RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-T07

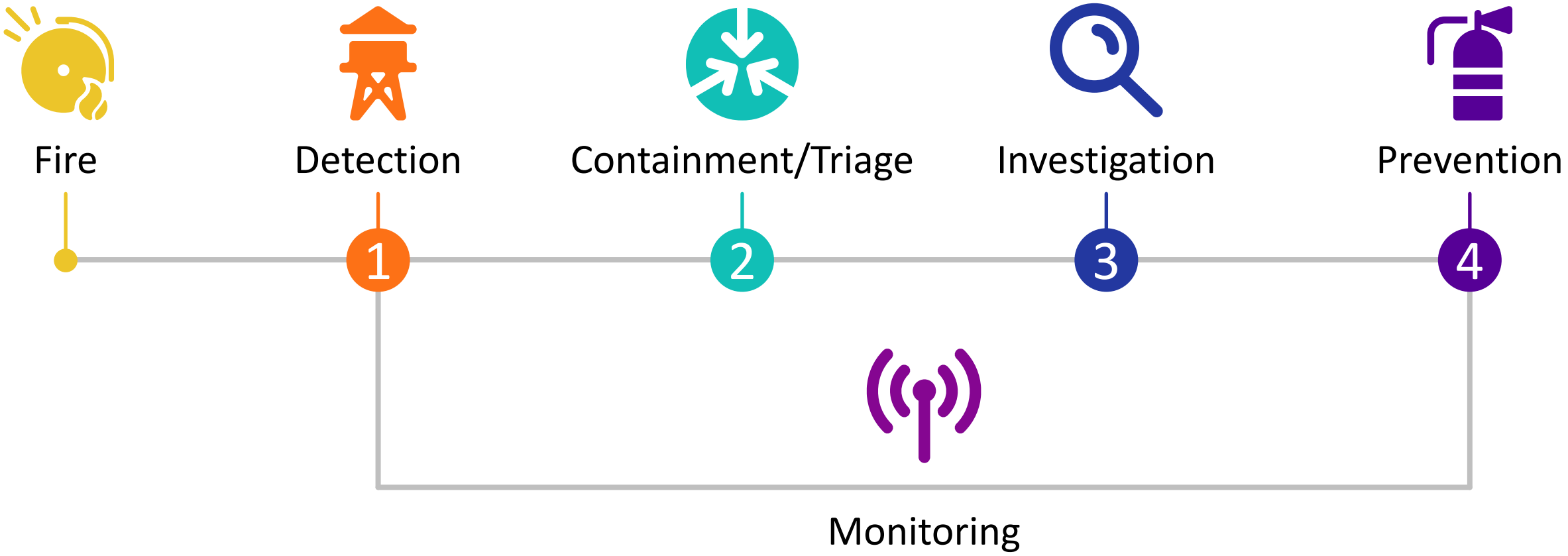
When the One You Trust Hurts You Most: Real-World Attack, Real-Time Response

Bret Hartman
VP and CTO
Cisco Security Business Group

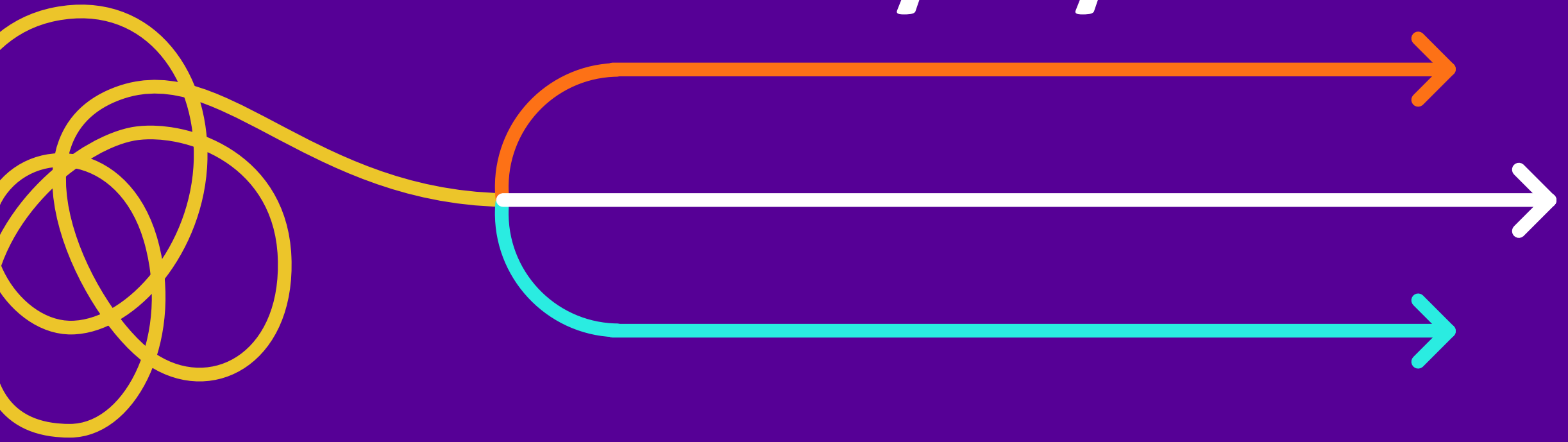
Jyoti Verma
Technical Leader
Cisco Security Business Group


“This is the new abnormal, and this new abnormal will continue.”
Jerry Brown,
Former California Governor

Fire Response Timeline



Nyetya



Search

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

To: Customer

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?

Network Behavioral Analytics

Dashboards | Monitor | Analyze | Jobs | Configure | Deploy

Desktop Client

Host Group Report | Internal Networks

Change Host Group

Alarming Hosts

Summary

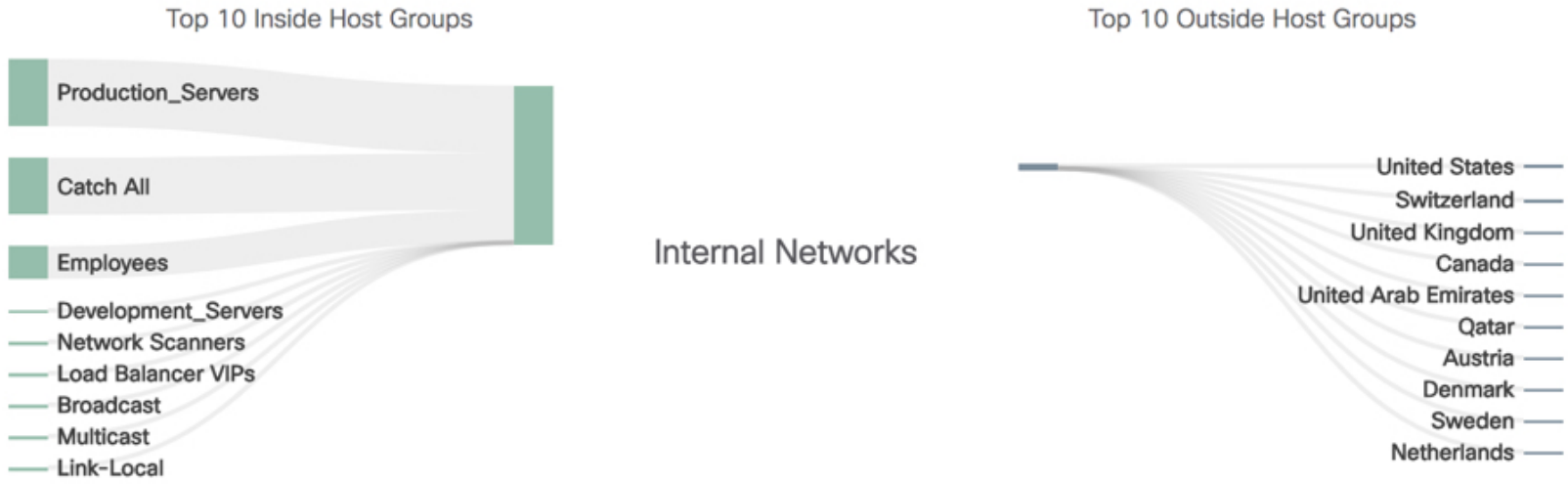
Top Alarming Hosts

HOST	CATEGORY
10.201.3.83 Production_Servers	PV DH CI RC
10.201.3.103 Production_Servers	PV CI EX
10.201.3.179 Production_Servers	PV CI RC DH
10.201.3.99 Production_Servers	DH CI
10.201.3.149 Production_Servers	DH RC CI EX
10.201.3.47 Production_Servers	CI DH RC
10.201.3.13 Production_Servers	CI DH

