Best Practices for Rapid Containment of Incidents

Noam Syrkin
Sr. Technical Marketing Engineer, RedSeal

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

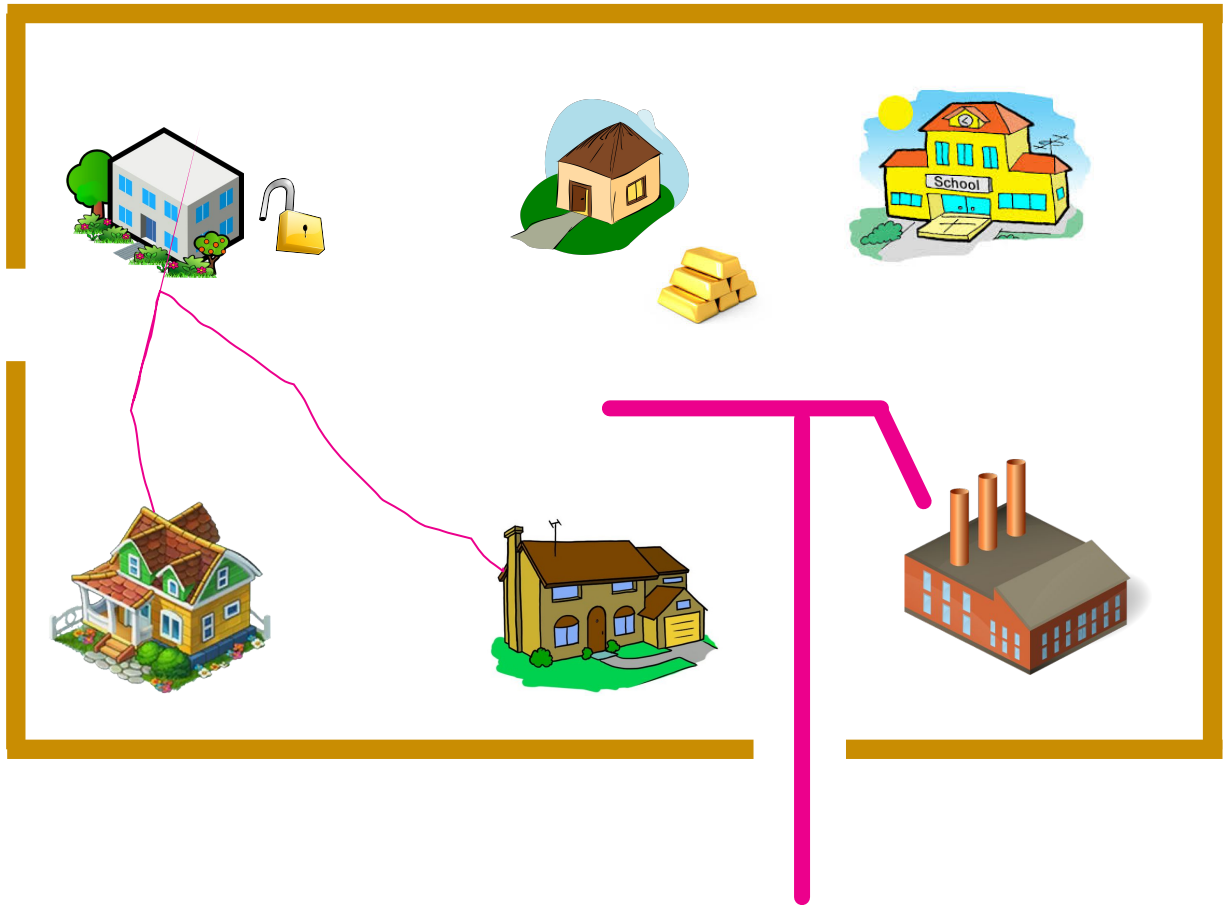
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- The importance of network terrain
- The shifting terrain
- Splunk ES and RedSeal
- Summary
- Q&A

Defending a City

What do you need to know?



What is in the city?

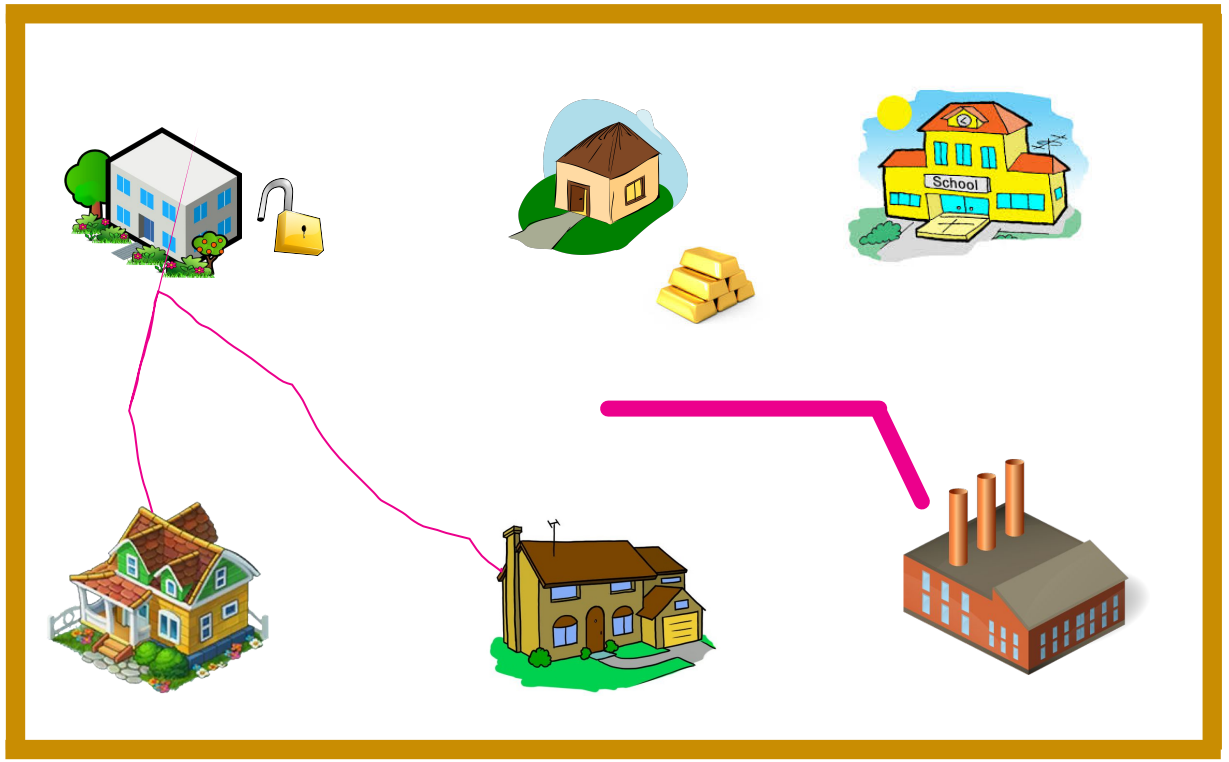
Where is the valuable stuff?

How would attacker get in?

How would the attacker move around?

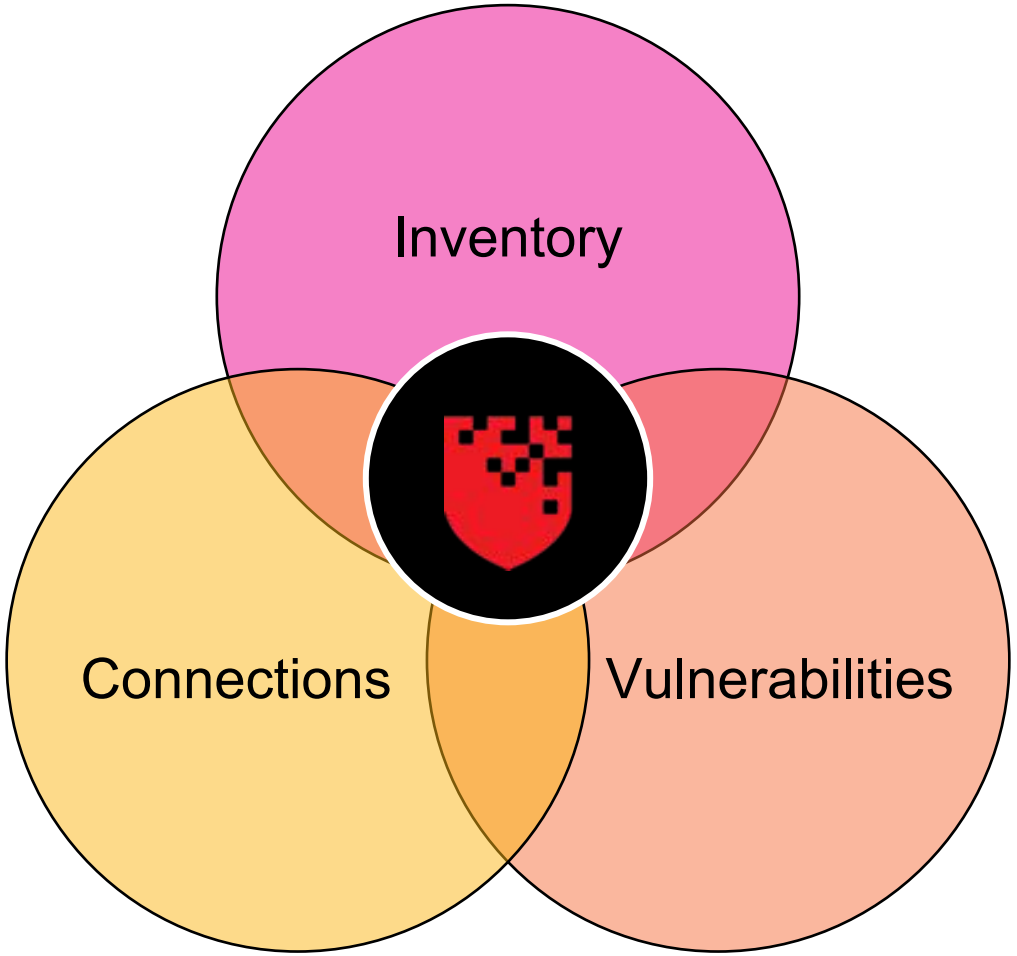
How We Try to Identify Cyber Terrain Today…

