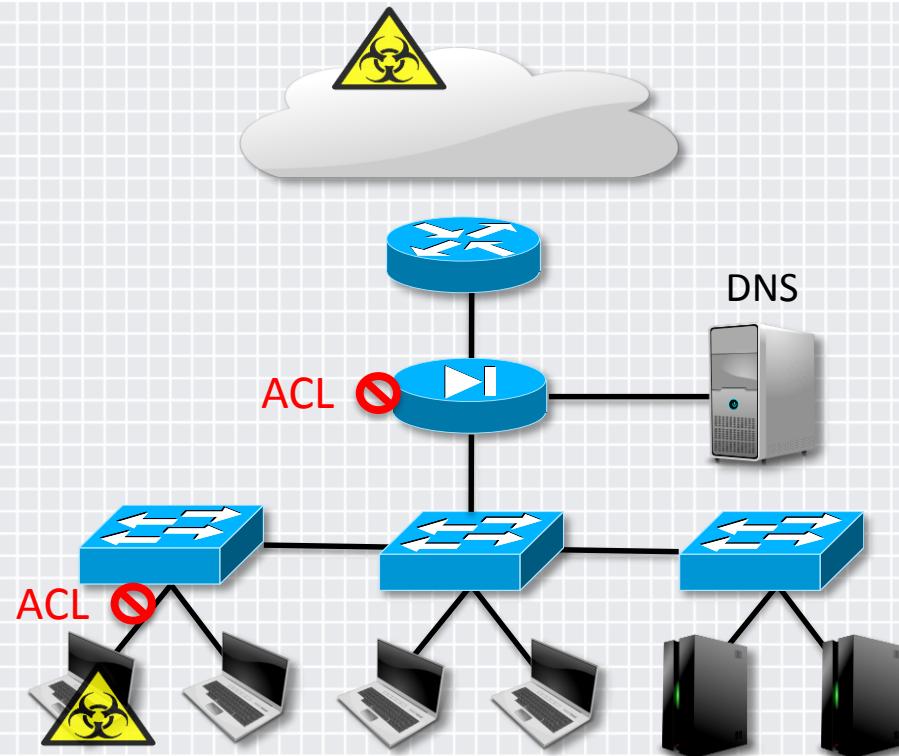
1. Perimeter block
2. Internal block

Actions:

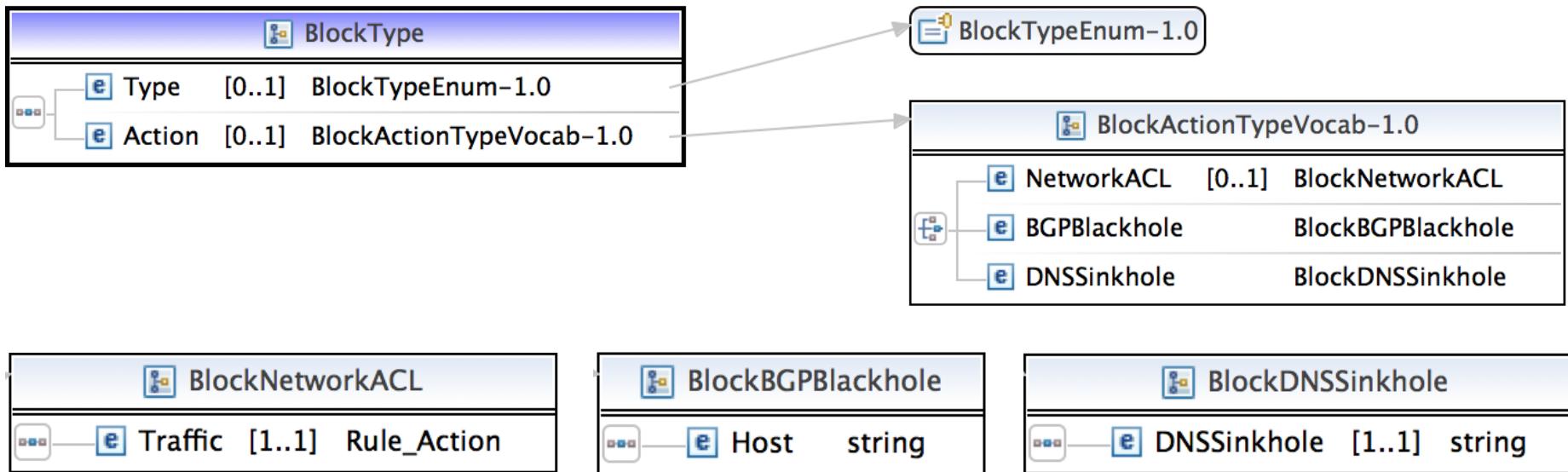
1. Network ACL
2. BGP black-hole
3. DNS sink-hole

What is needed to apply this rule?