View All Hosts >

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

Update



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

Top Applications (Last 12 Hours)

Network Behavioral Analytics

Dashboards | Monitor | Analyze | Jobs | Configure | Deploy

Desktop Client

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

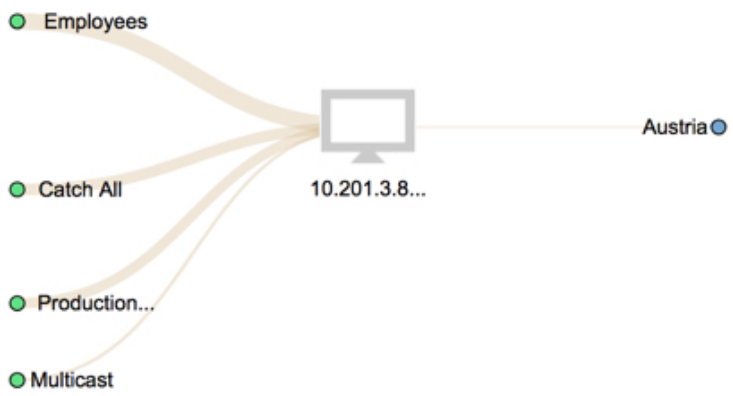
Host IP
10.201.3.83

Flows | Classify | History

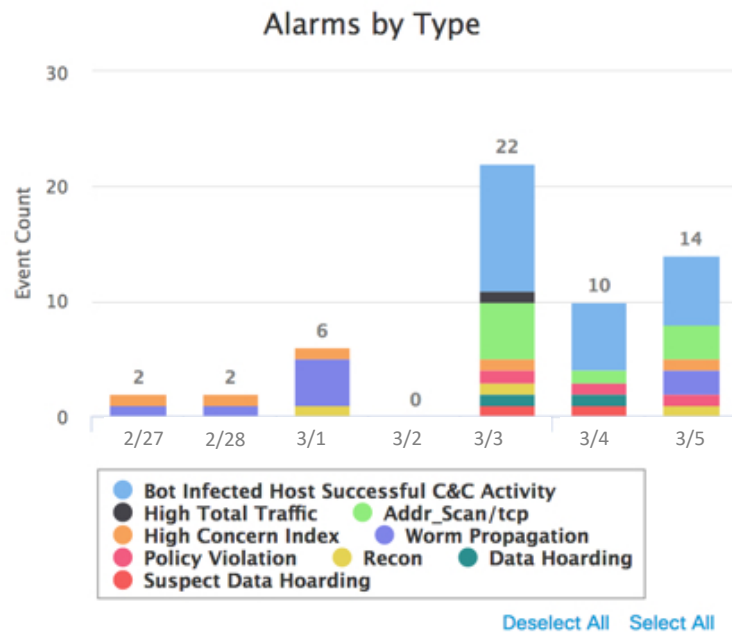
Status: Active
Hostname: n-083
Host Groups: Production_Servers
Location: RFC 1918
First Seen: 2/27/19 5:17 PM
Last Seen: 3/5/19 8:17 AM
Policies: Malware Spread Event - Scanner (10.201.3.83),Insid e,Insider Threat Use Case Policy
MAC Address: 88:c3:a7:45:fa:1f

Quarantine | Unquarantine

Traffic by Peer Host Group (last 12 hours)



Alarms by Type (last 7 days)



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	

DETAILS
--

DESCRIPTION
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	

DETAILS
Worm propagated from Source Host using smb (TCP)

DESCRIPTION
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 Successf…	6	0	02/27 5:42:04 AM	10.201.3.83	Production_Servers	146.112.61.107	Austria	

DETAILS
--

DESCRIPTION
Bot Infected Host Successful C&C Activity - 80: Bot Infected Host - Successful C&C Activity

Users & Sessions

MAC Address: 88:c3:a7:45:fa:1f
MAC Vendor:
Device Type: Windows10-Workstation

User	Start	End
brian	2/27/19 4:31 AM	★ Current

MAC Address: 76:c6:90:1b:89:85
MAC Vendor:
Device Type: Windows10-Workstation

User	Start	End
brian	2/27/19 4:31 AM	3/5/19 4:16 AM

Application Traffic

Internal | External

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
SSH/SCP…	51.48 MB	87.00	898.52 KB		50.6 MB		
SMB (unc…	5.45 MB	9.00	4.55 MB		918.55 KB		
syslog	1.13 MB	2.00	557.25 KB		603.64 KB		

