



San Francisco | March 4–8 | Moscone Center

A large, abstract graphic in the top right corner consists of numerous thin, colored lines (blue, green, yellow) radiating from a central point, resembling a network or a starburst pattern.

BETTER.

SESSION ID: PDAC-T07

# When the One You Trust Hurts You Most: Real-World Attack, Real-Time Response

**Bret Hartman**

VP and CTO  
Cisco Security Business Group

**Jyoti Verma**

Technical Leader  
Cisco Security Business Group

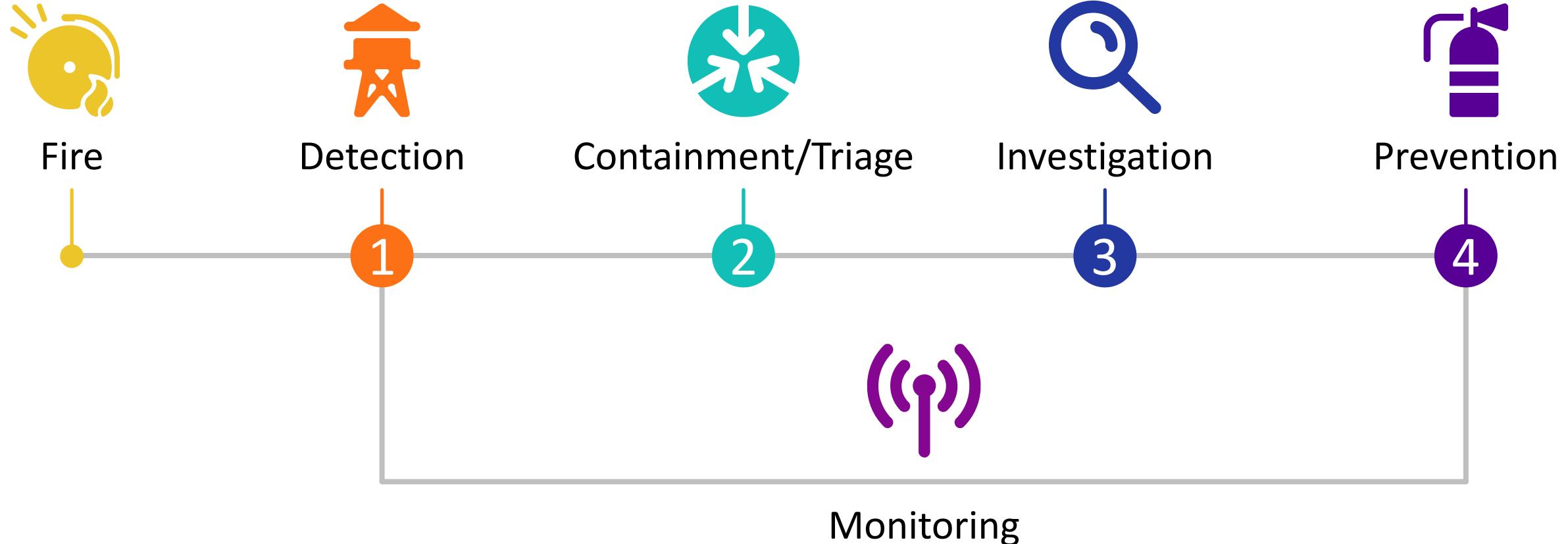
#RSAC

“This is the new abnormal, and this new abnormal will continue.”

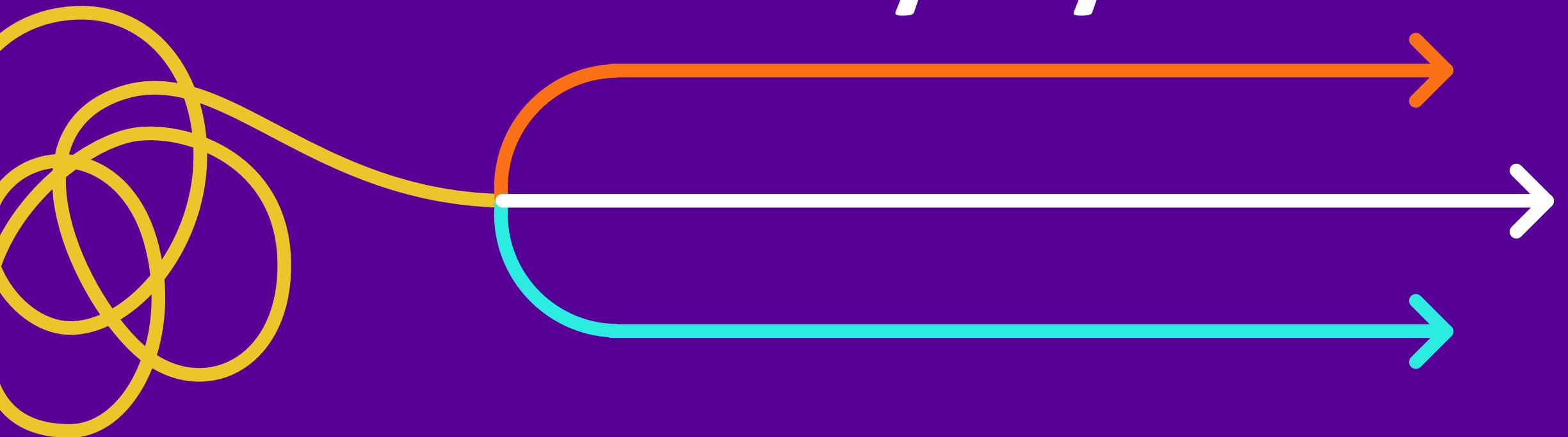
Jerry Brown,  
Former California Governor



# Fire Response Timeline



# Nyetya





Search

To: Customer



Isabel

Please, yes. LMK what you see/find. Thank you.

Hey Bret, yt? Think we have a problem. Help. It's critical.

Hi Isabel. In the middle of a talk at RSA. Will see what I can do. I have your login still from last week – let me take a look. Cool?