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



NetworkStructuredCOAType - Block Type



BLOCK

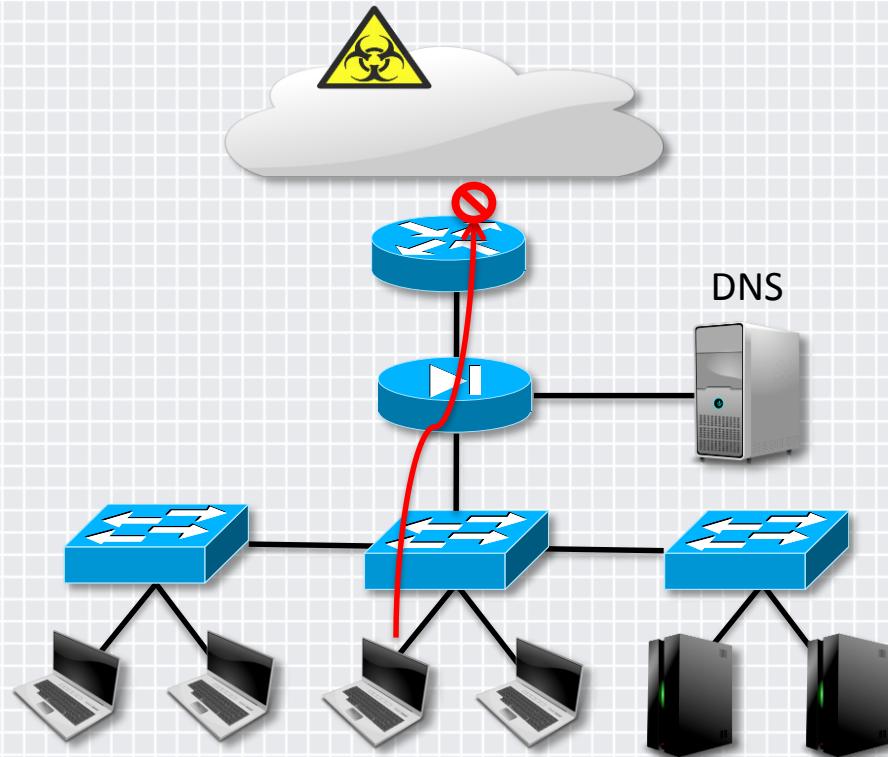
Types:

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:

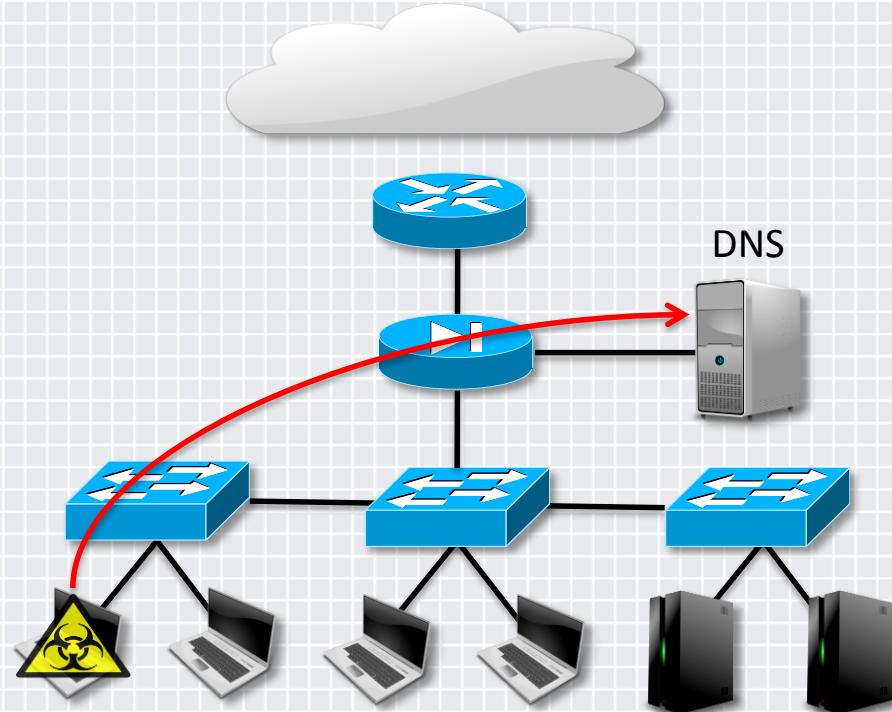
1. Perimeter block
2. Internal block

Actions:

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

What is needed to apply this rule?