Network Behavioral Analytics

Dashboards | Monitor | Analyze | Jobs | Configure | Deploy

Desktop Client

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

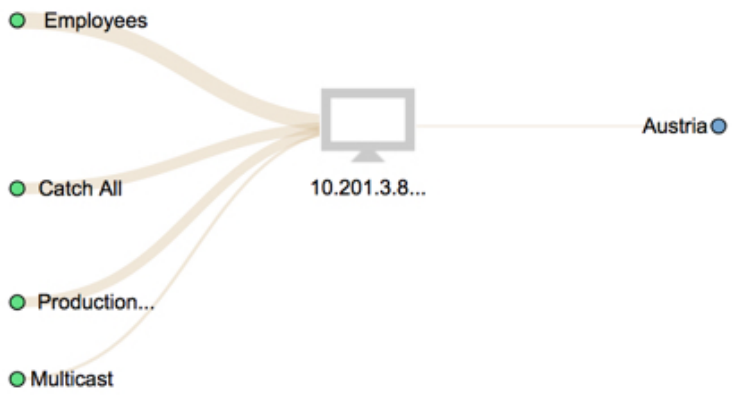
Host IP
10.201.3.83

Flows | Classify | History

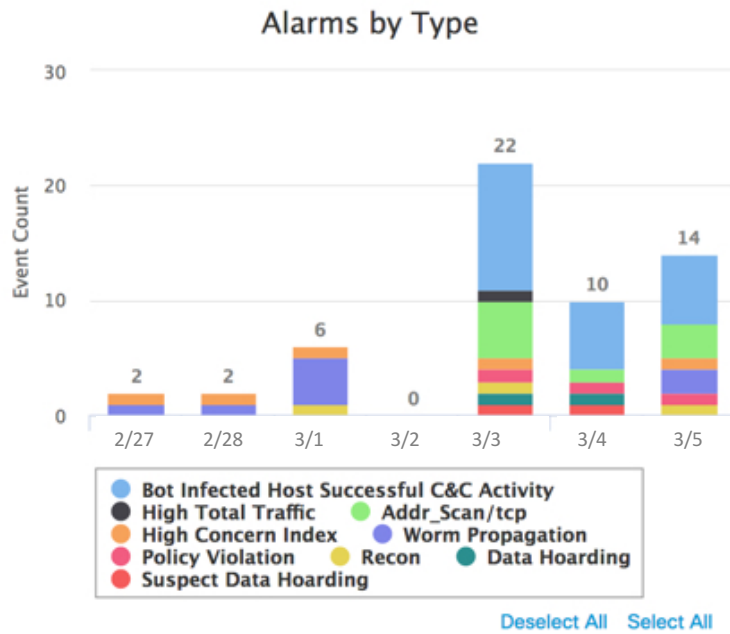
Status: Active
Hostname: n-083
Host Groups: Production_Servers
Location: RFC 1918
First Seen: 2/27/19 5:17 PM
Last Seen: 3/5/19 8:17 AM
Policies: Malware Spread Event - Scanner (10.201.3.83),Insid e,Insider Threat Use Case Policy
MAC Address: 88:c3:a7:45:fa:1f

Quarantine | Unquarantine

Traffic by Peer Host Group (last 12 hours)



Alarms by Type (last 7 days)



Network Behavioral Analytics

Dashboards Monitor Analyze Jobs Configure Deploy

Desktop Client

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

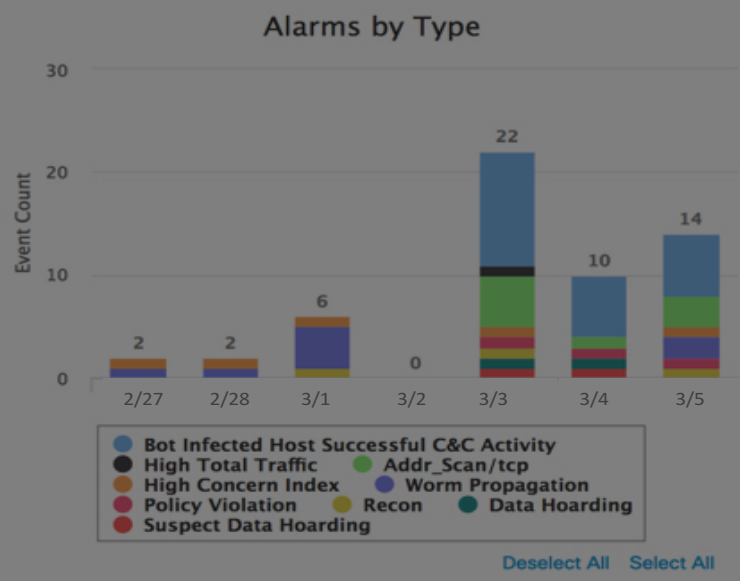
Status: Active
Hostname: n-083
Host Groups: Production_Servers
Location: RFC 1918
First Seen: 2/27/19 5:17 PM
Last Seen: 3/5/19 8:17 AM
Policies: Malware Spread Event - Scanner (10.201.3.83),Inside,Insider Threat Use Case Policy
MAC Address: 88:c3:a7:45:fa:1f

Quarantine | Unquarantine

Traffic by Peer Host Group (last 12 hours)

Production...
Multicast

Alarms by Type (last 7 days)