Delivered

Please, yes. LMK what you see/find. Thank you.

Hi Isabel. In the middle of a talk at RSA. Will see what I can do. I have your login still from last week – let me take a look. Cool?



Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

## Host Group Report | Internal Networks

Change Host Group

Alarming Hosts



Summary



Top Alarming Hosts



HOST

10.201.3.83

Production\_Servers

10.201.3.103

Production\_Servers

10.201.3.179

Production\_Servers

10.201.3.99

Production\_Servers

10.201.3.149

Production\_Servers

10.201.3.47

Production\_Servers

10.201.3.13

Production\_Servers

CATEGORY

[View All Hosts >](#)

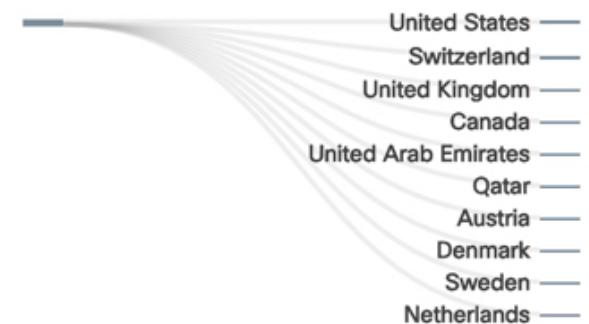
Top Host Groups By Traffic (Last 12 Hours) - Updated at 9:46 PM

[Update](#)

Top 10 Inside Host Groups



Top 10 Outside Host Groups



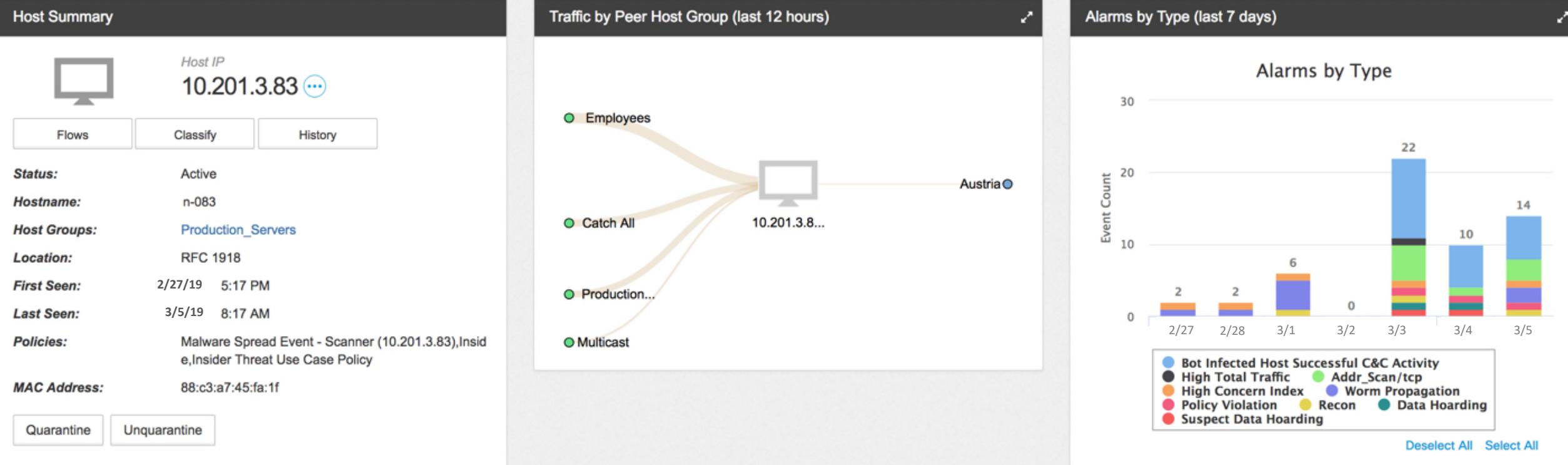
Internal Networks

161 Additional Host Groups (less than 1% of Outside Traffic)

Top Applications (Last 12 Hours)