- Custom DNS server



CONTAIN

Remediation:

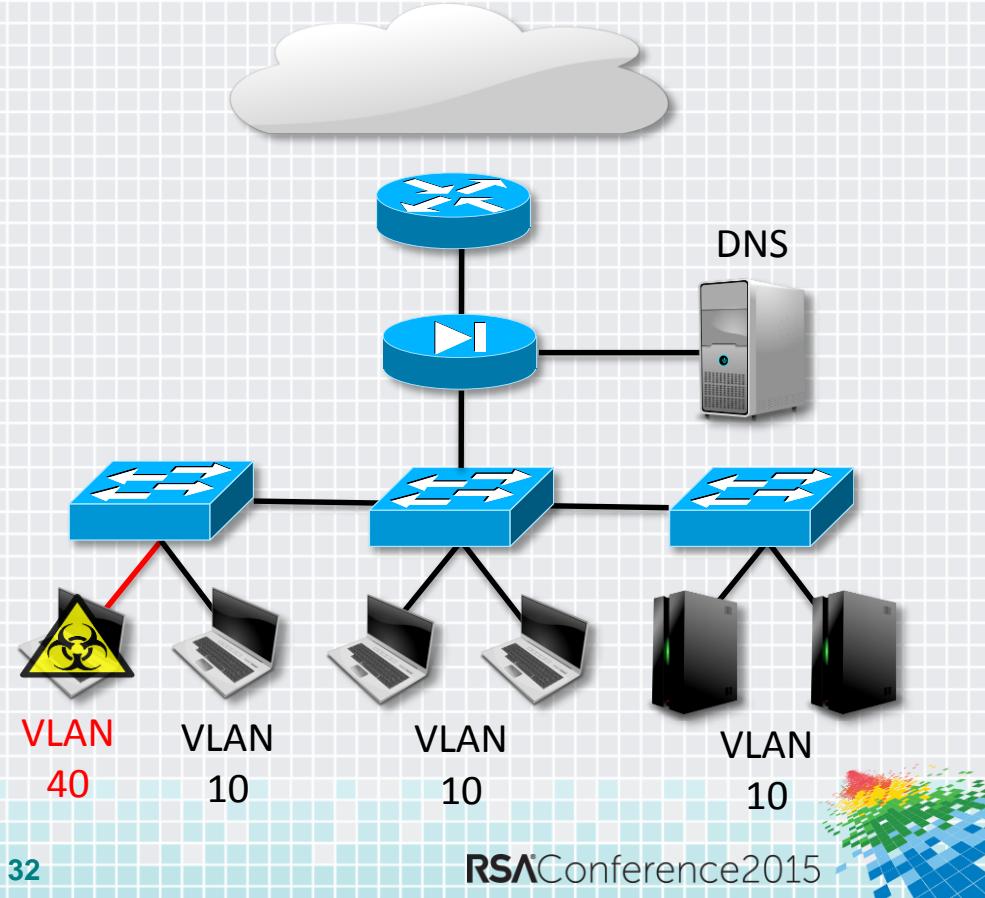
1. VLAN Containment
2. Security Group Tagging

What is needed to apply this rule?