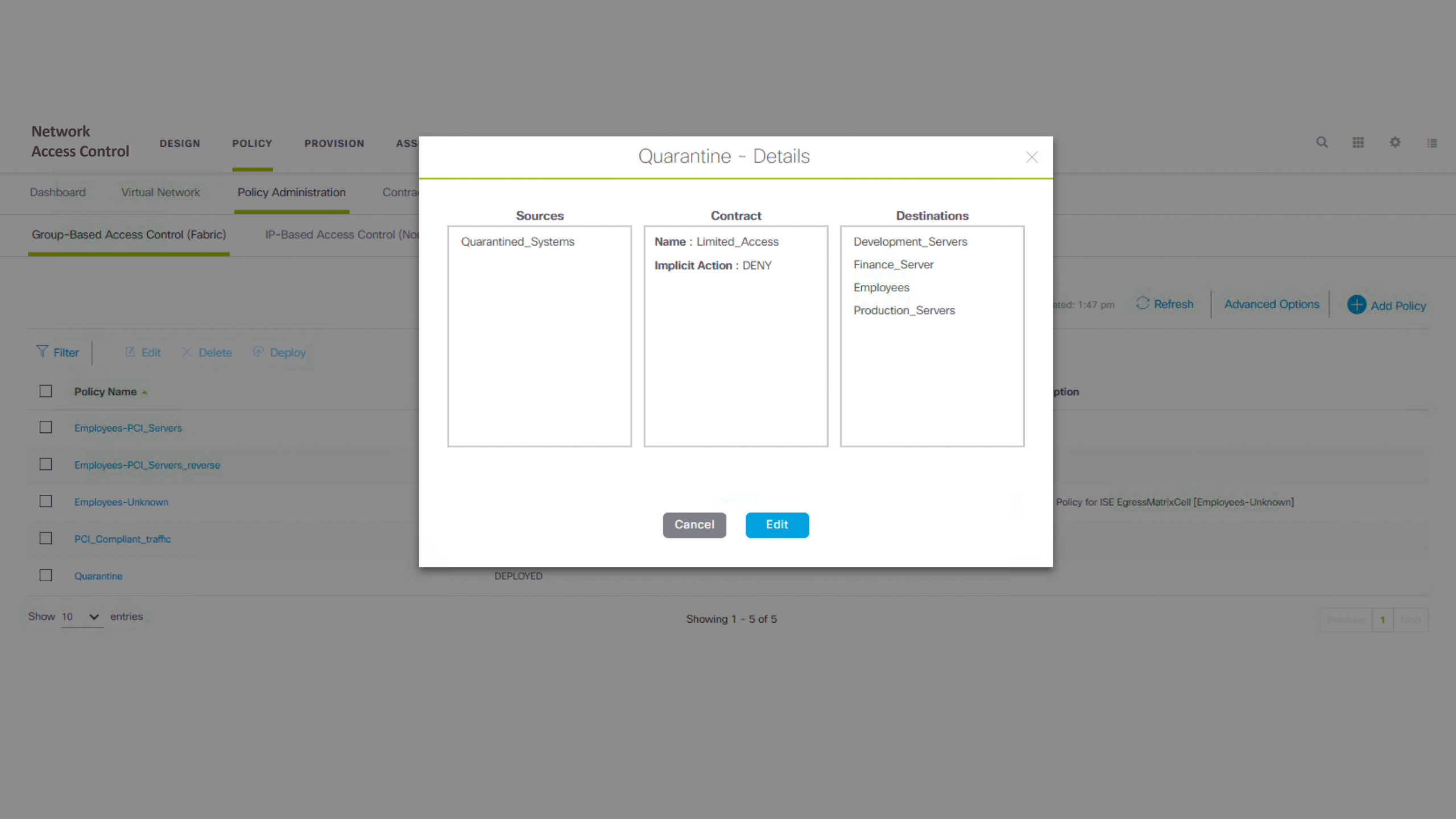
Deselect All Select All

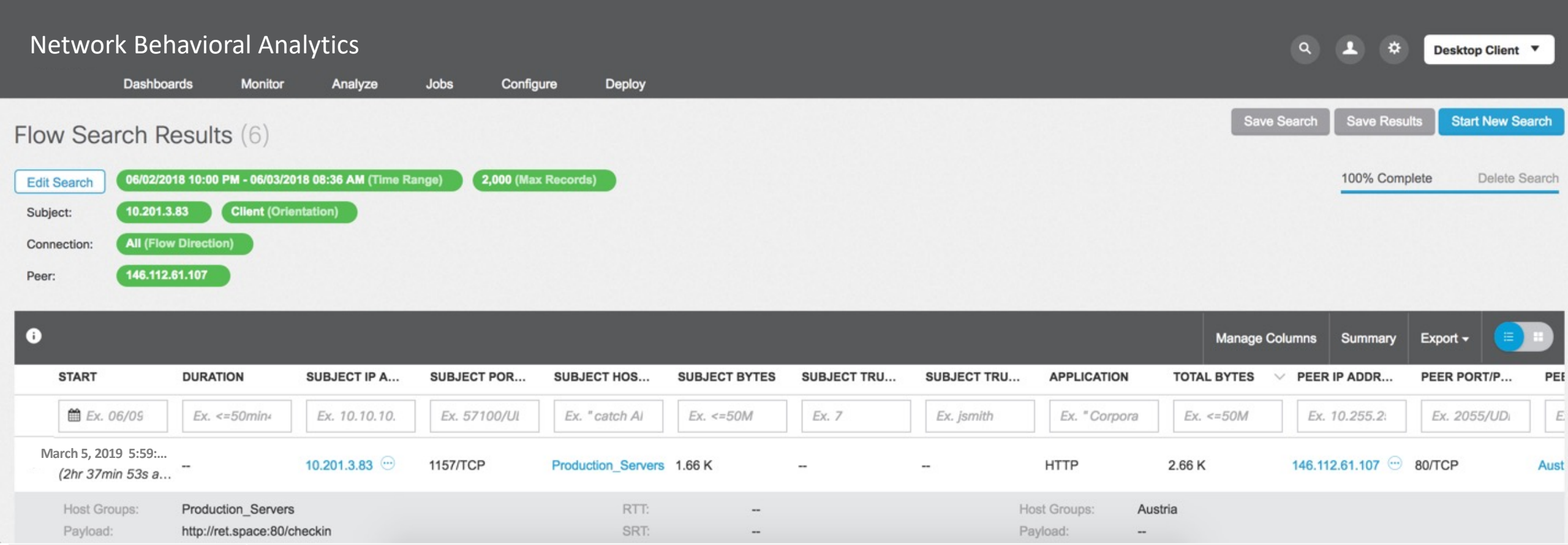
Quarantine Results

Cluster Name: ISE Simulator **Quarantine Result:** SUCCESS

Show Details

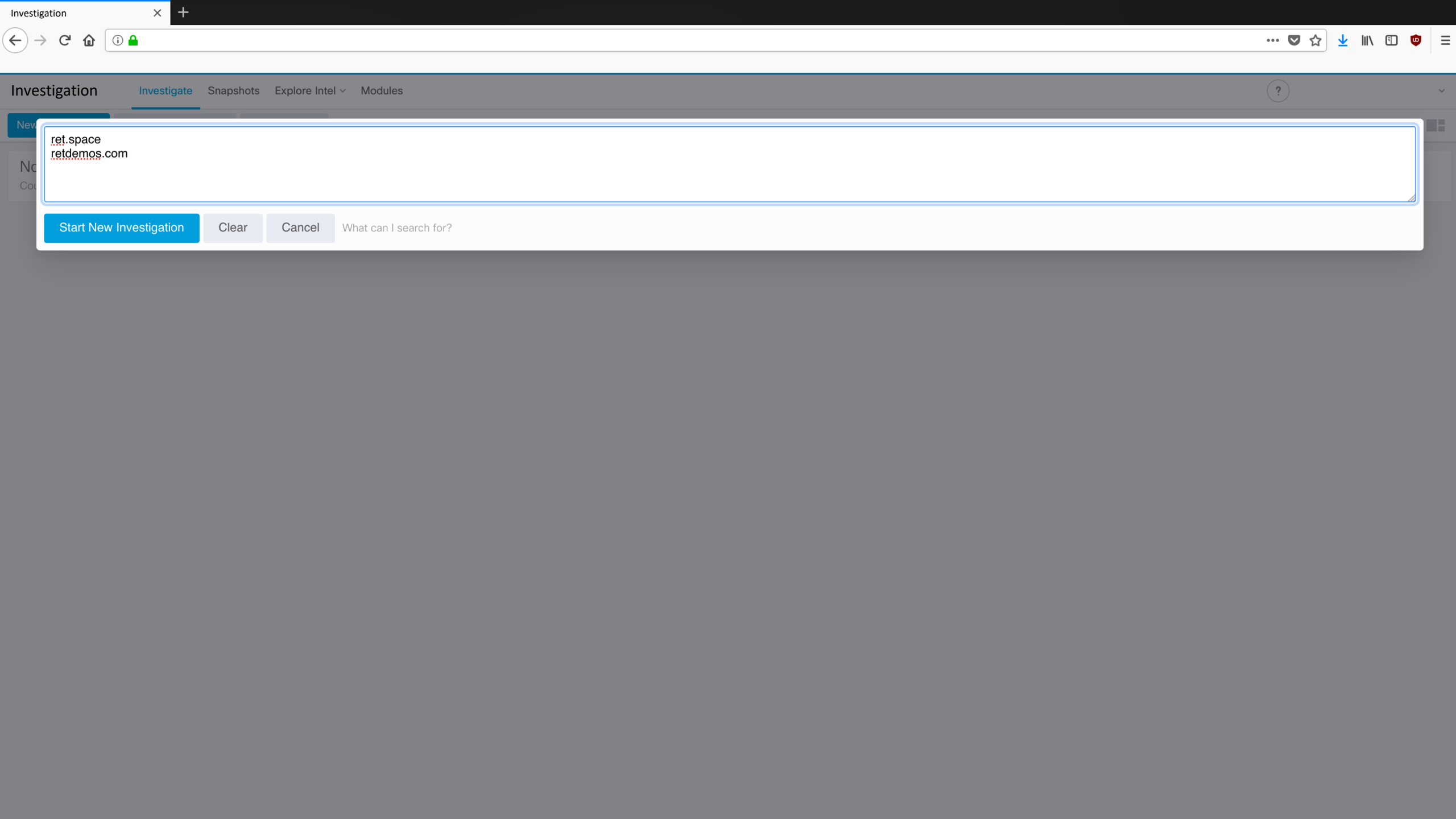
Ok


Network Access Control
DESIGN
POLICY
PROVISION
Dashboard
Virtual Network
Policy Administration
Group-Based Access Control (Fabric)
IP-Based Access Control
Refresh
Advanced Options
Add Policy
Filter
Edit
Delete
Deploy
Policy Name
Employees-PCI_Servers
Employees-PCI_Servers_reverse
Employees-Unknown
PCI_Compliant_traffic
Quarantine
DEPLOYED
Policy for ISE EgressMatrixCell [Employees-Unknown]
Show 10 entries
Showing 1 - 5 of 5
Previous
1
Next
Quarantine - Details
Sources
Quarantined_Systems
Contract
Name : Limited_Access
Implicit Action : DENY
Destinations
Development_Servers
Finance_Server
Employees
Production_Servers
Cancel
Edit



Host Groups: Production_Servers

Payload: http://ret.space:80/checkin


Investigation
Investigation
Investigate
Snapshots
Explore Intel
Modules
ret.space
retdemos.com
Start New Investigation
Clear
Cancel
What can I search for?