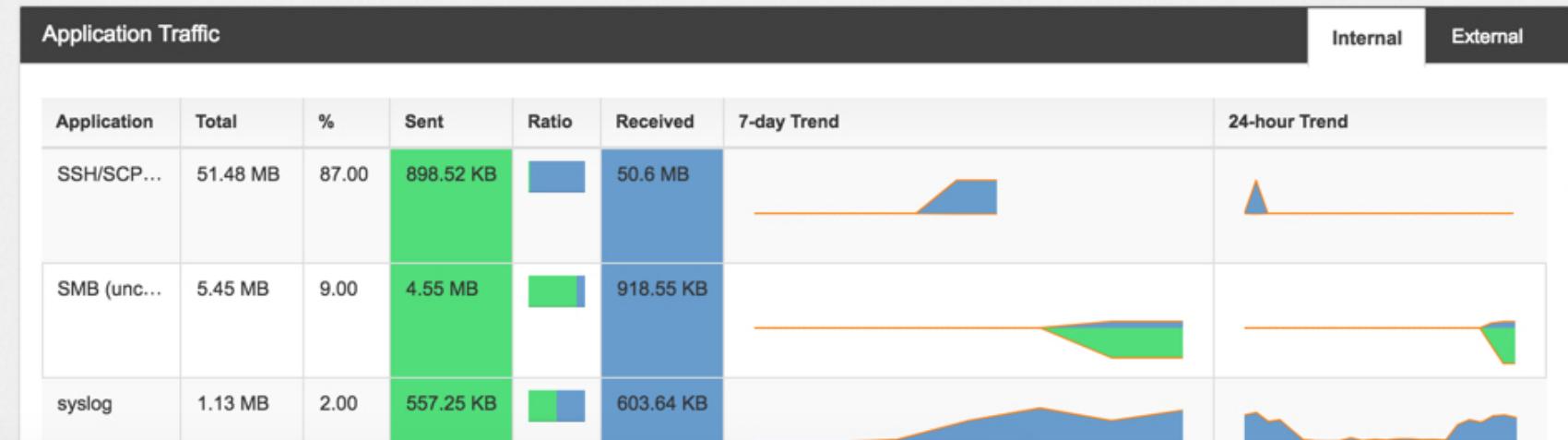
## Host Report | 10.201.3.83

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	1	0	0	0	0	0	0	1	0

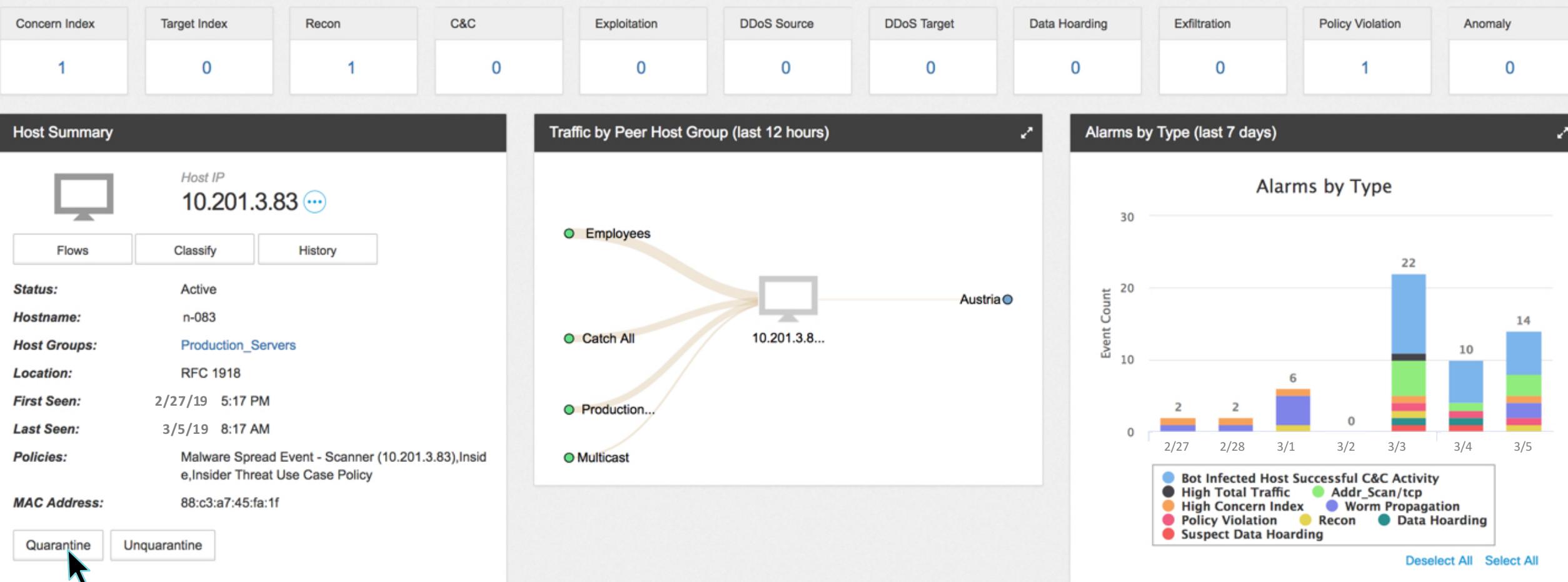


Top Security Events for 10.201.3.83								Source (10)	Target (3)
SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	SOURCE HOST	SOURCE HOST GROUP	TARGET HOST	TARGET HOST GROUP	ACTIONS	
▼ Addr_Scan/tcp - 445	1,574	1,045,574	02/27 5:34:07 AM	10.201.3.83 ⓘ	Production_Servers	10.201.1.0/24 ⓘ	Catch All	ⓘ	
<strong>DETAILS</strong>									
--									
<strong>DESCRIPTION</strong>									
Addr_Scan/tcp - 445: The source host is attempting to contact multiple hosts (using TCP) within a natural class C network (/24) on the same port and most connection attempts are either being rejected (TCP Reset) or the target hosts are not responding at all. This is used to trigger the Worm Activity and Worm Propagation alarms. These are commonly seen during network scanning or enumeration.									
▶ Addr_Scan/tcp - 445	1,036	689,036	02/27 5:34:15 AM	10.201.3.83 ⓘ	Production_Servers	10.201.8.0/24 ⓘ	Catch All	ⓘ	
▼ Worm Propagation - 445	2	38,402	02/27 6:36:21 AM	10.201.3.83 ⓘ	Production_Servers	10.120.100.254 ⓘ	Employees	ⓘ	
<strong>DETAILS</strong>									
Worm propagated from Source Host using smb (TCP)									
<strong>DESCRIPTION</strong>									
Worm Propagation - 445: The host has scanned and connected on a particular port across more than one subnet, and the host was previously scanned and connected to by a host for which the Worm Activity alarm has been raised.									
▼ Bot Infected Host Success... 6	0	0	02/27 5:42:04 AM	10.201.3.83 ⓘ	Production_Servers	146.112.61.107 ⓘ	Austria	ⓘ	
<strong>DETAILS</strong>									
--									
<strong>DESCRIPTION</strong>									
Bot Infected Host Successful C&C Activity - 80: Bot Infected Host - Successful C&C Activity									

Users & Sessions		
MAC Address:	MAC Vendor:	Device Type:
88:c3:a7:45:fa:1f		Windows10-Workstation
User	Start	End
brian	2/27/19 4:31 AM	★ Current
MAC Address:	MAC Vendor:	Device Type:
76:c6:90:1b:89:85		Windows10-Workstation
User	Start	End
brian	2/27/19 4:31 AM	3/5/19 4:16 AM