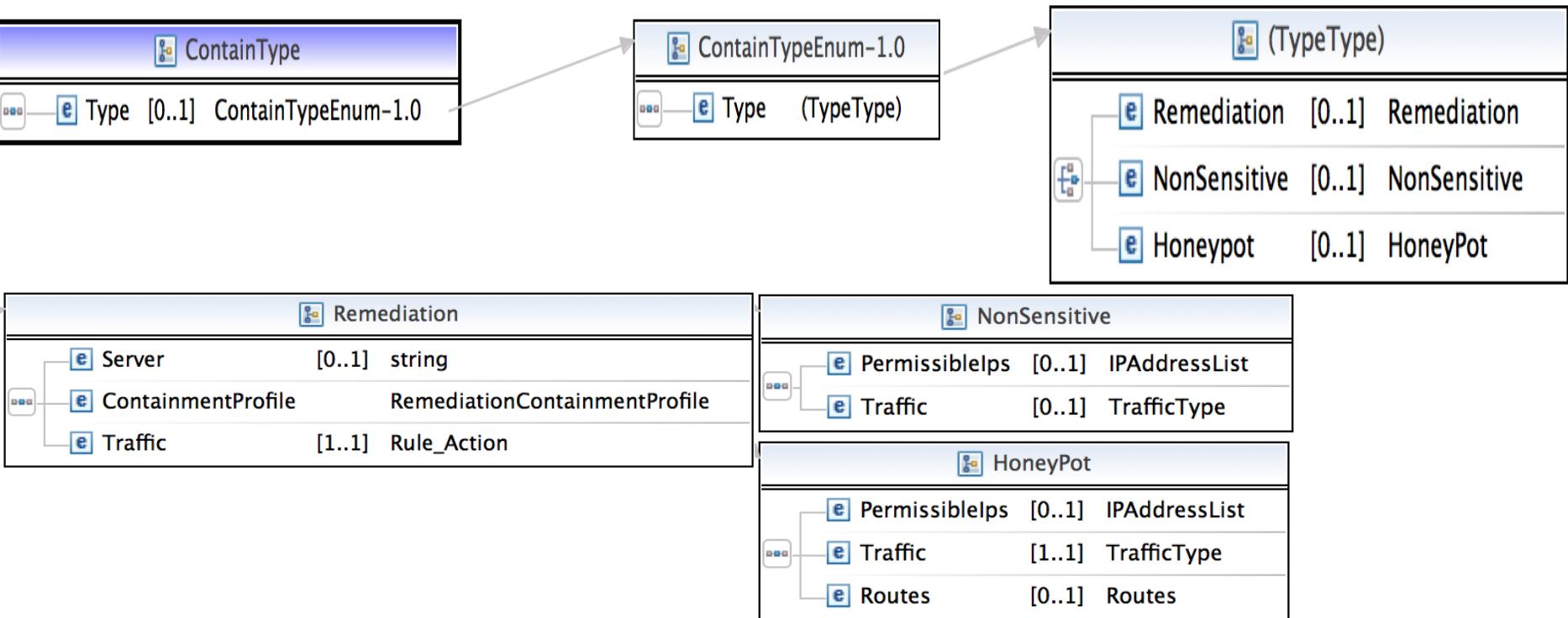
- VLAN Profile
- VLAN Tag

Other requirements

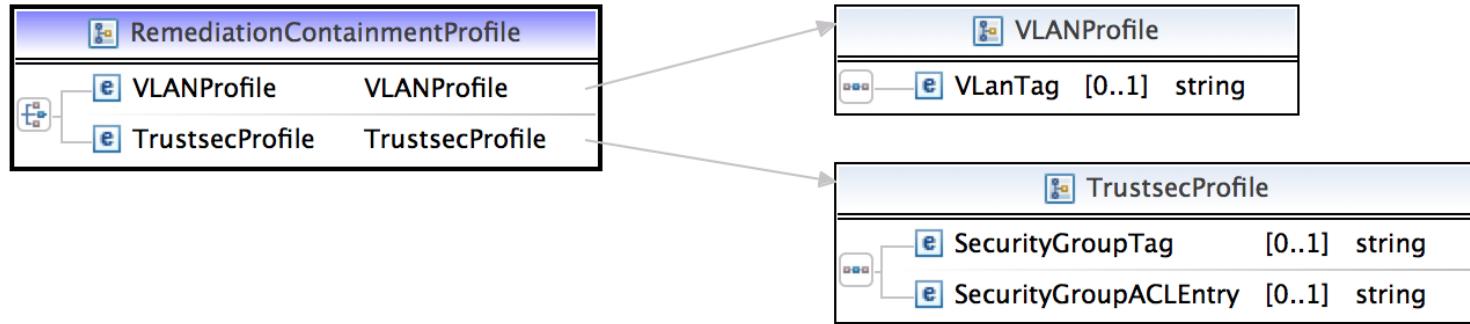
- Network infrastructure to handle VLANs



NetworkStructuredCOAType - ContainType



ContainType - Remediation



CONTAIN

Remediation:

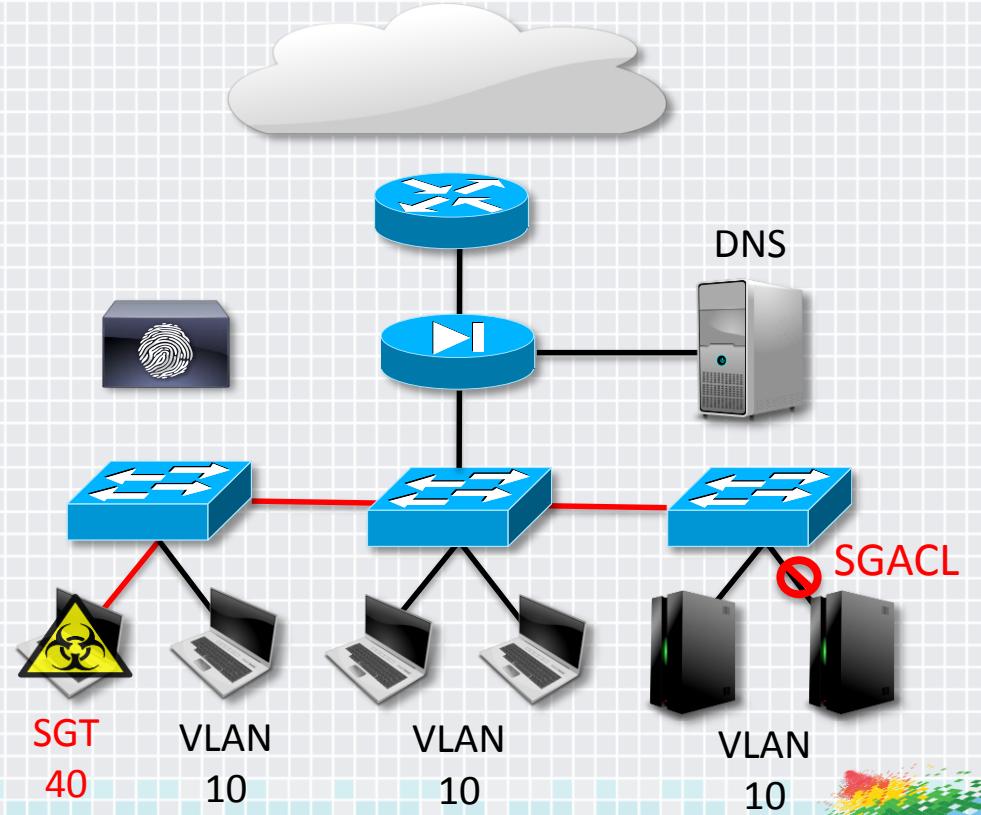
1. VLAN Containment
2. Security Group Tagging

What is needed to apply
This rule?

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

Other requirements

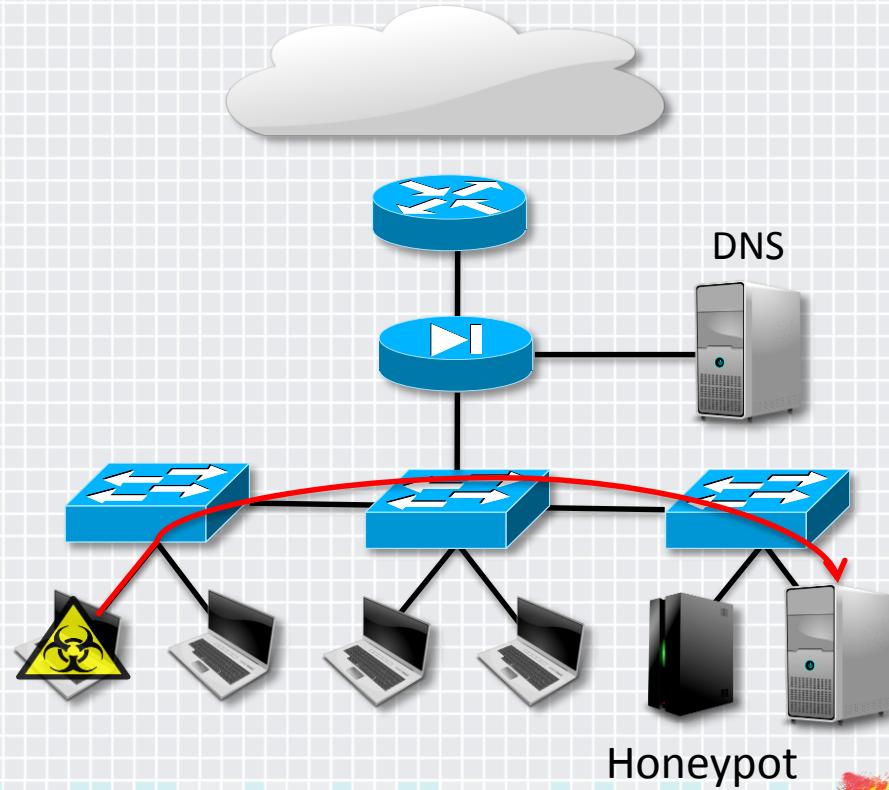
- Security Group Policy enforcer
- Network devices that can handle tags