Investigation

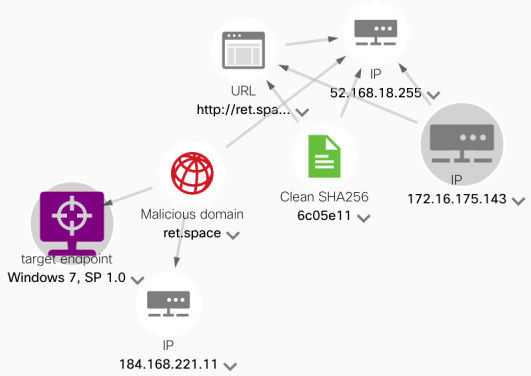
Investigation

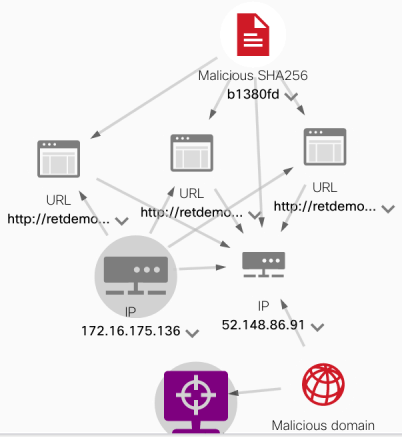
Investigate | Snapshots | Explore Intel | Modules

New Investigation | Edit This Investigation | Take Snapshot | 2 of 2 enrichments complete

2	2	2	2	0	0	0	5
Targets	Observables	Indicators	Domains	File Hashes	IP Addresses	URLs	Modules

Relations Graph





Observables

ret.space
Malicious Domain
Last seen on March 5th, 2019, in My Environment

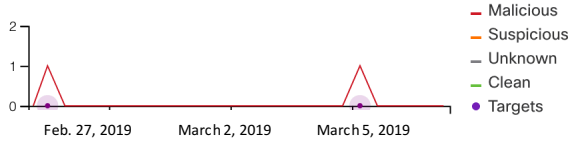
retdemos.com
Malicious Domain
Last seen on March 5th, 2019, in My Environment

ret.space

Malicious Domain

My Environment | Global

2 Sightings in My Environment
First: Feb 27th, 2019
Last: March 5th, 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

Sightings Timeline

Investigation

Investigation | Investigate | Snapshots

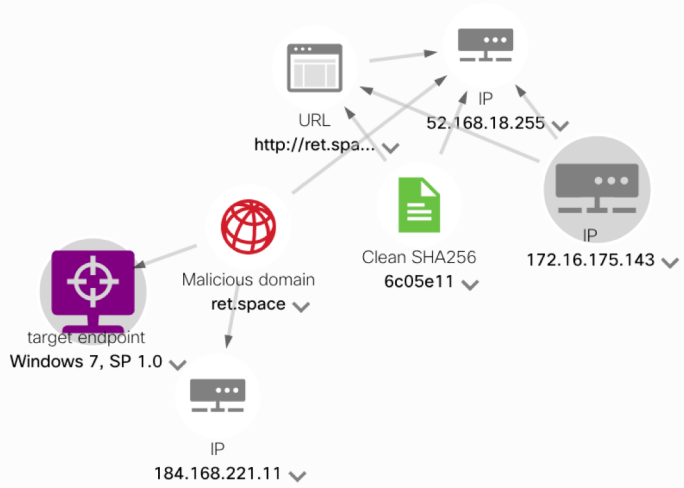
New Investigation | Edit This Investigation | Ta

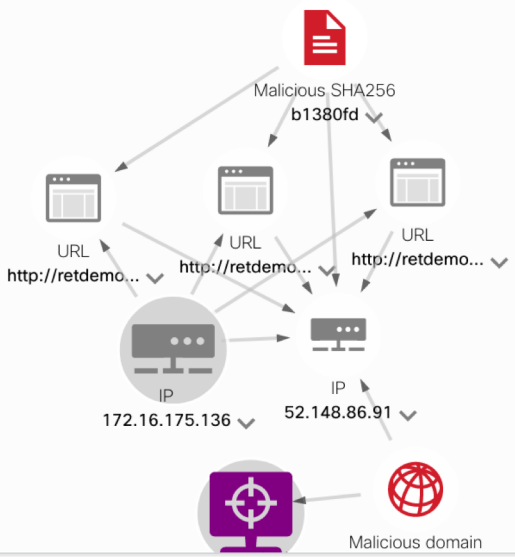
2 Targets

5 Modules

Relations Graph

Relations Graph





Malicious
Suspicious
Unknown
Clean
Targets

March 2, 2019
March 5, 2019

licators (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

Sightings Timeline

Investigation

Observables

ret.space
Malicious Domain
Last seen on March 5th, 2019, in My Environment

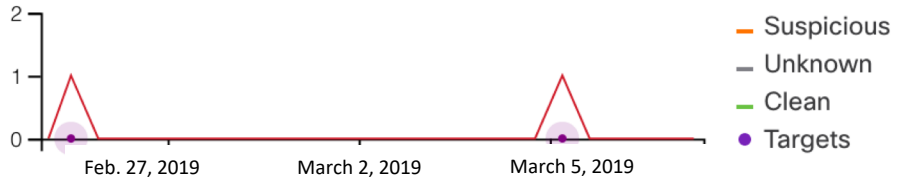
retdemos.com
Malicious Domain
Last seen on March 5th, 2019, in My Environment

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 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

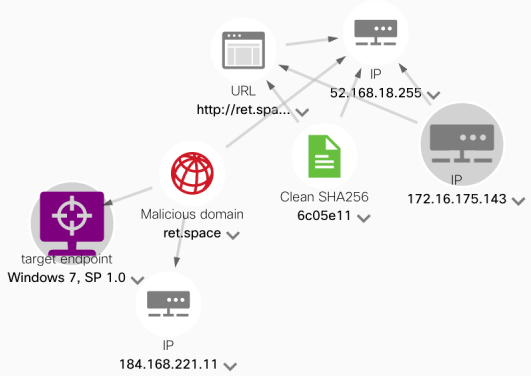
Investigation

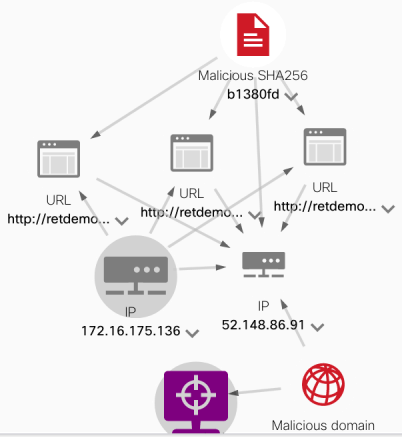
Investigate | Snapshots | Explore Intel | Modules

New Investigation | Edit This Investigation | Take Snapshot | 2 of 2 enrichments complete

2	2	2	2	0	0	0	5
Targets	Observables	Indicators	Domains	File Hashes	IP Addresses	URLs	Modules