## Host Report | 10.201.3.83



## Host Report | 10.201.3.83

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	1	0	0	0	0	0	0	1	0

## Host Summary

Host IP  
10.201.3.83

Flows Classify History

Status: Active

Hostname: n-083

Host Groups: Production\_Servers

Location: RFC 1918

First Seen: 2/27/19 5:17 PM

Last Seen: 3/5/19 8:17 AM

Policies: Malware Spread Event - Scanner (10.201.3.83), Inside, Insider Threat Use Case Policy

MAC Address: 88:c3:a7:45:fa:1f

Quarantine Unquarantine

## Quarantine Results

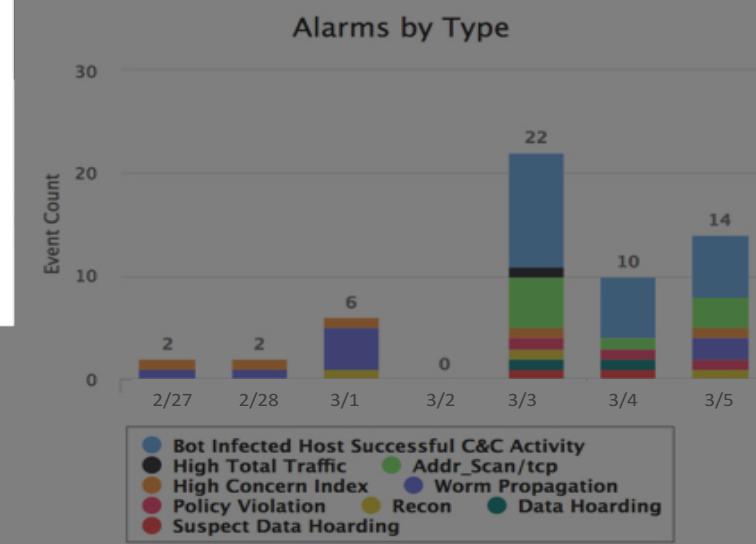
Cluster Name: ISE Simulator Quarantine Result: SUCCESS

[Show Details](#)

Ok



## Alarms by Type (last 7 days)



## Network Access Control

DESIGN POLICY PROVISION ASS

Dashboard Virtual Network Policy Administration Contracts

Group-Based Access Control (Fabric) IP-Based Access Control (No)

Filter Edit Delete Deploy

- Policy Name ▾
- Employees-PCI\_Servers
- Employees-PCI\_Servers\_reverse
- Employees-Unknown
- PCI\_Compliant\_traffic
- Quarantine

Show 10 entries

Quarantine - Details

Sources: Quarantined\_Systems

Contract: Name : Limited\_Access  
Implicit Action : DENY

Destinations: Development\_Servers  
Finance\_Server  
Employees  
Production\_Servers

Created: 1:47 pm Refresh Advanced Options Add Policy

DEPLOYED

Showing 1 - 5 of 5

Previous 1 Next

## Flow Search Results (6)

Edit Search

06/02/2018 10:00 PM - 06/03/2018 08:36 AM (Time Range)

2,000 (Max Records)

100% Complete

Delete Search

Subject: 10.201.3.83 Client (Orientation)

Connection: All (Flow Direction)

Peer: 146.112.61.107



Manage Columns

Summary

Export ▾



START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	SUBJECT TRU...	SUBJECT TRU...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEE
Ex. 06/05	Ex. <=50min	Ex. 10.10.10.	Ex. 57100/UDI	Ex. "catch Al	Ex. <=50M	Ex. 7	Ex. jsmith	Ex. "Corpora	Ex. <=50M	Ex. 10.255.2:	Ex. 2055/UDI	E
March 5, 2019 5:59:... (2hr 37min 53s a... --		10.201.3.83	1157/TCP	Production_Servers	1.66 K	--	--	HTTP	2.66 K	146.112.61.107	80/TCP	Aust

Host Groups: Production\_Servers  
Payload: http://ret.space:80/checkin

RTT: --

SRT: --

Host Groups: Austria  
Payload: --

Host Groups: Production\_Servers  
Payload: http://ret.space:80/checkin

Investigation

ret.space  
retdemos.com

Start New Investigation Clear Cancel What can I search for?

Investigation

Investigate Snapshots Explore Intel Modules



New Investigation

Edit This Investigation

Take Snapshot

2 of 2 enrichments complete



2

Targets

2

Observables

2

Indicators

2

Domains

0

File Hashes

0

IP Addresses

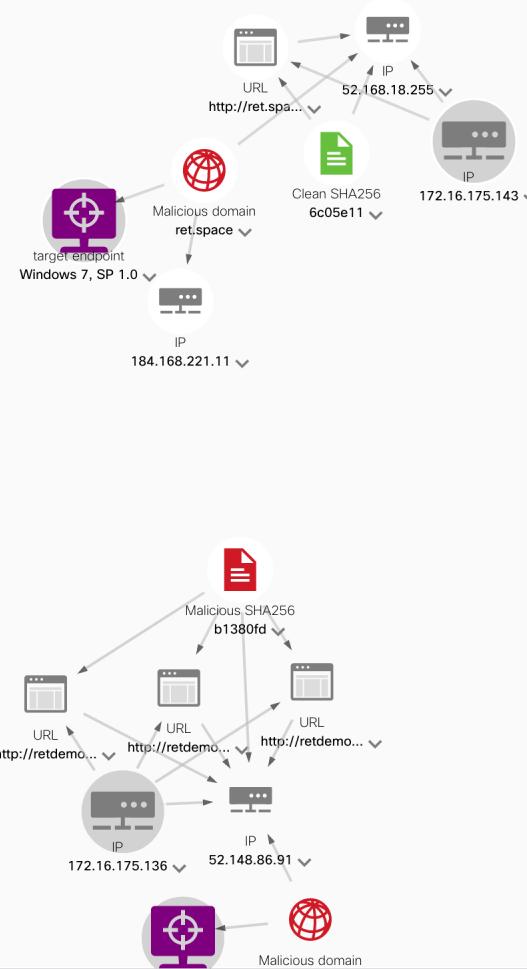
0

URLs

5

Modules

Relations Graph



Observables

ret.space

Malicious Domain

Last seen on March 5<sup>th</sup>, 2019, in My Environment

retdeemos.com

Malicious Domain

Last seen on March 5<sup>th</sup>, 2019, in My Environment

ret.space

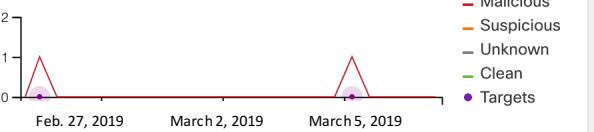
Malicious Domain

My Environment Global

2 Sightings in My Environment

First: Feb 27<sup>th</sup>, 2019

Last: March 5<sup>th</sup>, 2019



Judgements (18) Verdicts (2) Sightings (103) Indicators (2)