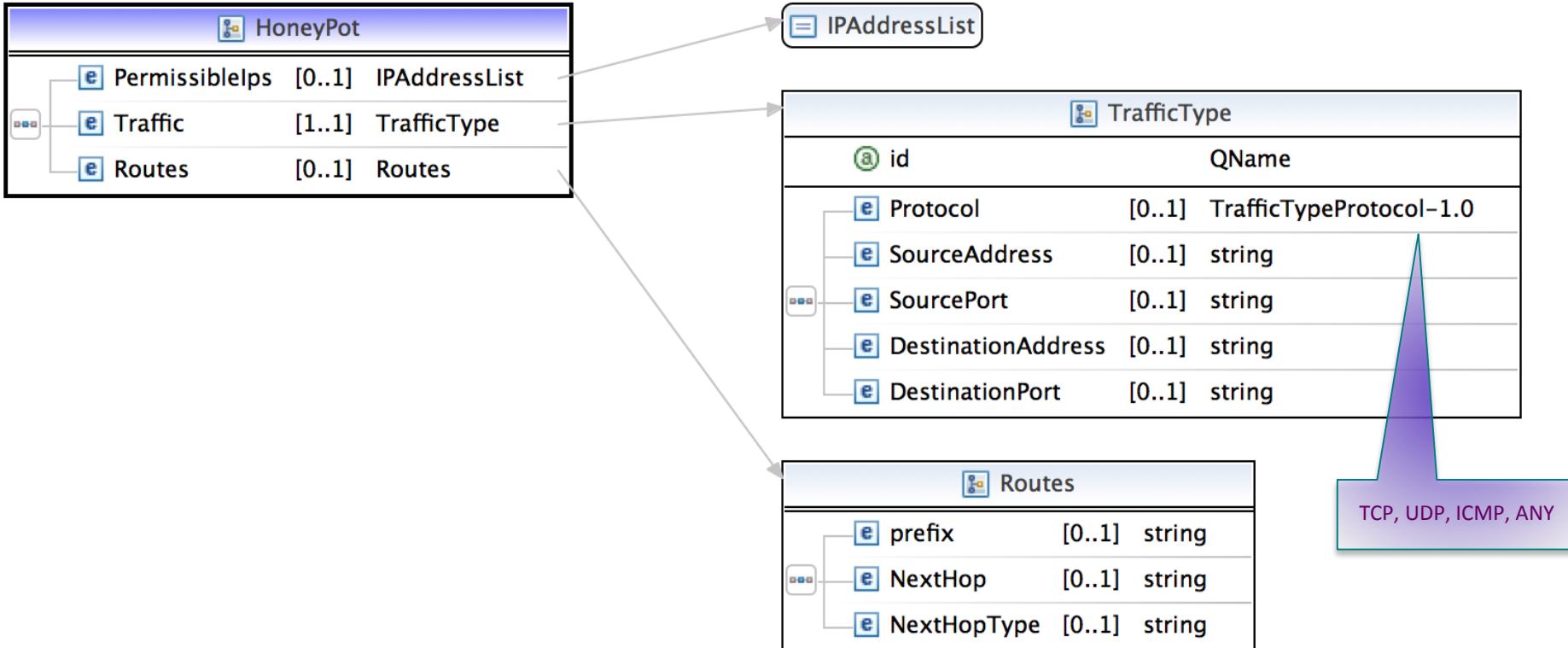
CONTAINMENT TO HONEYNET

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



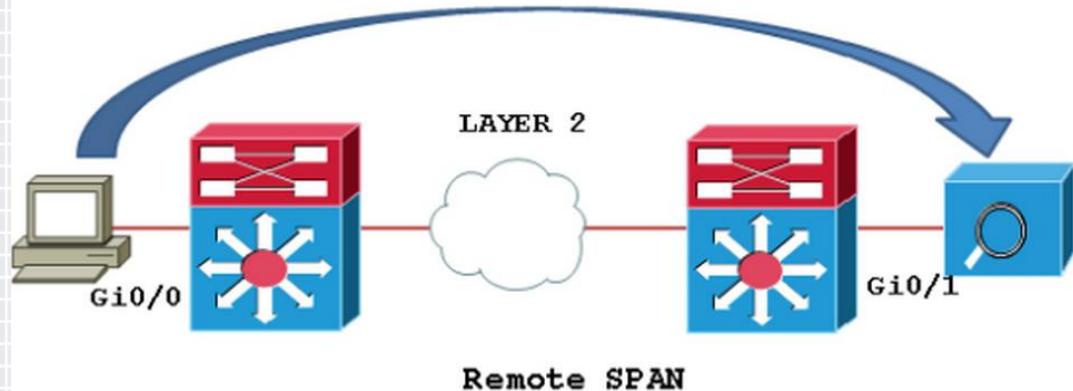
ContainType - HoneyPot



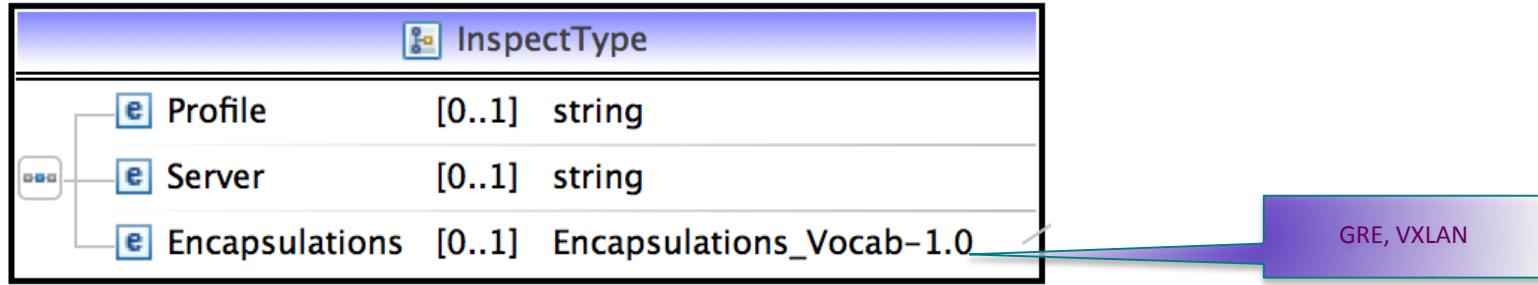
INSPECTION ON DEMAND

What is needed to achieve this?

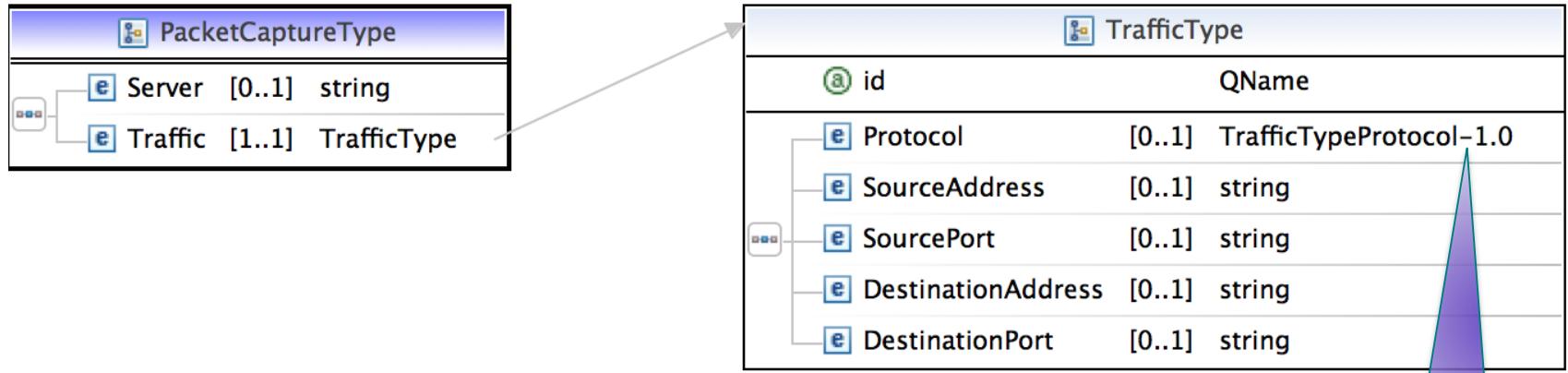
- Inspection profile
- Inspection Server
- Encapsulations – GRE, VXLAN etc.



NetworkStructuredCOAType - InspectType



PacketCaptureType



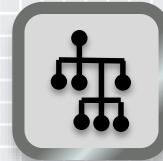
TCP, UDP, ICMP, ANY

Workflow

Threat Analytics



API



Network
Controller



Identity
Services
Engine



Workflow

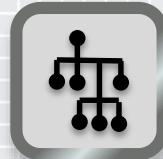
Threat Analytics



1. Export incidents in a given time range



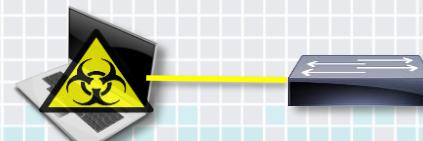
API



Network
Controller



Identity
Services
Engine

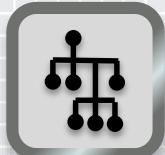


Workflow

Threat Analytics



2. STIX report for exported incidents with suggested course of actions



Network
Controller

API

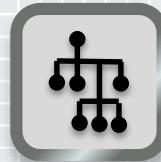
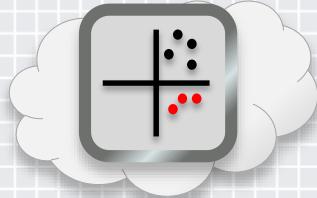