- What is in the city?
  - Hosts, routers, switches, firewalls, etc.
  - CMDB
  - Vulnerability Scans
  - Endpoint Protection
- Where is the valuable stuff?
  - Data Discovery
  - Tagging
  - Tribal knowledge?
- How would an attacker get in?
  - Security Awareness
  - Pen Testing
- How would an attacker move around?
  - Traceroute, Ping
  - Live Traffic



RedSeal Helps You Understand All Your Cyber Terrain

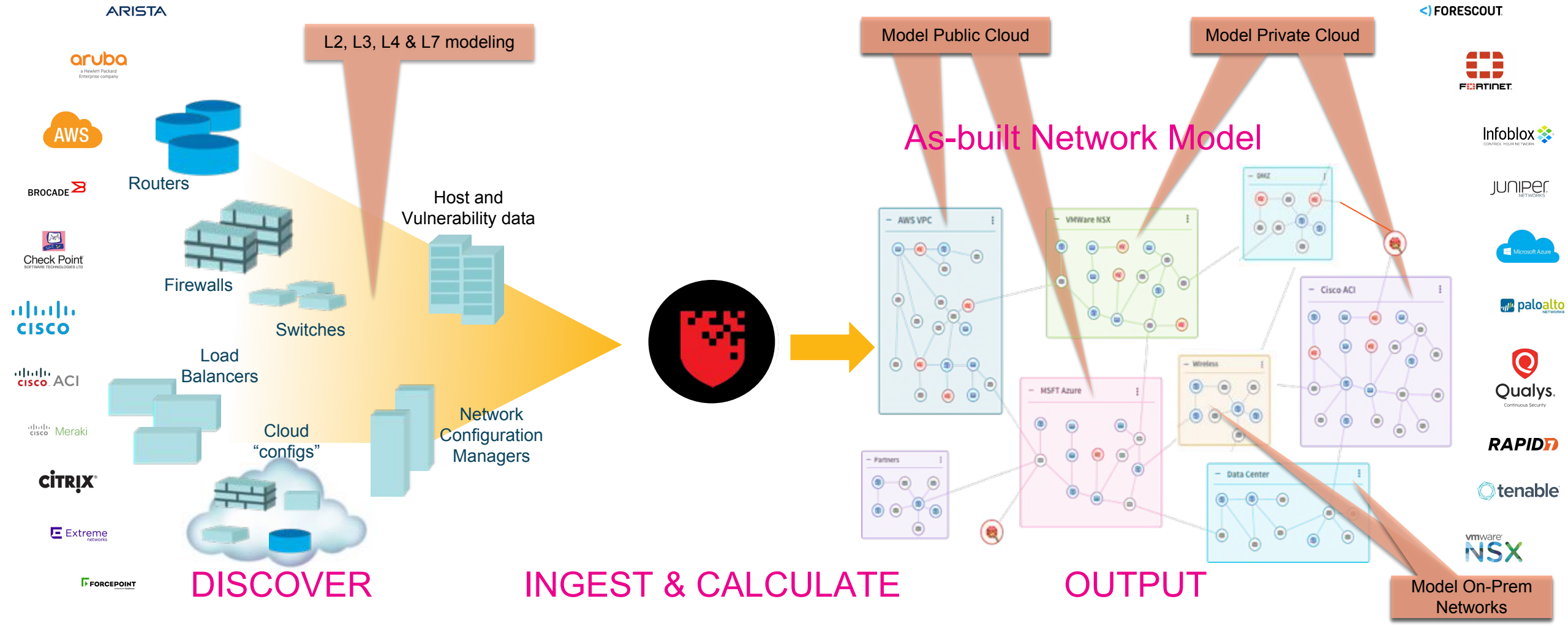
Across public cloud, SDN and physical environments



Knowing what you have and how it's all connected

The Platform

Ingest Information to Create a Model



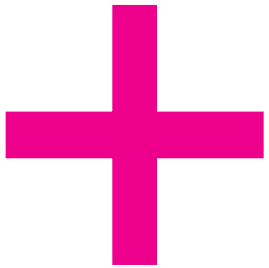
splunk> .conf19

The Shifting Terrain

.conf19
splunk>

Why Is The Terrain Shifting?

- ✔ Software defined everything
- ✔ Digital transformation
- ✔ Hybrid datacenters
- ✔ Internet of things
- ✔ Shadow IT



Skills Shortage

82%

of global IT leaders report significant labor shortages in cybersecurity

Source | April 2016
TechCrunch CIO Report

What Should Be One Integrated World …

Is Really a Complex Ecosystem

Your Fabric

F5, Check Point Software Technologies Ltd., Huawei, Aruba Networks, Alcatel-Lucent, Brocade, Cisco, Fortinet, Juniper Networks, Arista, Palo Alto Networks

Cloud & SDN

Amazon Web Services, Microsoft Azure, VMware

Security Technologies

Infoblox, HP ArcSight, IBM Radar, Lockpath, RSA Archer GRC, tenable network security, Intel Security, RAPID7, Agiliance, Qualys, solarwinds, beyondtrust, tripwire, Symantec, ForeScout, splunk>

Network Engineers
Access & Policy

Security Auditor
Audit & Compliance

Security Engineers
Prioritization & Speed

splunk> .conf19

With Serious Gaps

Your Fabric

Cloud & SDN

Separate Worlds

Incomplete Information

Too Many Interfaces

Security Technologies

Network Engineers
Access & Policy

Security Auditor
Audit & Compliance

Security Engineers
Prioritization & Speed

Splunk + RedSeal

Minimizing the time to contain incidents

.conf19

splunk>

Integration with RedSeal

Observe
Point Products → Orient
Analytics → Decision Making → Acting

Understand your network terrain

Valuable Threat Source Data

Where is it located?
Both logically and physically?
What other assets can it reach?
What is the access path and the source to the target?