Module	Disposition	Reason	Source	Sev.	Conf.	TLP	Expiration
Talos Intelligence	Malicious	Poor Talos Intelligenc...	Talos	High	High	White	Invalid start time
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 14 days ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 3 months ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 3 months ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 4 months ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 4 months ago

Show 12 more ▾

**Investigation**

**Relations Graph**

**Targets** 2

**Malicious domain** **ret.space**

**Clean SHA256** **6c05e11**

**IP** **184.168.221.11**

**IP** **52.168.18.255**

**IP** **172.16.175.143**

**target endpoint** **Windows 7, SP 1.0**

**Malicious SHA256** **b1380fd**

**URL** **http://retdemo...**

**URL** **http://retdemo...**

**URL** **http://retdemo...**

**IP** **172.16.175.136**

**IP** **52.148.86.91**

**Malicious domain**

**Legend:**

- Malicious
- Suspicious
- Unknown
- Clean
- Targets

**March 2, 2019**   **March 5, 2019**

**Indicators (2)**

	Sev.	Conf.	TLP	Expiration
	High	High	White	Invalid start time
rid rat-dns feed	High	High	Green	Expired 14 days ago
rid rat-dns feed	High	High	Green	Expired 3 months ago
rid rat-dns feed	High	High	Green	Expired 3 months ago
rid rat-dns feed	High	High	Green	Expired 4 months ago
rid rat-dns feed	High	High	Green	Expired 4 months ago

Investigation

Observables

**ret.space**  
Malicious Domain  
Last seen on March 5<sup>th</sup>, 2019, in My Environment

**retdemos.com**  
Malicious Domain  
Last seen on March 5<sup>th</sup>, 2019, in My Environment

**ret.space**

Malicious Domain

My Environment Global

2 Sightings in My Environment

First: February 27, 2019  
Last: March 5, 2019

Judgements (18) Verdicts (2) Sightings (103) Indicators (2)

Module	Disposition	Reason	Source	Sev.	Conf.	TLP	Expiration
Talos Intelligence	Malicious	Poor Talos Intelligence...	Talos	High	High	White	Invalid start time
AMP Global Intel	Malicious	Remote Access Trojan (F)	Threat Grid rat-dns feed	High	High	Green	Expired 14 days ago
AMP Global Intel	Malicious	Remote Access Trojan (F)	Threat Grid rat-dns feed	High	High	Green	Expired 3 months ago
AMP Global Intel	Malicious	Remote Access Trojan (F)	Threat Grid rat-dns feed	High	High	Green	Expired 3 months ago
AMP Global Intel	Malicious	Remote Access Trojan (F)	Threat Grid rat-dns feed	High	High	Green	Expired 4 months ago
AMP Global Intel	Malicious	Remote Access Trojan (F)	Threat Grid rat-dns feed	High	High	Green	Expired 4 months ago

Show 12 more ▾

Conf.	TLP	Expiration
High	White	Invalid start time
High	Green	Expired 14 days ago
High	Green	Expired 3 months ago
High	Green	Expired 3 months ago
High	Green	Expired 4 months ago
High	Green	Expired 4 months ago