Relations Graph





Observables

ret.space
Malicious Domain
Last seen on March 5th, 2019, in My Environment

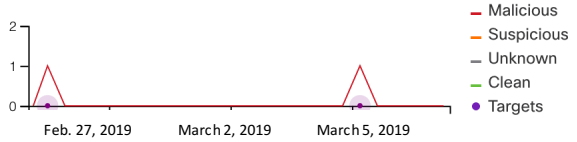
retdemos.com
Malicious Domain
Last seen on March 5th, 2019, in My Environment

ret.space

Malicious Domain

My Environment | Global

2 Sightings in My Environment
First: Feb 27th, 2019
Last: March 5th, 2019

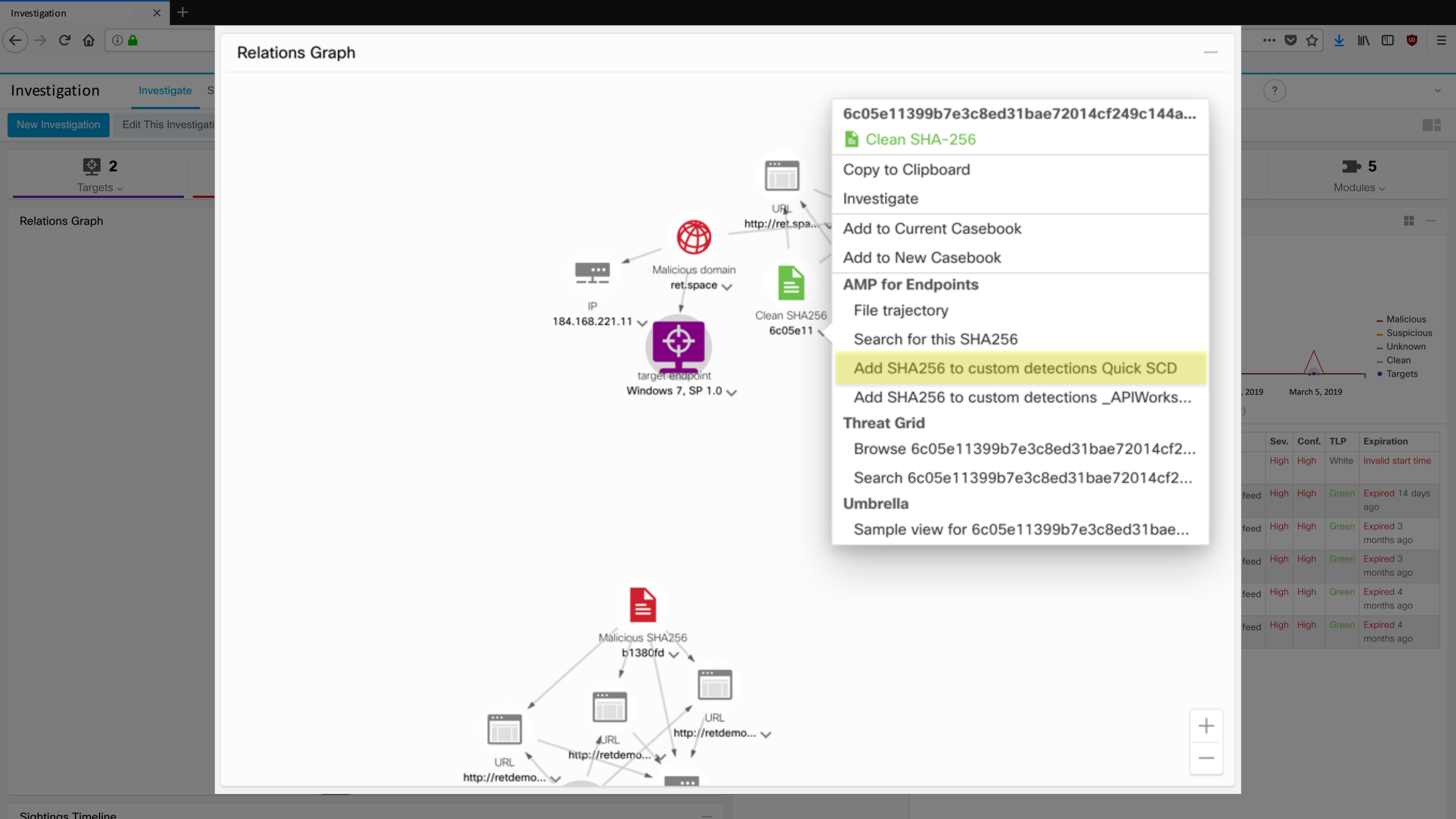


Judgements (18) | Verdicts (2) | Sightings (103) | Indicators (2)

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

Sightings Timeline


Relations Graph
6c05e11399b7e3c8ed31bae72014cf249c144a...
Clean SHA-256
Copy to Clipboard
Investigate
Add to Current Casebook
Add to New Casebook
AMP for Endpoints
File trajectory
Search for this SHA256
Add SHA256 to custom detections Quick SCD
Add SHA256 to custom detections _APIWorks...
Threat Grid
Browse 6c05e11399b7e3c8ed31bae72014cf2...
Search 6c05e11399b7e3c8ed31bae72014cf2...
Umbrella
Sample view for 6c05e11399b7e3c8ed31bae...
URL
http://ret.spa...
Malicious domain
ret.space
IP
184.168.221.11
target endpoint
Windows 7, SP 1.0
Clean SHA256
6c05e11
Malicious SHA256
b1380fd
URL
http://retdemo...
URL
http://retdemo...
URL
http://retdemo...
URL
http://retdemo...

InfoSec-Collab

InfoSec Administrator

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.

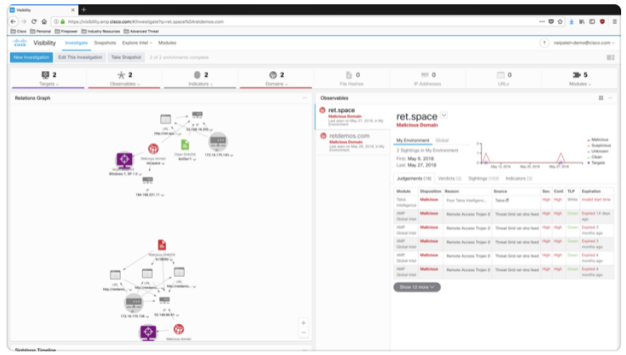
Only visible to you

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.