Identity
Services
Engine



Workflow

Threat Analytics



Network
Controller

API

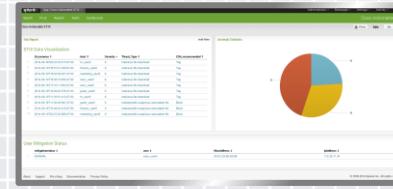
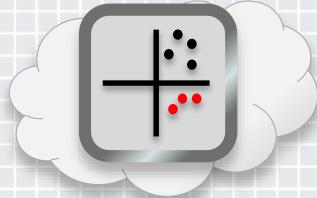


Identity
Services
Engine

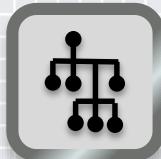


Workflow

Threat Analytics



API



Network
Controller



Identity
Services
Engine

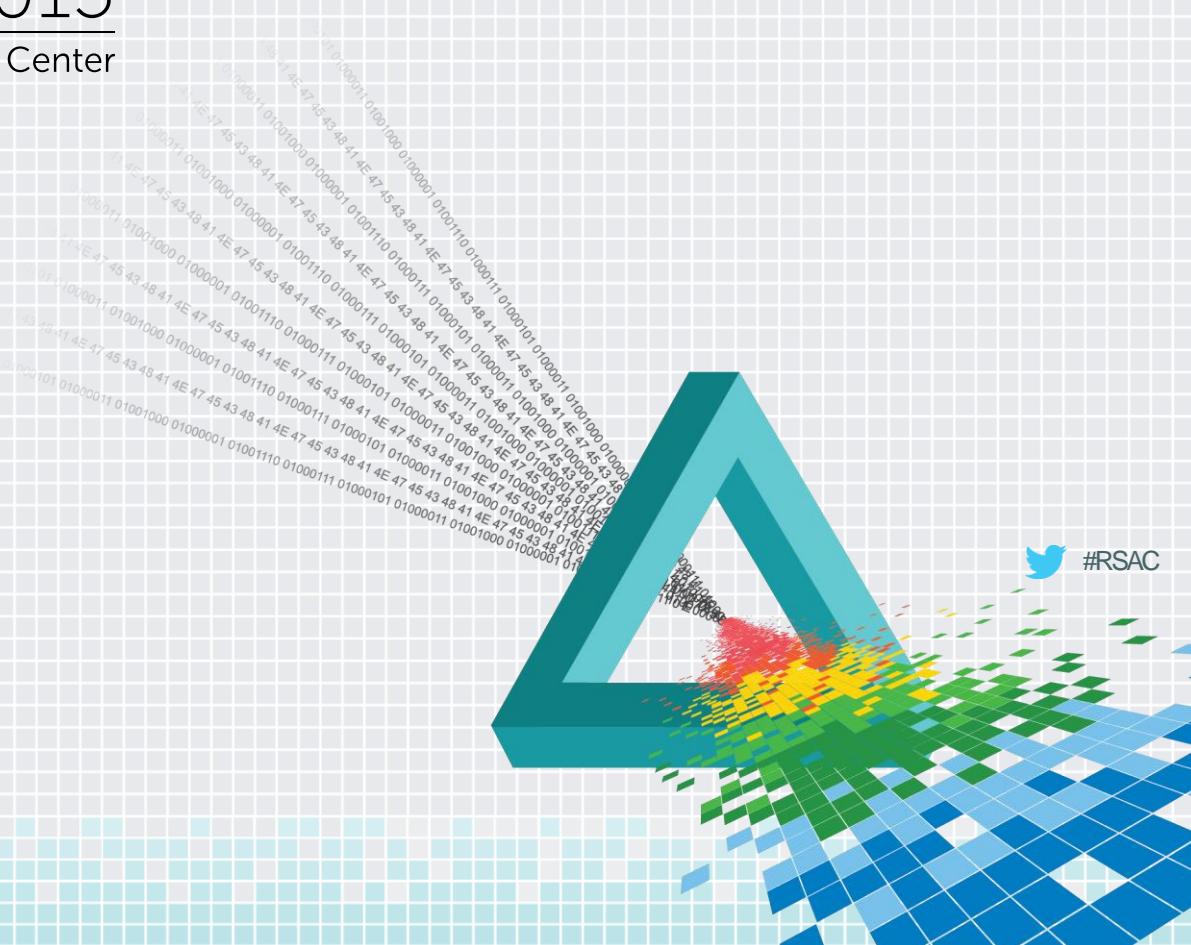
4. SDN & ISE TD system responds



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Demonstration



Future work

Threat Analytics



5. SIEM feeds back COA
Taken to TIA

6. TIA updates incident
with COA Taken



Network
Controller



Identity
Services
Engine



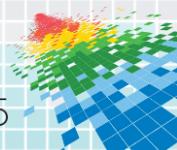
Summary

- ◆ 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



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Thanks for your attention



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>
```