Investigation

Investigate Snapshots Explore Intel Modules



New Investigation

Edit This Investigation

Take Snapshot

2 of 2 enrichments complete



2

Targets

2

Observables

2

Indicators

2

Domains

0

File Hashes

0

IP Addresses

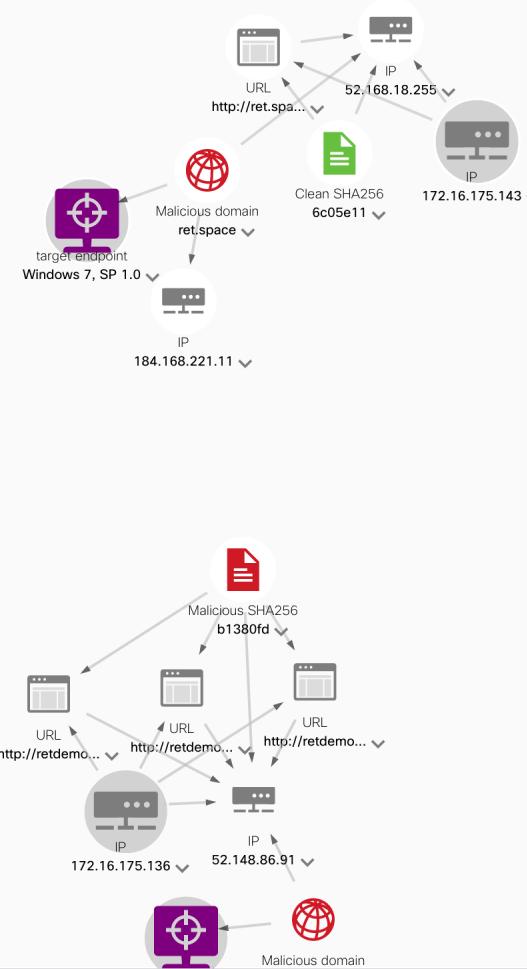
0

URLs

5

Modules

Relations Graph



Observables

ret.space

Malicious Domain

Last seen on March 5<sup>th</sup>, 2019, in My Environment

retdemos.com

Malicious Domain

Last seen on March 5<sup>th</sup>, 2019, in My Environment

ret.space

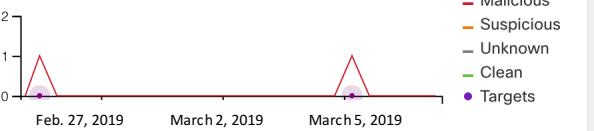
Malicious Domain

My Environment Global

2 Sightings in My Environment

First: Feb 27<sup>th</sup>, 2019

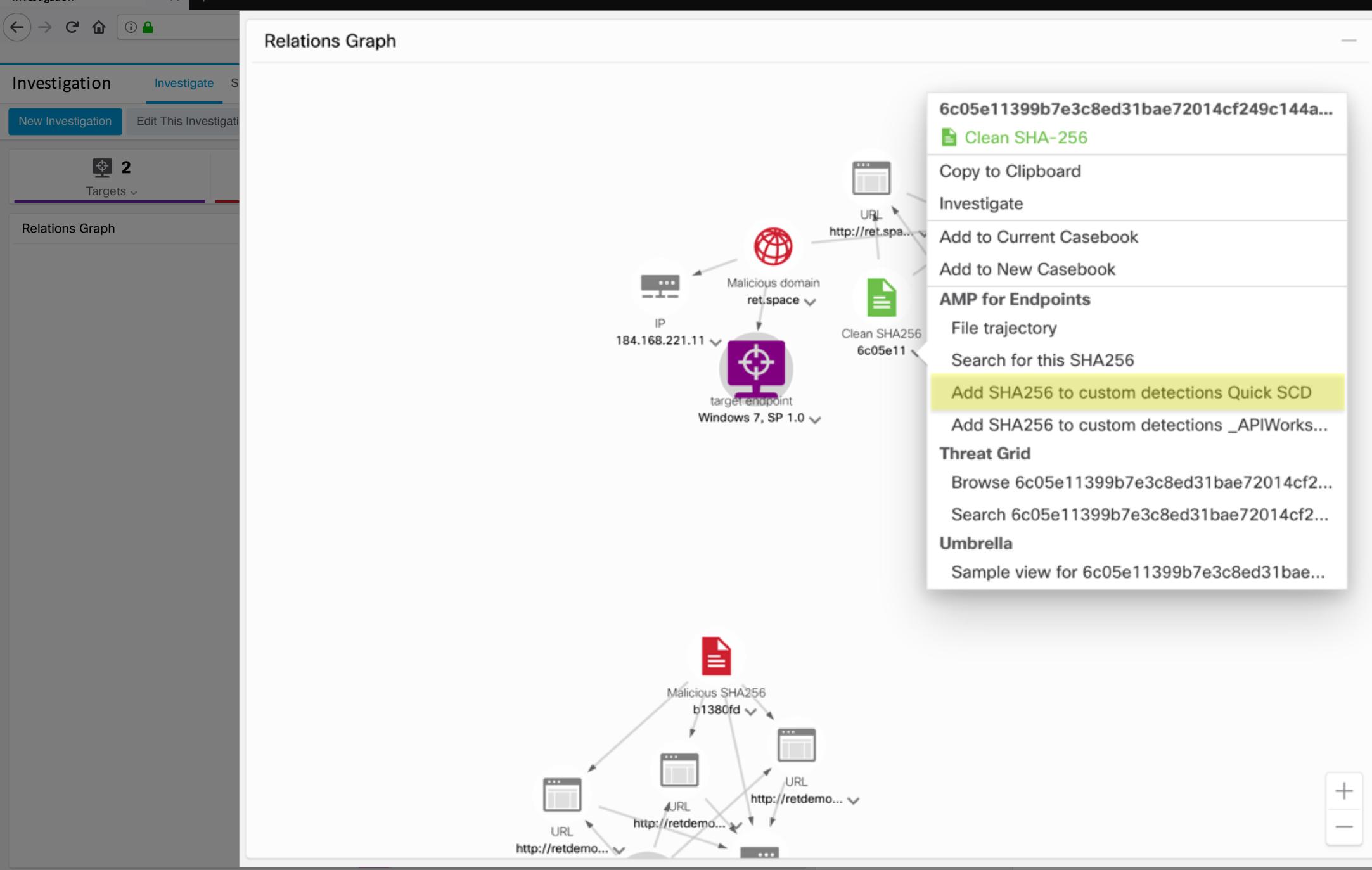
Last: March 5<sup>th</sup>, 2019



Judgements (18) Verdicts (2) Sightings (103) Indicators (2)

Module	Disposition	Reason	Source	Sev.	Conf.	TLP	Expiration
Talos Intelligence	Malicious	Poor Talos Intelligenc...	Talos	High	High	White	Invalid start time
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 14 days ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 3 months ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 3 months ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 4 months ago
AMP Global Intel	Malicious	Remote Access Trojan (f	Threat Grid rat-dns feed	High	High	Green	Expired 4 months ago

Show 12 more ▾



?

## 5

Modules ▾

—

2019      March 5, 2019

)

—

	Sev.	Conf.	TLP	Expiration
	High	High	White	Invalid start time
feed	High	High	Green	Expired 14 days ago
feed	High	High	Green	Expired 3 months ago
feed	High	High	Green	Expired 3 months ago
feed	High	High	Green	Expired 4 months ago
feed	High	High	Green	Expired 4 months ago



All Threads

Channels

# general

# random

# secops

Direct Messages

slackbot

InfoSec Administrator ...

+ Invite people

Apps

## #secops

☆ | 1 | 0 | Add a topic



Search

@ ⭐ :

# # secops

You created this channel today. This is the very beginning of the # secops channel.

 Set a purpose  Add an app  Invite others to this channel

Today



InfoSec Administrator 12:50 PM

joined #secops.

 Only visible to you



slackbot 12:51 PM

Hello  @InfoSec Administrator! I'm Slackbot, your automated helper in Slack. I'm just a computer program, but I do my best to help.