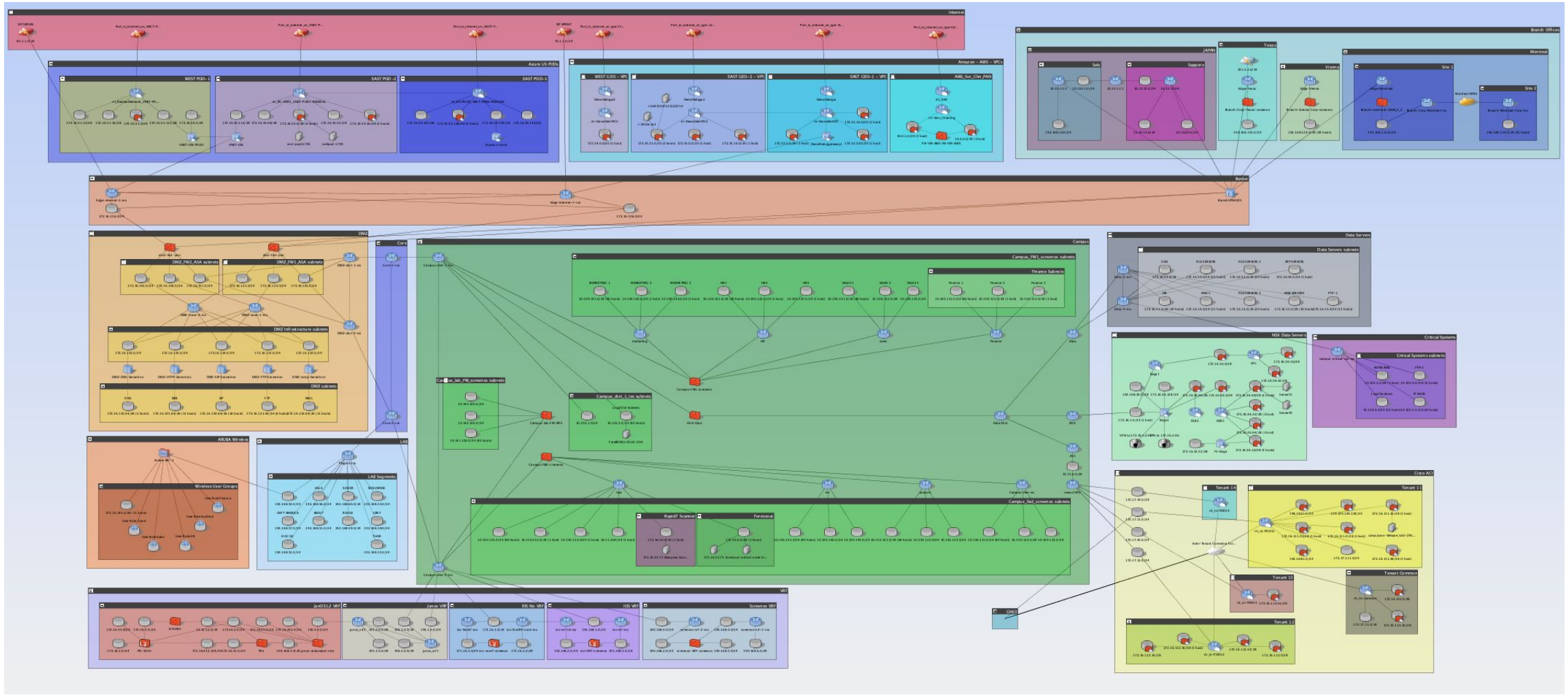
Accelerate Containment

Model & Understand Hybrid Environments

Bring all your assets into one place…

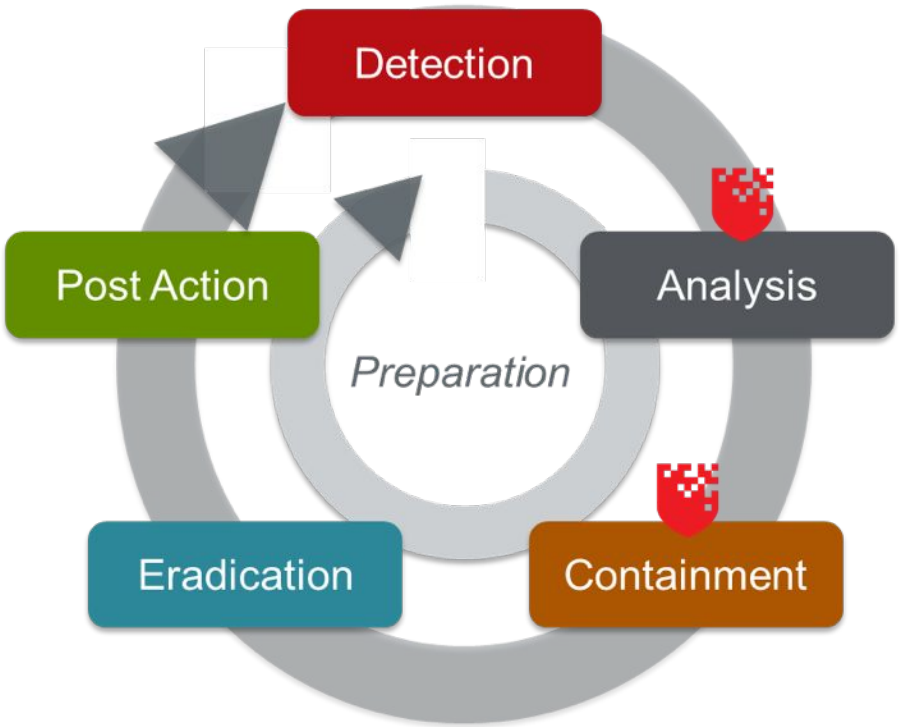
Model & Understand Hybrid Environments

Bring all your assets into one place…



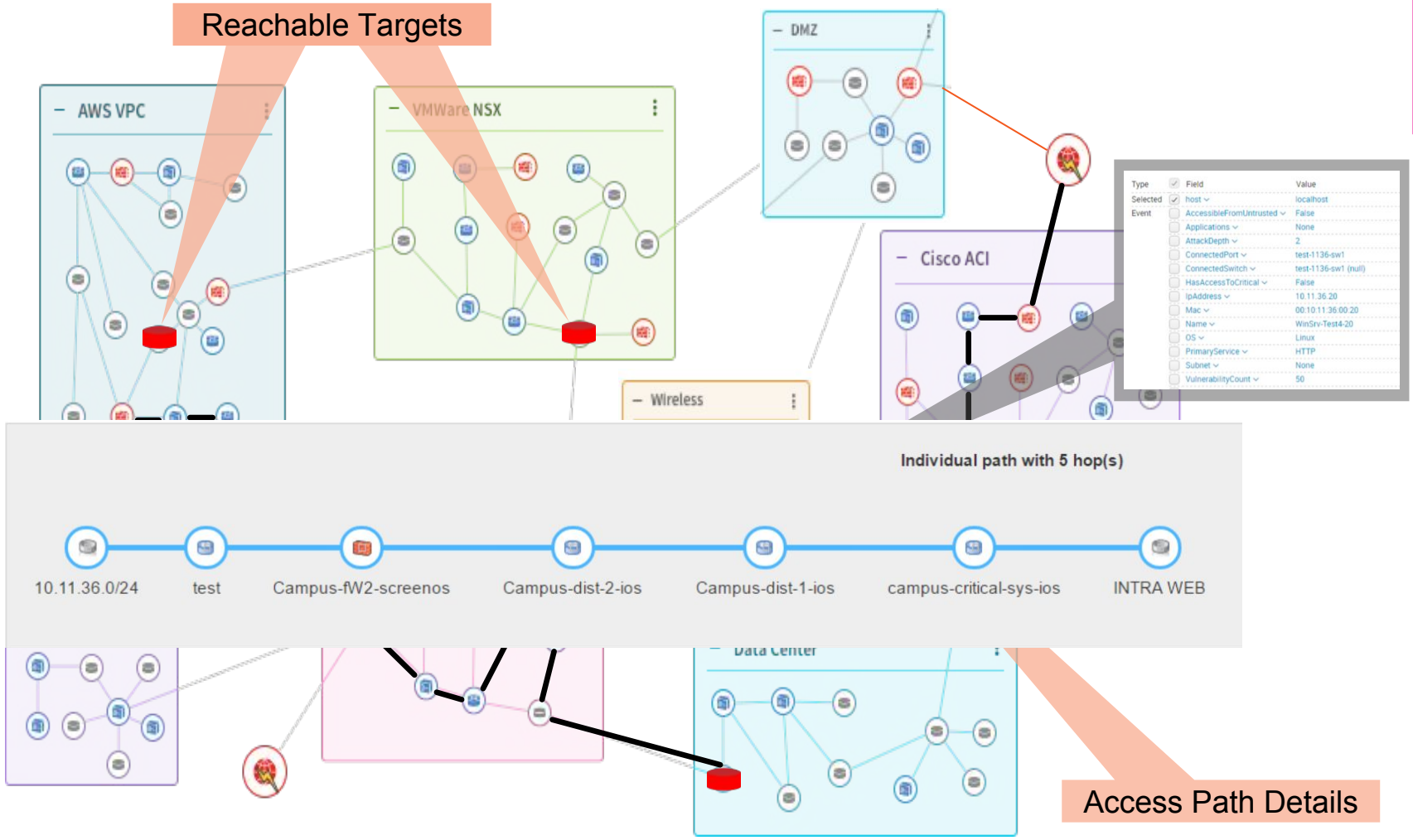
Incident Investigation

A threat is detected, now what?



- Top 4 questions:
  - What are the details of Threat Source?
  - Where is it located? Both logically and physically?
  - What other assets can it reach?
  - What is the access path and the devices from Threat source to the destination target?
- Can you answer these questions within minutes?

How does RedSeal Help?



1. Model and understand hybrid environments, compute access paths
2. Rapidly provide data on IoC – location, OS, services, switch port, etc.
3. Identify top reachable target groups
4. Details on access path and devices along the path
5. Identified all needed information to implement containment of IoC

splunk> .conf19

Incident Review

Urgency

CRITICAL	5
HIGH	119
MEDIUM	556
LOW	0
INFO	0

Status: × All

Name:

Owner: × All

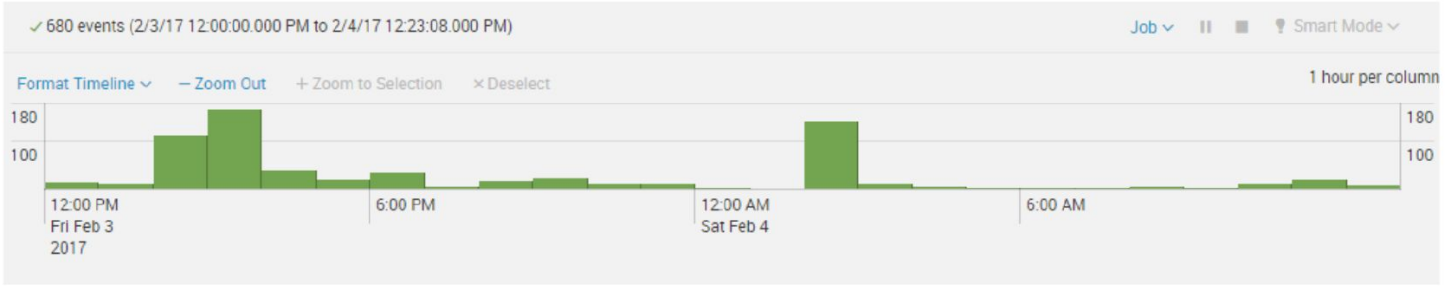
Search:

Security Domain: × All

Time: Last 24 hours

Tag:

Submit



Edit Selected | Edit All 680 Matching Events | Add Selected to Investigation

« prev 1 2 3 4 5 6 7 8 9 10 next »

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	2/3/17 9:10:52.000 PM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.11.36.20	Critical	New	unassigned	
>	2/3/17 6:10:33.000 PM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.20	Critical	New	unassigned	
>	2/3/17 4:10:39.000 PM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.20	Critical	New	unassigned	
>	2/3/17 2:10:43.000 PM	Network	Abnormally High Number of HTTP POST Request Events By 10.12.34.56	Critical	New	unassigned	
>	2/3/17 2:10:43.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.11.36.20	Critical	New	unassigned	
>	2/4/17 11:10:32.000 AM	Network	Abnormally High Number of HTTP CONNECT Request Events By 192.168.3.153	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.9	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.8	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.8	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.7	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.6	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.6	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.5	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.5	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.40	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.40	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.4	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.39	High	New	unassigned	
>	2/4/17 2:10:31.000 AM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.39	High	New	unassigned	

splunk> App: Enterprise Security | Administrator | 3 Messages | Settings | Activity | Help | Find

Security Posture | Incident Review | My Investigations | Glass Tables | Security Intelligence | Security Domains | Audit | Search | Configure | Enterprise Security