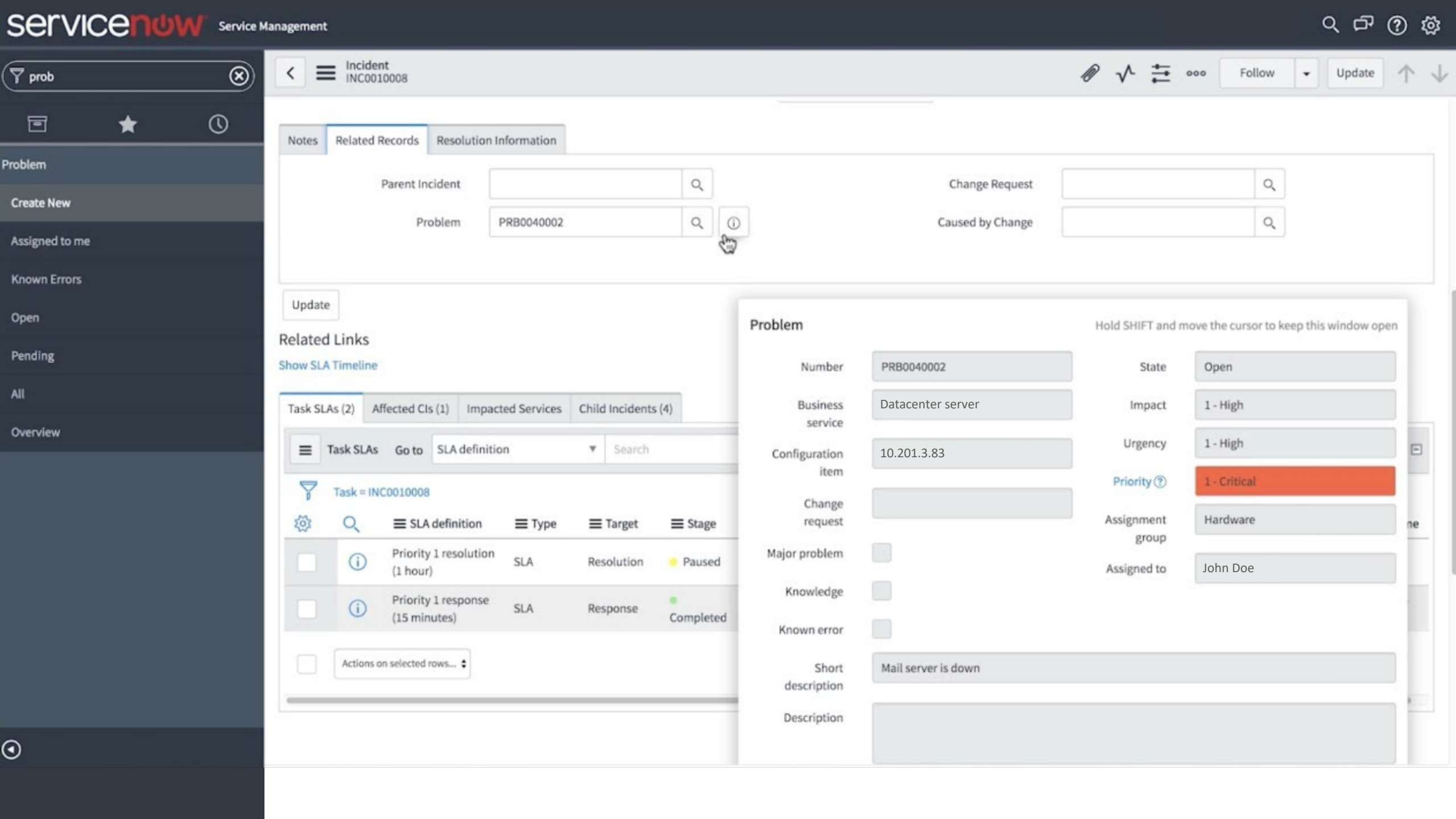
Right now — even if you don't have teammates in Slack yet — you can set the stage for conversation in #secops. Sending a message or sharing a file will give your teammates something to respond to when they arrive.

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!