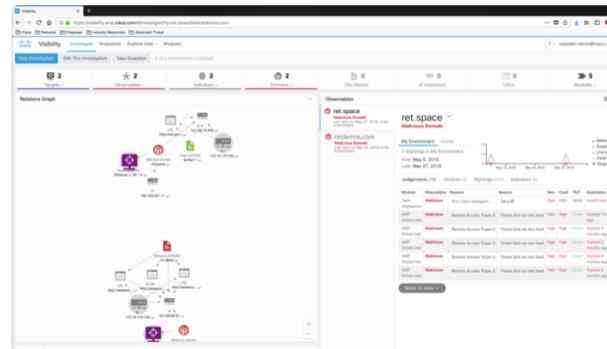
Right now – even if you don't have teammates in Slack yet – you can set the stage for conversation in #secops. Sending a message or sharing a file will give your teammates something to respond to when they arrive.

Use the input field below to **type a message**, and press Enter to send. Or, click the plus sign to the left of the input field to **upload a file**. If you have any questions, look for my name on the left and send me a direct message!



InfoSec Administrator 12:53 PM

 @here - Take a look at [retspace.com](#). Looks like the hash associated with it is now malicious and causing havoc!



Message #secops



prob

 Incident  
INC0010008

Follow

Update



Problem

Create New

Assigned to me

Known Errors

Open

Pending

All

Overview

Notes Related Records Resolution Information

Parent Incident

Change Request

Problem

PRB0040002



Caused by Change

Update

## Related Links

Show SLA Timeline

Task SLAs (2) Affected CIs (1) Impacted Services Child Incidents (4)

Task SLAs	Go to	SLA definition	Search
Task = INC0010008			
SLA definition	Type	Target	Stage
<input type="checkbox"/> Priority 1 resolution (1 hour)	SLA	Resolution	Paused
<input type="checkbox"/> Priority 1 response (15 minutes)	SLA	Response	Completed
<input type="checkbox"/> Actions on selected rows...			

## Problem

Hold SHIFT and move the cursor to keep this window open

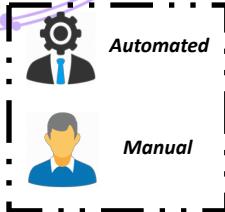
Number	PRB0040002	State	Open
Business service	Datacenter server	Impact	1 - High
Configuration item	10.201.3.83	Urgency	1 - High
Change request		Priority	1 - Critical
Major problem		Assignment group	Hardware
Knowledge		Assigned to	John Doe
Known error			
Short description	Mail server is down		
Description			

# Automated Playbook Detection, Containment and Remediation

# Pre-processing

Network Behavioral  
Analytics (NBA) Alert

Start



Preprocessing

Extract artifacts from Alert(Source information)



Query NBA (source IP sessions with alert time window)



Extract external IPs from the session list



IP Reputation check



Malicious IP  
found?

Yes

No

**Mitigation**  
Perimeter block

Add IP to watch-list



Query Threat intelligence sources for  
additional artifacts



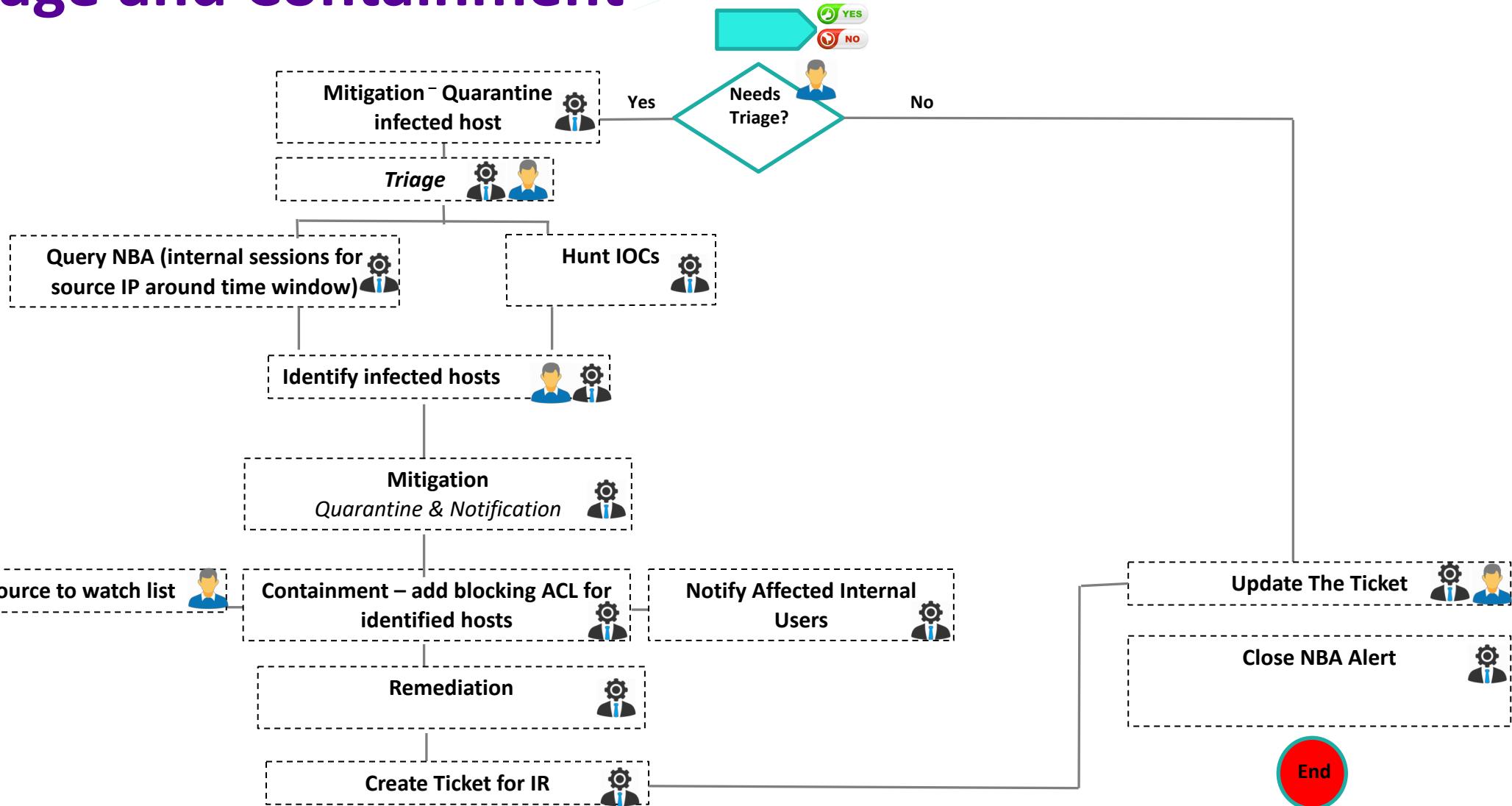
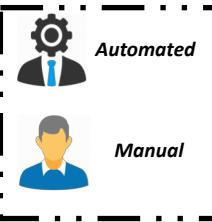
Annotate Incident Context  
Notes about Malware