Incident Review

Urgency

CRITICAL	5
HIGH	119
MEDIUM	556
LOW	0
INFO	0

Status: × All

Name:

Owner: × All

Search:

Security Domain: × All

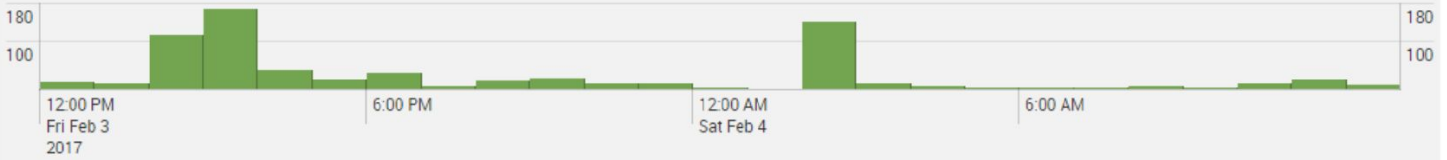
Time: Last 24 hours

Tag:

Submit

✓ 680 events (2/3/17 12:00:00.000 PM to 2/4/17 12:23:08.000 PM) Job | Smart Mode

Format Timeline | − Zoom Out | + Zoom to Selection | × Deselect | 1 hour per column



Edit Selected | Edit All 680 Matching Events | Add Selected to Investigation

« prev 1 2 3 4 5 6 7 8 9 10 next »

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
	2/3/17 9:10:52.000 PM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.11.36.20	Critical	New	unassigned	

Description:

A system (10.11.36.20) was detected as generating an abnormally high number of CONNECT request events.

Additional Fields	Value	Action
HTTP Method	CONNECT	
Source	10.11.36.20 240	
Source Business Unit	americas	
Source Category	pci	
	splunk	
Source City	Pleasanton	
Source Country	USA	
Source IP Address	10.11.36.20	
Source Expected	true	
Source Latitude	37.694452	
Source Longitude	-121.894461	
Source Owner	Bill_williams	
Source PCI Domain	trust	
Source Requires Antivirus	false	
Source Should Time Synchronize	true	
Source Should Update	true	

IoC IP Address

Event Details:

Correlation Search:

Web - Abnormally High Number of HTTP Method Events By Src - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View Web Activity on 10.11.36.20

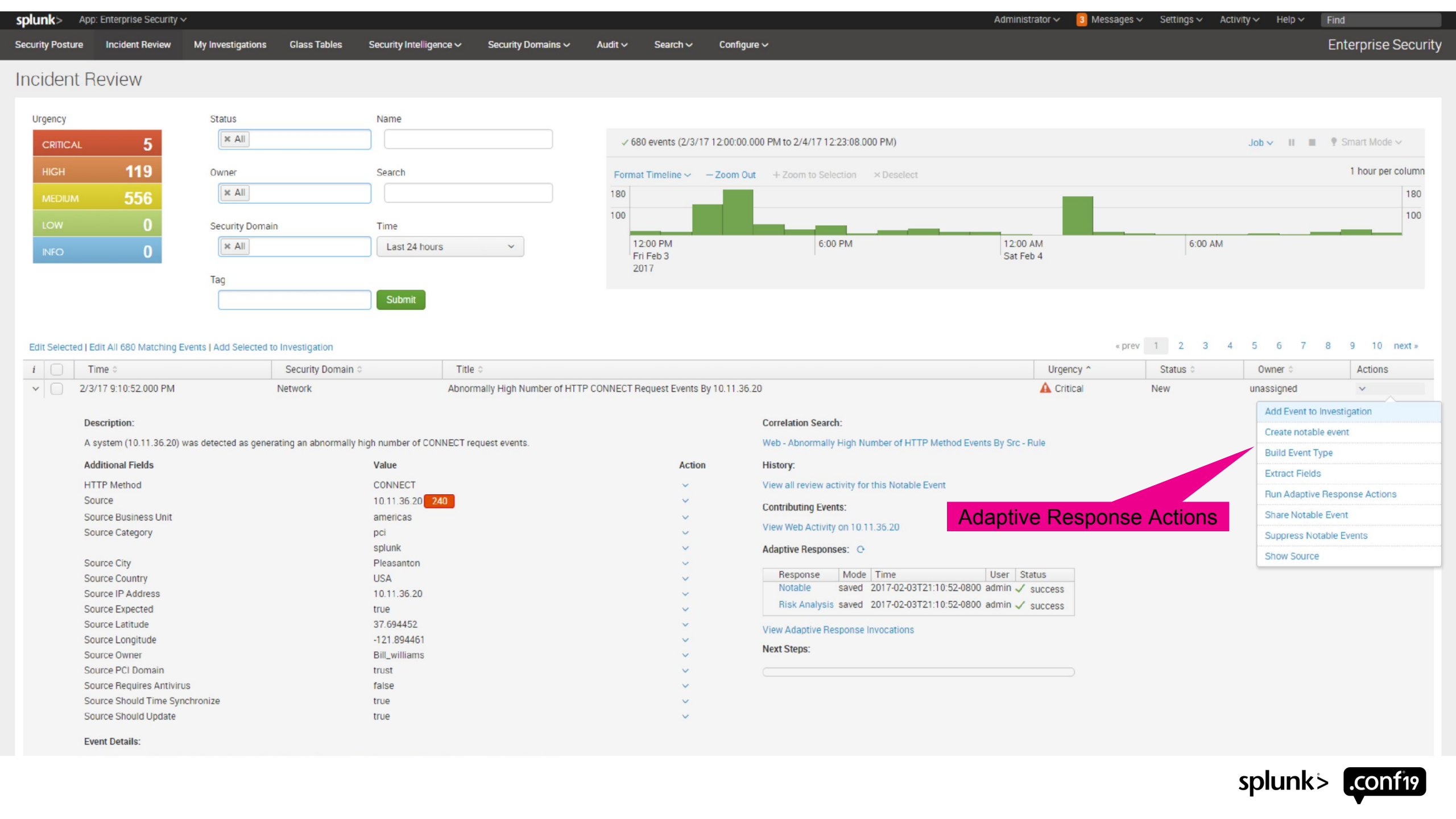
Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2017-02-03T21:10:52-0800	admin	✓ success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	✓ success

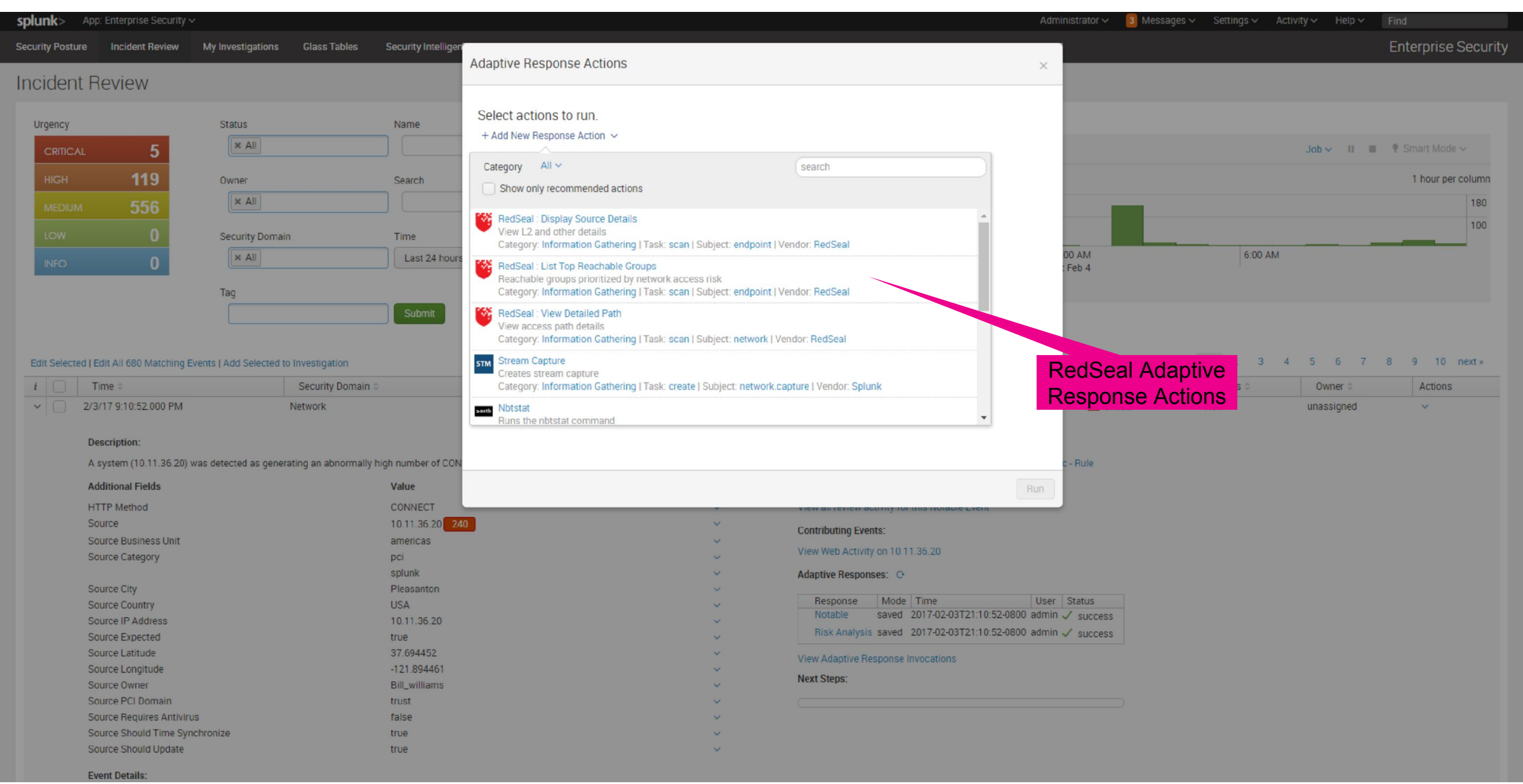
View Adaptive Response Invocations

Next Steps:

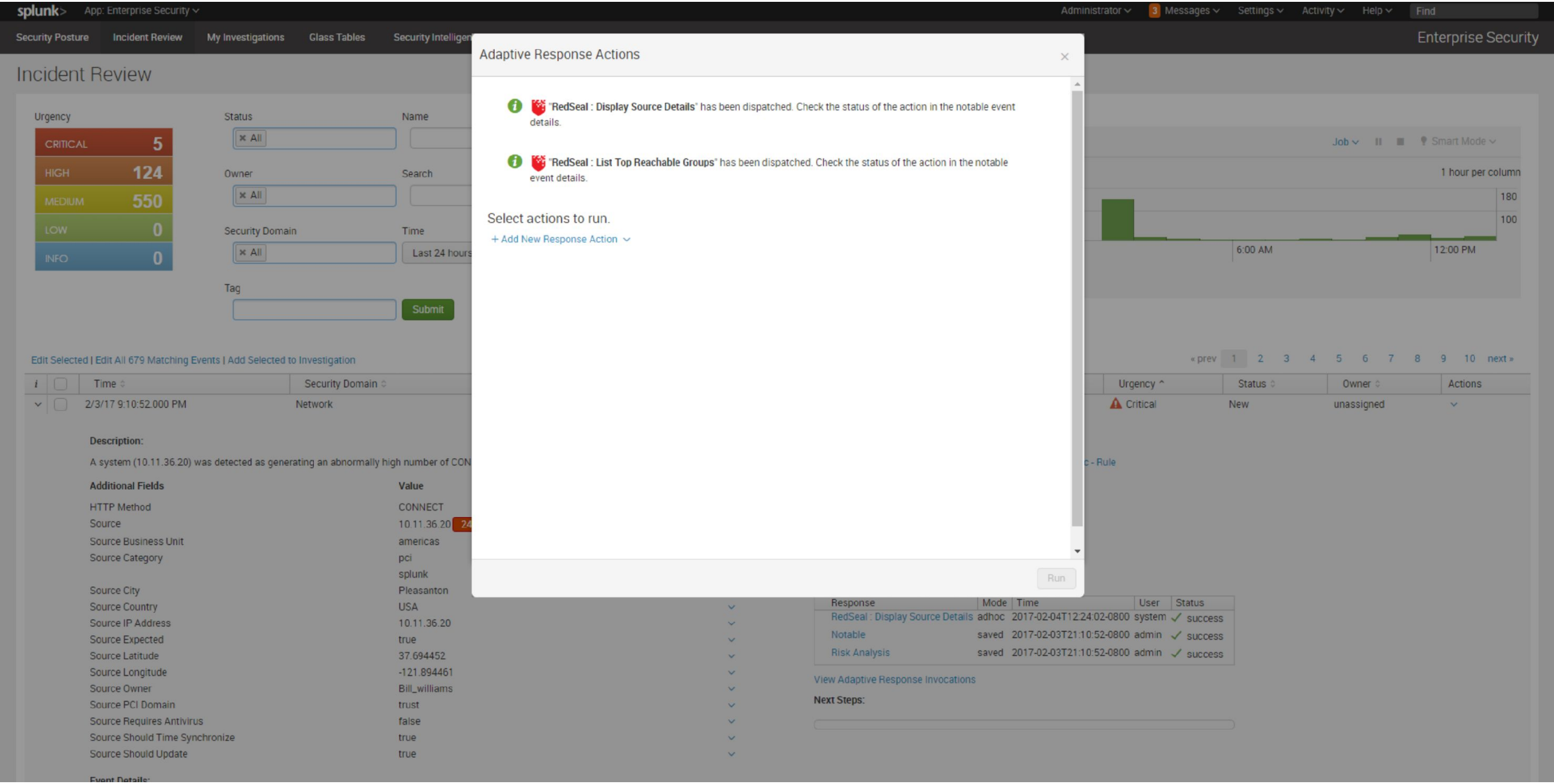
splunk> .conf19



splunk> .conf19



splunk> .conf19



splunk> .conf19

Incident Review

Urgency

CRITICAL	5
HIGH	124
MEDIUM	550
LOW	0
INFO	0

Status: × All

Name:

Owner: × All

Search:

Security Domain: × All

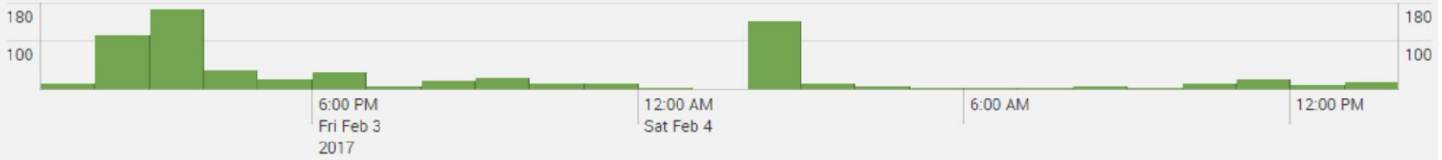
Time: Last 24 hours

Tag:

Submit

✓ 679 events (2/3/17 1:00:00.000 PM to 2/4/17 1:30:54.000 PM) Job | Smart Mode

Format Timeline | − Zoom Out | + Zoom to Selection | × Deselect | 1 hour per column



Edit Selected | Edit All 679 Matching Events | Add Selected to Investigation

« prev 1 2 3 4 5 6 7 8 9 10 next »

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
	2/3/17 9:10:52.000 PM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.11.36.20	Critical	New	unassigned	

Description:

A system (10.11.36.20) was detected as generating an abnormally high number of CONNECT request events.

Additional Fields	Value	Action
HTTP Method	CONNECT	
Source	10.11.36.20 240	
Source Business Unit	americas	
Source Category	pci	
	splunk	
Source City	Pleasanton	
Source Country	USA	
Source IP Address	10.11.36.20	
Source Expected	true	
Source Latitude	37.694452	
Source Longitude	-121.894461	
Source Owner	Bill_williams	
Source PCI Domain	trust	
Source Requires Antivirus	false	
Source Should Time Synchronize	true	
Source Should Update	true	

Event Details:

Correlation Search:

Web - Abnormally High Number of HTTP Method Events By Src - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View Web Activity on 10.11.36.20

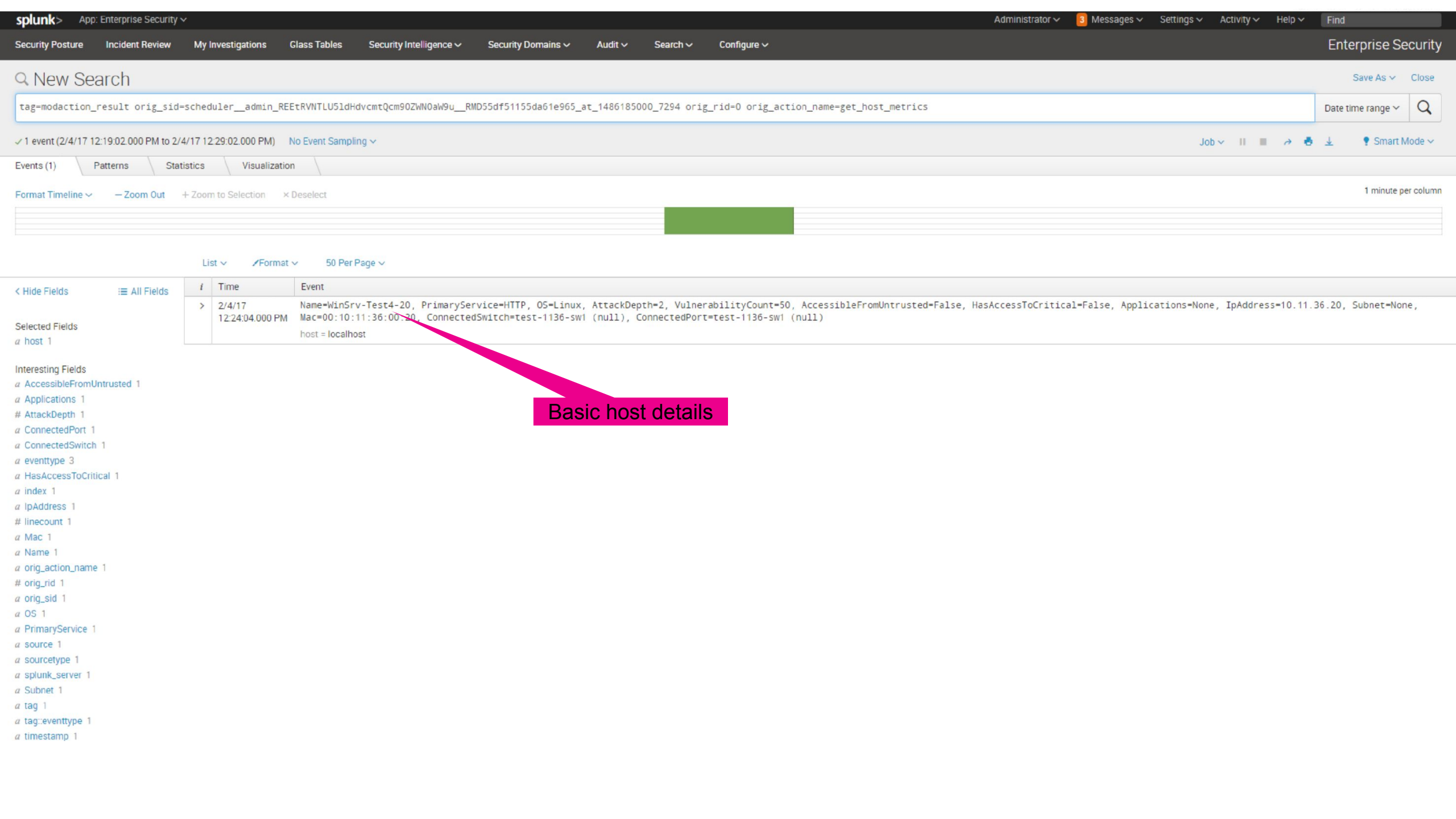
Adaptive Responses:

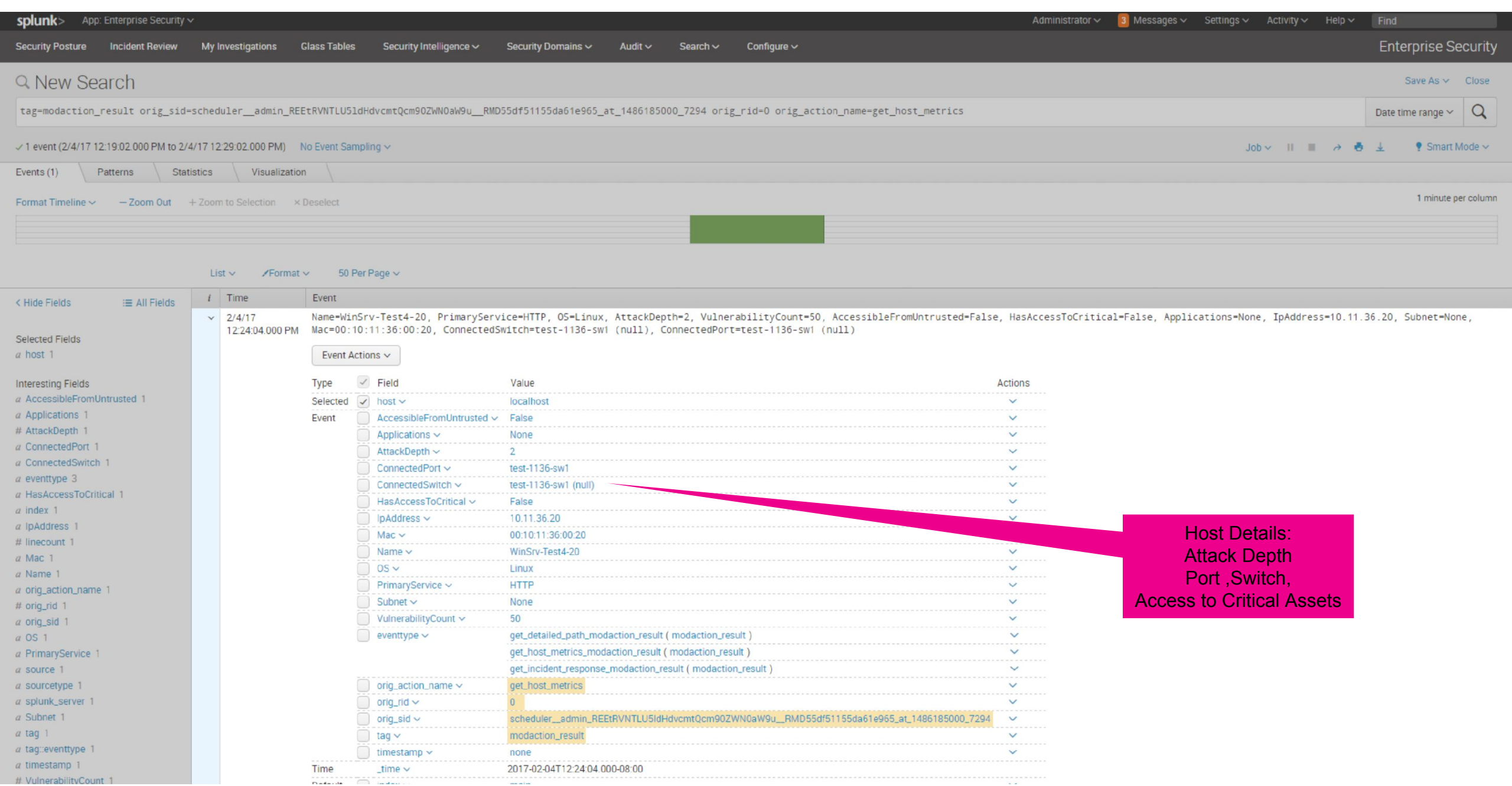
Response	Mode	Time	User	Status
RedSeal : List Top Reachable Groups	adhoc	2017-02-04T13:43:32-0800	system	✓ success
RedSeal : Display Source Details	adhoc	2017-02-04T12:24:02-0800	system	✓ success
Notable	saved	2017-02-03T21:10:52-0800	admin	✓ success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	✓ success

View Adaptive Response Invocations

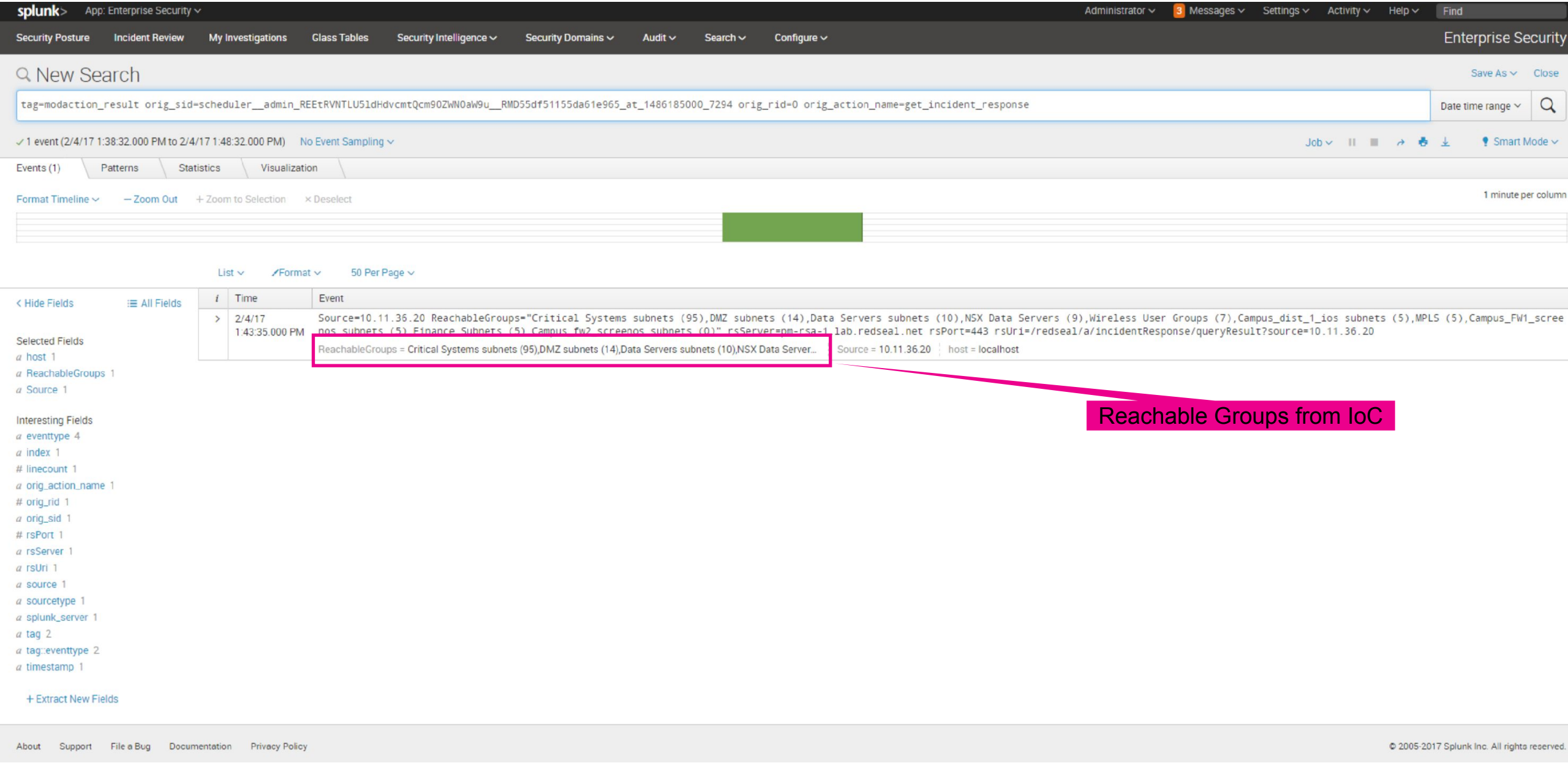
Next Steps:

RedSeal AR Reports


splunk> App: Enterprise Security
Administrator
3 Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
My Investigations
Glass Tables
Security Intelligence
Security Domains
Audit
Search
Configure
Enterprise Security
New Search
Save As
Close
tag=modaction_result orig_sid=scheduler__admin_REEtRVNTLU5ldHdvcmtQcm90ZWNOaW9u__RMD55df51155da61e965_at_1486185000_7294 orig_rid=0 orig_action_name=get_host_metrics
Date time range
✓ 1 event (2/4/17 12:19:02.000 PM to 2/4/17 12:29:02.000 PM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 minute per column
List
Format
50 Per Page
Hide Fields
All Fields
Time
Event
2/4/17 12:24:04.000 PM
Name=WinSrv-Test4-20, PrimaryService=HTTP, OS=Linux, AttackDepth=2, VulnerabilityCount=50, AccessibleFromUntrusted=False, HasAccessToCritical=False, Applications=None, IpAddress=10.11.36.20, Subnet=None, Mac=00:10:11:36:00:20, ConnectedSwitch=test-1136-sw1 (null), ConnectedPort=test-1136-sw1 (null)
host = localhost
Selected Fields
a host 1
Interesting Fields
a AccessibleFromUntrusted 1
a Applications 1
AttackDepth 1
a ConnectedPort 1
a ConnectedSwitch 1
a eventtype 3
a HasAccessToCritical 1
a index 1
a IpAddress 1
linecount 1
a Mac 1
a Name 1
a orig_action_name 1
orig_rid 1
a orig_sid 1
a OS 1
a PrimaryService 1
a source 1
a sourcetype 1
a splunk_server 1
a Subnet 1
a tag 1
a tag::eventtype 1
a timestamp 1
Basic host details