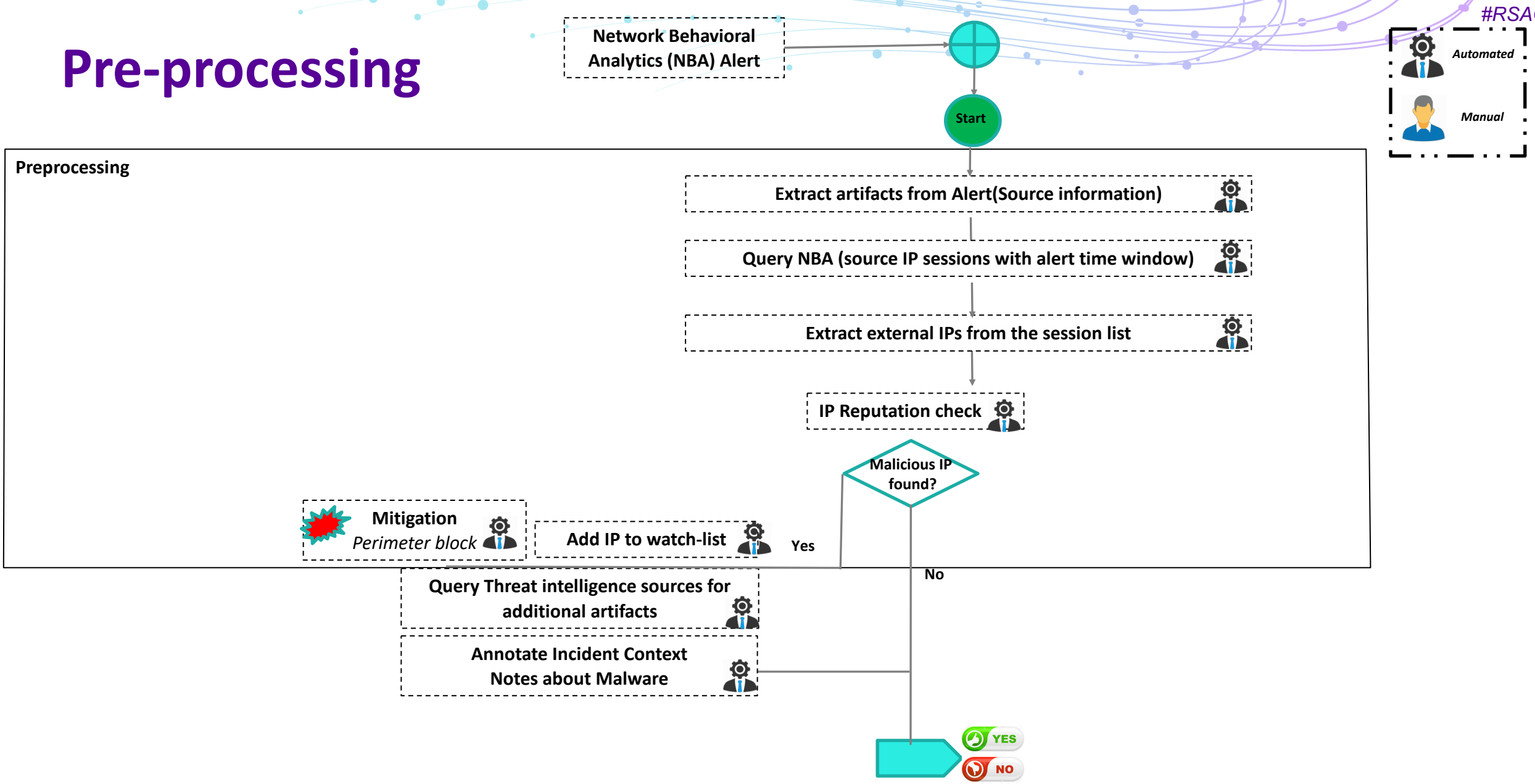


Message #secops

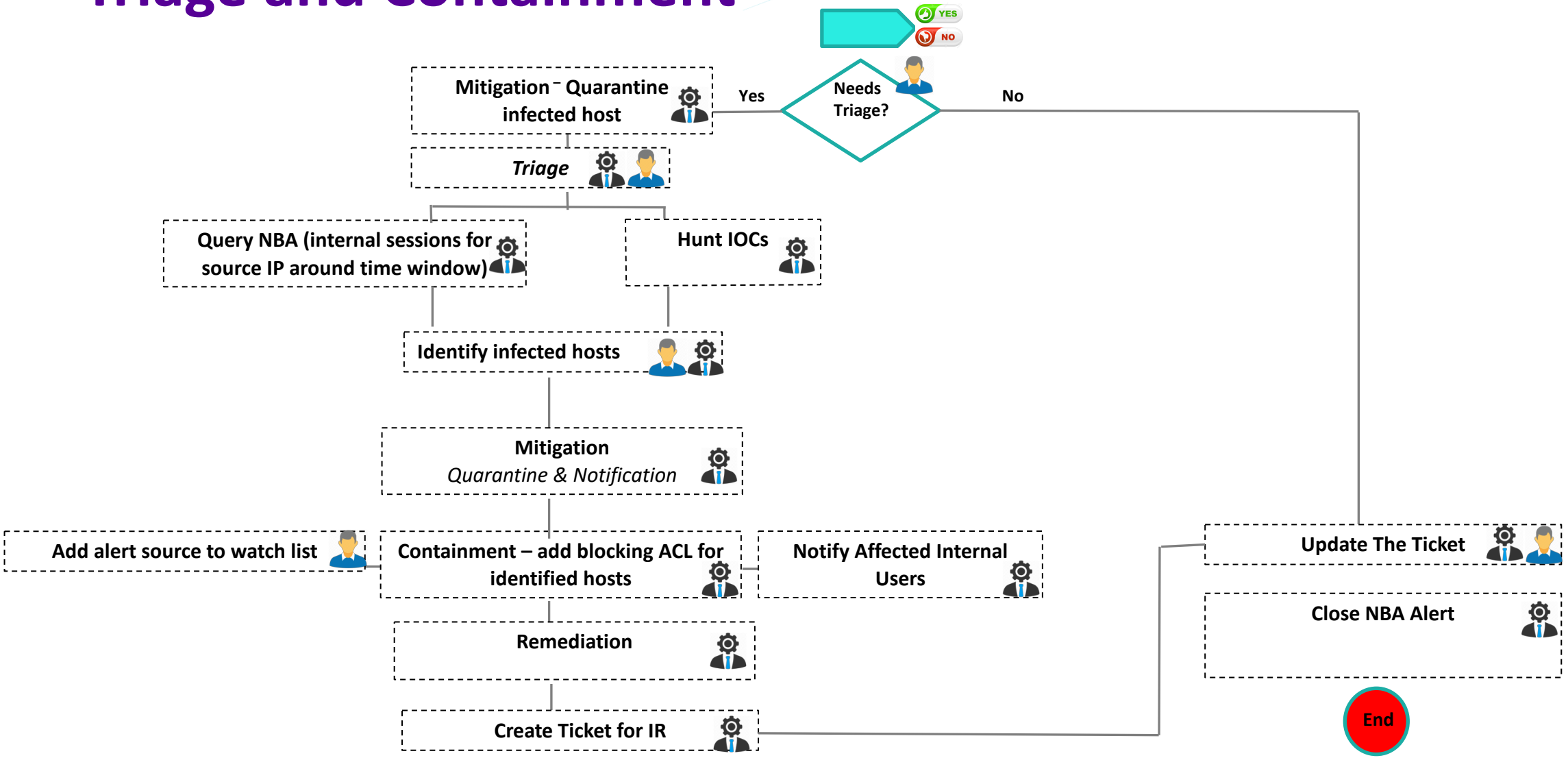

servicenow Service Management
prob
Problem
Create New
Assigned to me
Known Errors
Open
Pending
All
Overview
Incident
INC0010008
Follow
Update
Notes
Related Records
Resolution Information
Parent Incident
Problem
PRB0040002
Change Request
Caused by Change
Update
Related Links
Show SLA Timeline
Task SLAs (2)
Affected CIs (1)
Impacted Services
Child Incidents (4)
Task SLAs
Go to
SLA definition
Search
Task = INC0010008
SLA definition
Type
Target
Stage
Priority 1 resolution (1 hour)
SLA
Resolution
Paused
Priority 1 response (15 minutes)
SLA
Response
Completed
Actions on selected rows...
Problem
Hold SHIFT and move the cursor to keep this window open
Number
PRB0040002
Business service
Datacenter server
Configuration item
10.201.3.83
Change request
Major problem
Knowledge
Known error
Short description
Mail server is down
Description
State
Open
Impact
1 - High
Urgency
1 - High
Priority
1 - Critical
Assignment group
Hardware
Assigned to
John Doe

Automated Playbook
Detection, Containment and Remediation

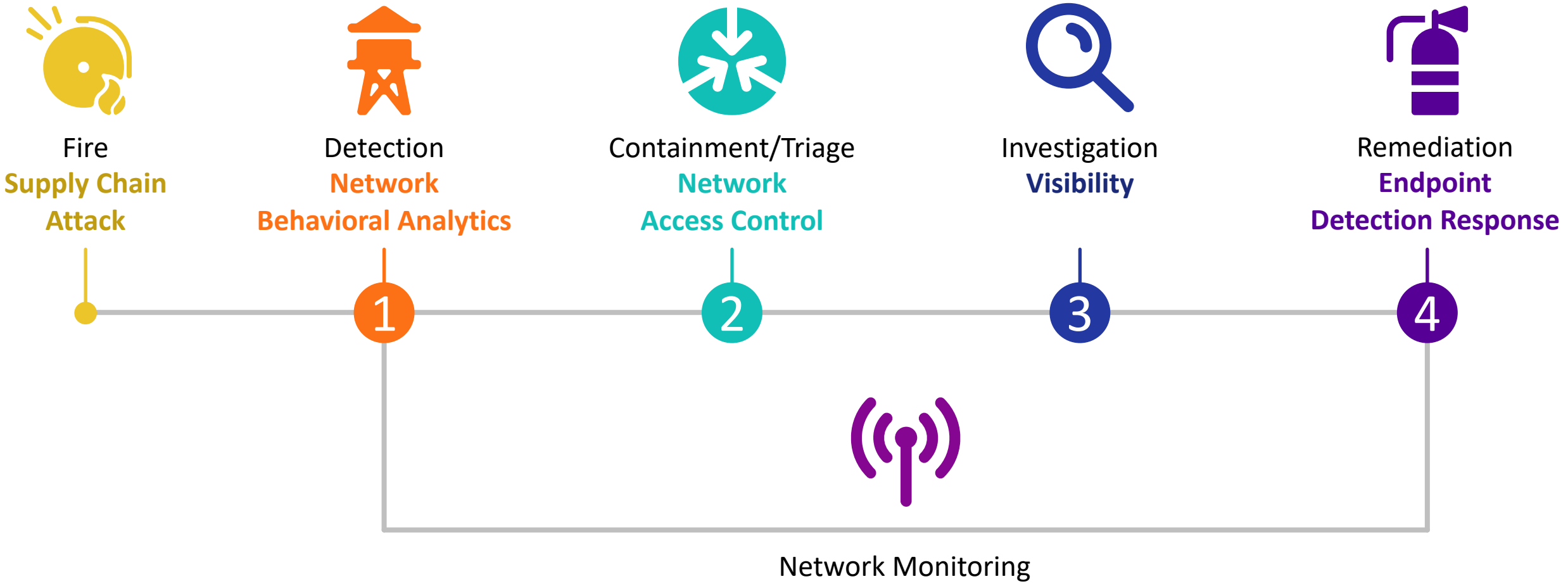
Pre-processing



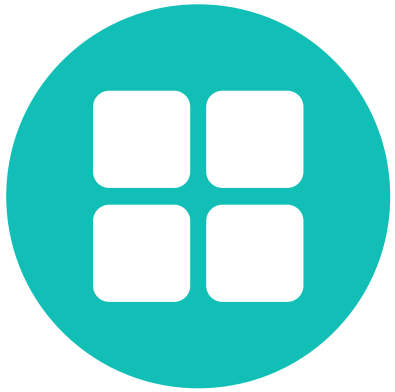
Triage and Containment



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?

RSAConference2019

Thank you.

How to Support Fire Victims

American Red Cross
www.redcross.org