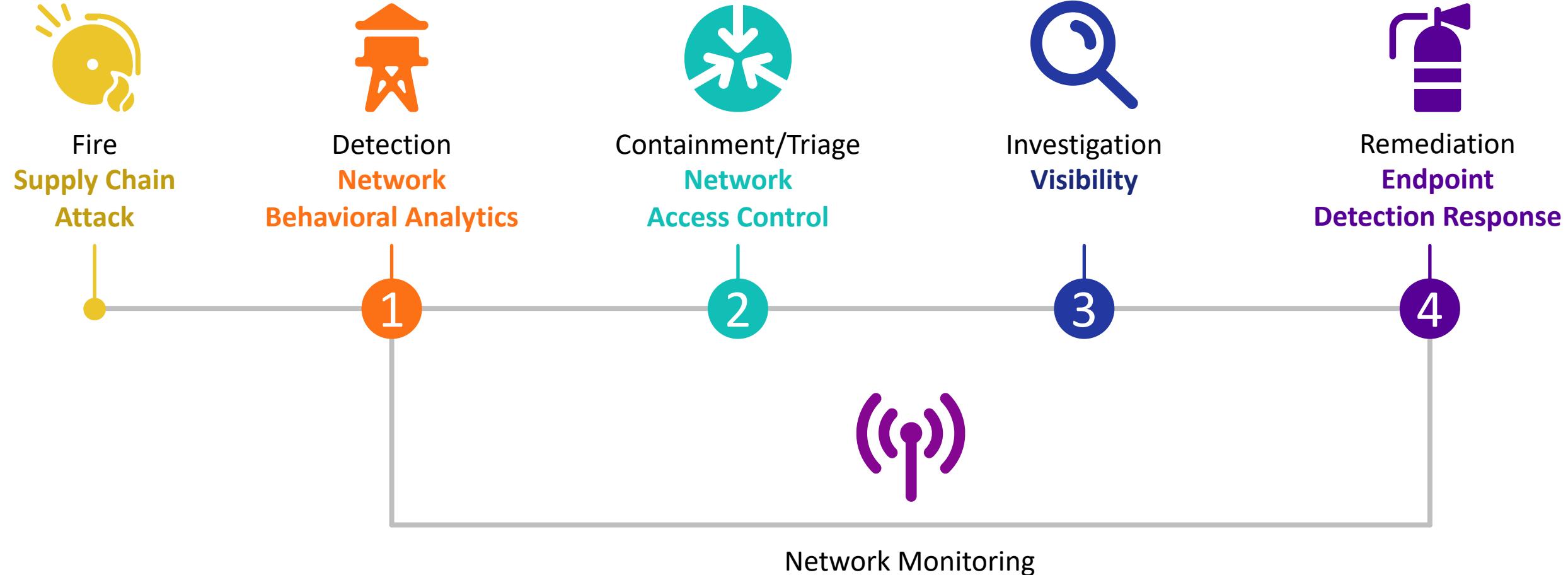
YES

NO

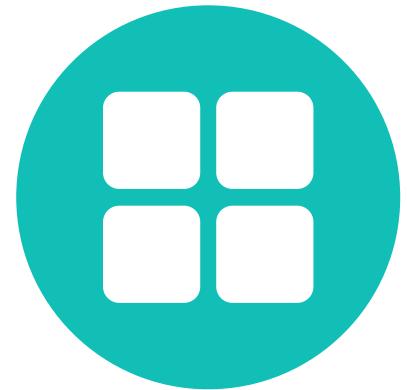
# Triage and Containment



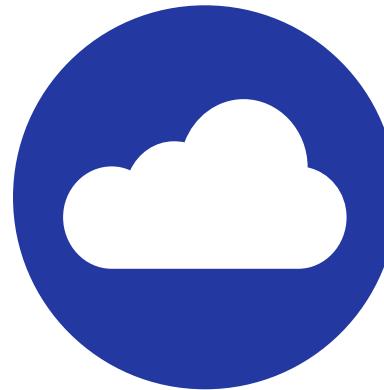
# Response Recap



# Lessons Learned



Supply Chain



No Borders



Machine Speed

# Apply It

- **Now:** Study up!
  - Ongoing standards:
    - NIST Cybersecurity Framework
    - MITRE ATT&CK Framework
    - OASIS - STIX, OpenC2
    - CACAO
  - RSA Sessions
- **Three Months:** Do you have the right foundation?
  - **Assess** the detection and response systems within your own organization and determine if you have enough in place.
- **Six Months:** How would you **apply** what you have to a more automated environment?

# RSA® Conference 2019

Thank you.

**How to Support Fire Victims**

**American Red Cross**  
[www.redcross.org](http://www.redcross.org)