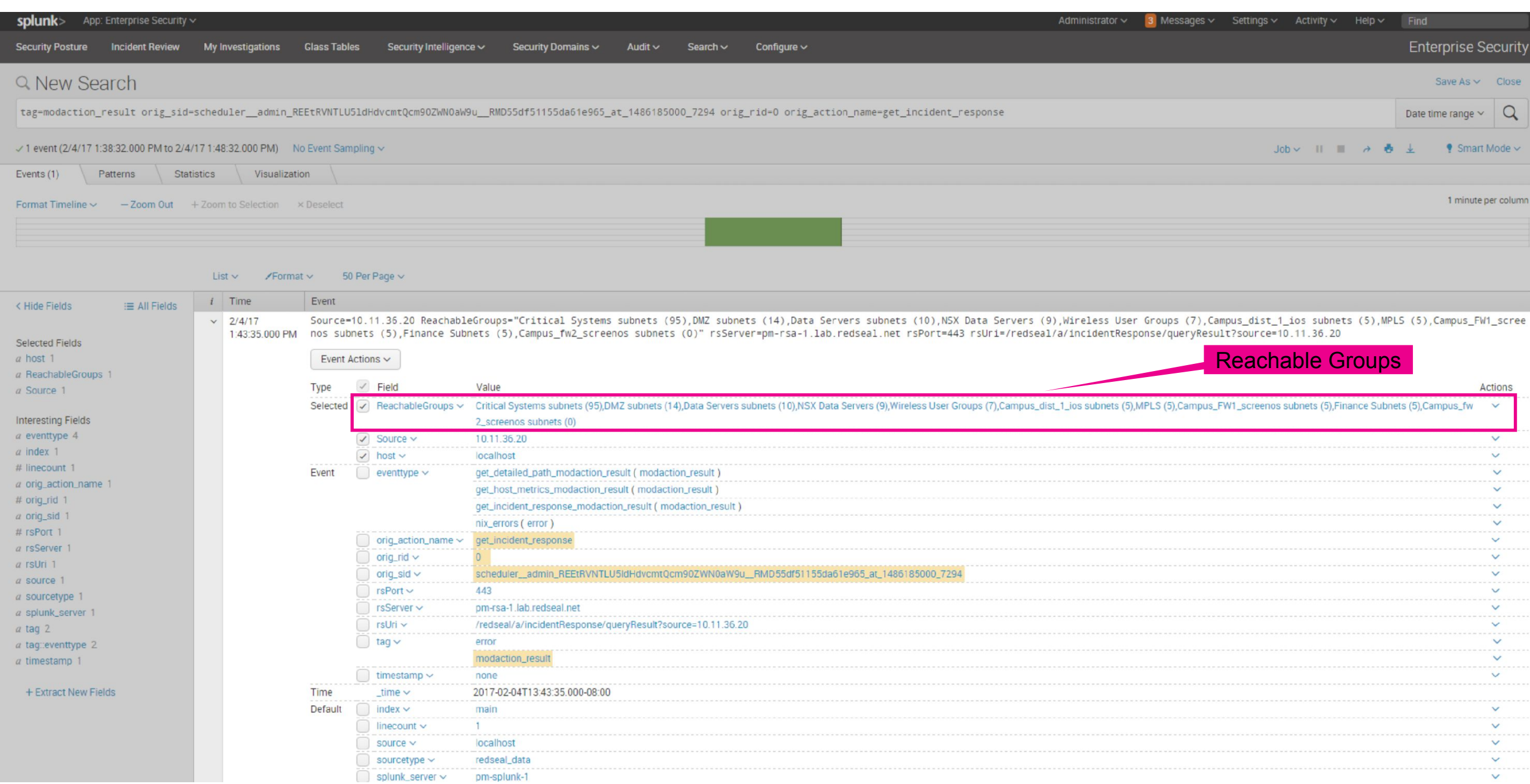


splunk> .conf19

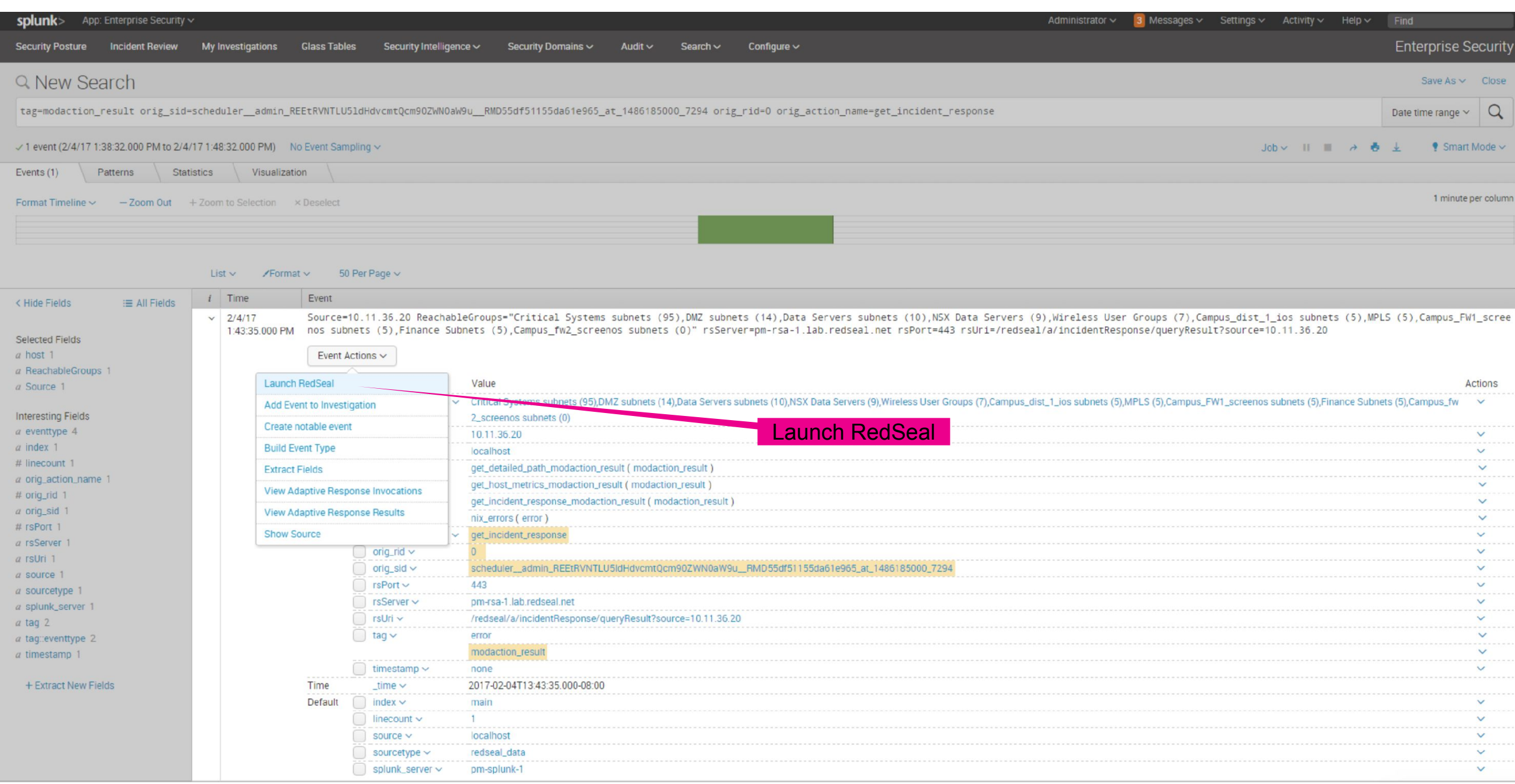


Reachable Groups from IoC

splunk> .conf19



splunk> .conf19


splunk> App: Enterprise Security
Administrator 3 Messages Settings Activity Help Find
Security Posture Incident Review My Investigations Glass Tables Security Intelligence Security Domains Audit Search Configure
Enterprise Security
New Search
Save As Close
tag=modaction_result orig_sid=scheduler__admin_REEtRVNTLU5ldHdvcmtQcm90ZWN0aW9u__RMD55df51155da61e965_at_1486185000_7294 orig_rid=0 orig_action_name=get_incident_response
Date time range
1 event (2/4/17 1:38:32.000 PM to 2/4/17 1:48:32.000 PM) No Event Sampling
Job Smart Mode
Events (1) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect
1 minute per column
List Format 50 Per Page
Hide Fields All Fields
Selected Fields
a host 1
a ReachableGroups 1
a Source 1
Interesting Fields
a eventtype 4
a index 1
linecount 1
a orig_action_name 1
orig_rid 1
a orig_sid 1
rsPort 1
a rsServer 1
a rsUri 1
a source 1
a sourcetype 1
a splunk_server 1
a tag 2
a tag::eventtype 2
a timestamp 1
Extract New Fields
Time
Event
2/4/17 1:43:35.000 PM
Source=10.11.36.20 ReachableGroups="Critical Systems subnets (95),DMZ subnets (14),Data Servers subnets (10),NSX Data Servers (9),Wireless User Groups (7),Campus_dist_1_ios subnets (5),MPLS (5),Campus_FW1_screenos subnets (5),Finance Subnets (5),Campus_fw2_screenos subnets (0)" rsServer=pm-rsa-1.lab.redseal.net rsPort=443 rsUri=/redseal/a/incidentResponse/queryResult?source=10.11.36.20
Event Actions
Launch RedSeal
Add Event to Investigation
Create notable event
Build Event Type
Extract Fields
View Adaptive Response Invocations
View Adaptive Response Results
Show Source
Value
Actions
Launch RedSeal
Critical Systems subnets (95),DMZ subnets (14),Data Servers subnets (10),NSX Data Servers (9),Wireless User Groups (7),Campus_dist_1_ios subnets (5),MPLS (5),Campus_FW1_screenos subnets (5),Finance Subnets (5),Campus_fw
2_screenos subnets (0)
10.11.36.20
localhost
get_detailed_path_modaction_result (modaction_result)
get_host_metrics_modaction_result (modaction_result)
get_incident_response_modaction_result (modaction_result)
nix_errors (error)
get_incident_response
orig_rid 0
orig_sid scheduler__admin_REEtRVNTLU5ldHdvcmtQcm90ZWN0aW9u__RMD55df51155da61e965_at_1486185000_7294
rsPort 443
rsServer pm-rsa-1.lab.redseal.net
rsUri /redseal/a/incidentResponse/queryResult?source=10.11.36.20
tag error
modaction_result
timestamp none
Time _time 2017-02-04T13:43:35.000-08:00
Default index main
linecount 1
source localhost
sourcetype redseal_data
splunk_server pm-splunk-1

REDSEAL

Launch Java App | Help | Logged in as: uiadmin

Control Center | Network Map | Network Access | Threats | Vulnerabilities | Configuration Issues | Security Impact | Detailed Path | Incident Response

Find Threat Source: 10.11.36.20

IP of IoC

Threat Source Overview

Host Information

Name: 10.11.36.20

Operating System: Linux

Applications: HTTPD, OpenSSH, rquotad, vsFTPd

What is it?

Groups

Policy Groups: Trusted, Campus_fw2_screenos subnets

Topology Groups:

Topology

IP Address: 10.11.36.20

Subnet: 10.11.36.0/24

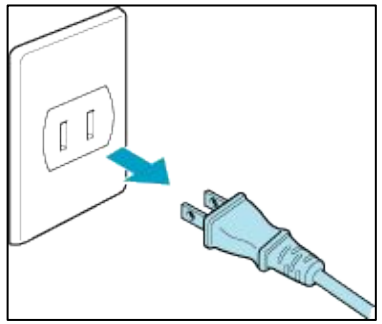
Layer 2 Location

MAC Address: 00:10:11:36:00:20

Connected Switch: test-1136-sw1 (null)

Connected Port: GigabitEthernet0/20

Where is it at?



Reachable Groups

Group	Value
Critical Systems subnets	95
DMZ subnets	14
Data Servers subnets	10
NSX Data Servers	9
Wireless User Groups	7
Campus_dist_1_ios subnets	5
MPLS	5
Campus_FW1_screenos subnets	5
Finance Subnets	5
Campus_fw2_screenos subnets	0

Reachable Targets

Reachable Target Overview

REDSEAL

Launch Java App | Help | Logged in as: uiadmin

Control Center | Network Map | Network Access | Threats | Vulnerabilities | Configuration Issues | Security Impact | Detailed Path | Incident Response

Find Threat Source: 10.11.36.20

Where can they go?

Threat Source Overview

Host Information

Name	10.11.36.20
Operating System	Linux
Applications	HTTPD OpenSSH rquotad vsFTPd

Groups

Policy Groups	Trusted Campus_fw2_screenos subnets
Topology Groups	

Topology

IP Address	10.11.36.20
Subnet	10.11.36.0/24

Layer 2 Location

MAC Address	00:10:11:36:00:20
Connected Switch	test-1136-sw1 (null)
Connected Port	GigabitEthernet0/20

Reachable Groups

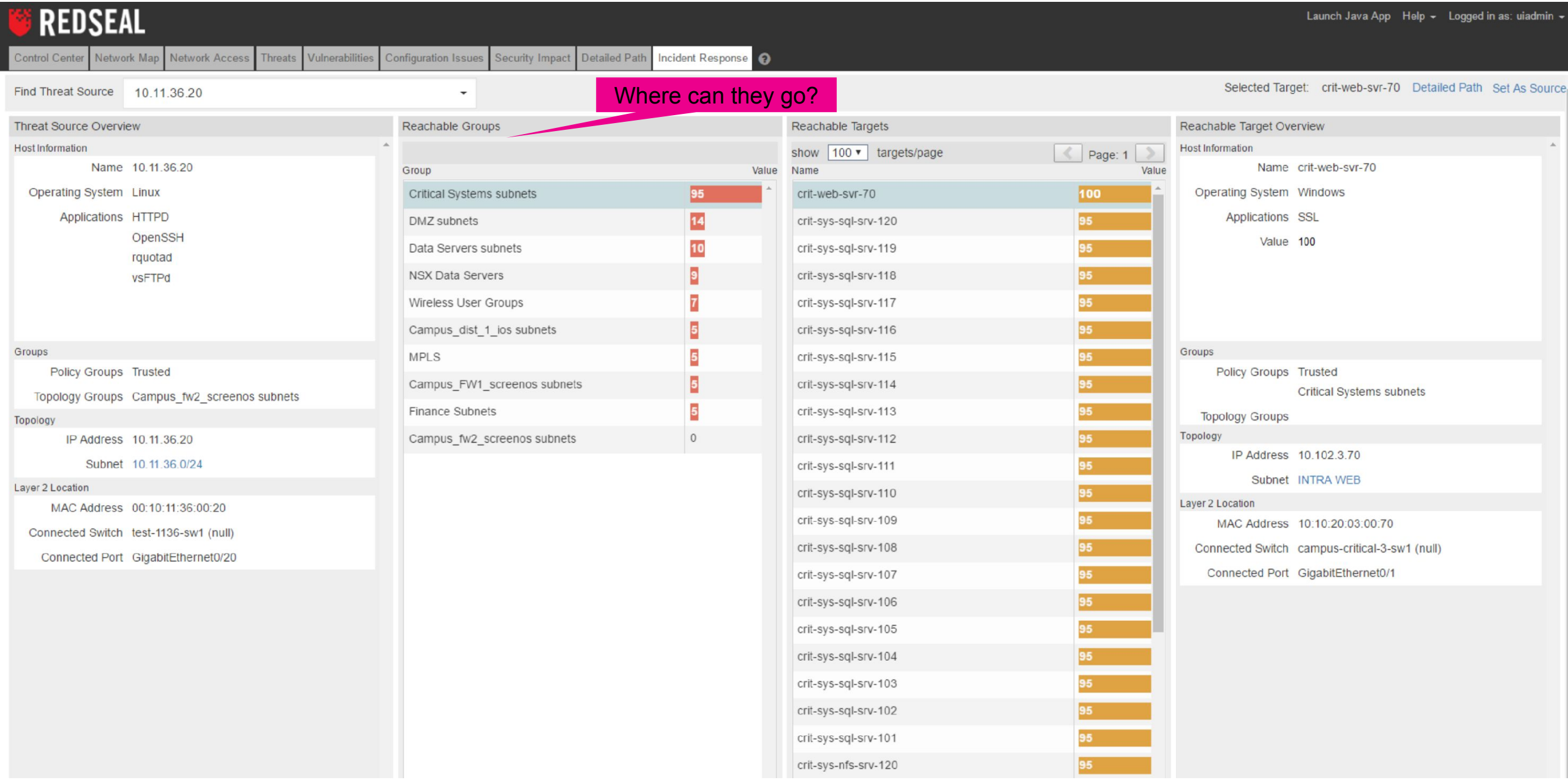
Group	Value
Critical Systems subnets	95
DMZ subnets	14
Data Servers subnets	10
NSX Data Servers	9
Wireless User Groups	7
Campus_dist_1_ios subnets	5
MPLS	5
Campus_FW1_screenos subnets	5
Finance Subnets	5
Campus_fw2_screenos subnets	0

Reachable Targets

show 100 targets/page Page: 1

Name	Value
crit-web-svr-70	100
crit-sys-sql-srv-120	95
crit-sys-sql-srv-119	95
crit-sys-sql-srv-118	95
crit-sys-sql-srv-117	95
crit-sys-sql-srv-116	95
crit-sys-sql-srv-115	95
crit-sys-sql-srv-114	95
crit-sys-sql-srv-113	95
crit-sys-sql-srv-112	95
crit-sys-sql-srv-111	95
crit-sys-sql-srv-110	95
crit-sys-sql-srv-109	95
crit-sys-sql-srv-108	95
crit-sys-sql-srv-107	95
crit-sys-sql-srv-106	95
crit-sys-sql-srv-105	95
crit-sys-sql-srv-104	95
crit-sys-sql-srv-103	95
crit-sys-sql-srv-102	95
crit-sys-sql-srv-101	95
crit-sys-nfs-srv-120	95

Reachable Target Overview



splunk> .conf19

RedSeal

Not Secure https://pm-rsa-1.lab.redseal.net/redseal/a/map/2c90030557546a1e015754780b7b18b7

REDSEAL

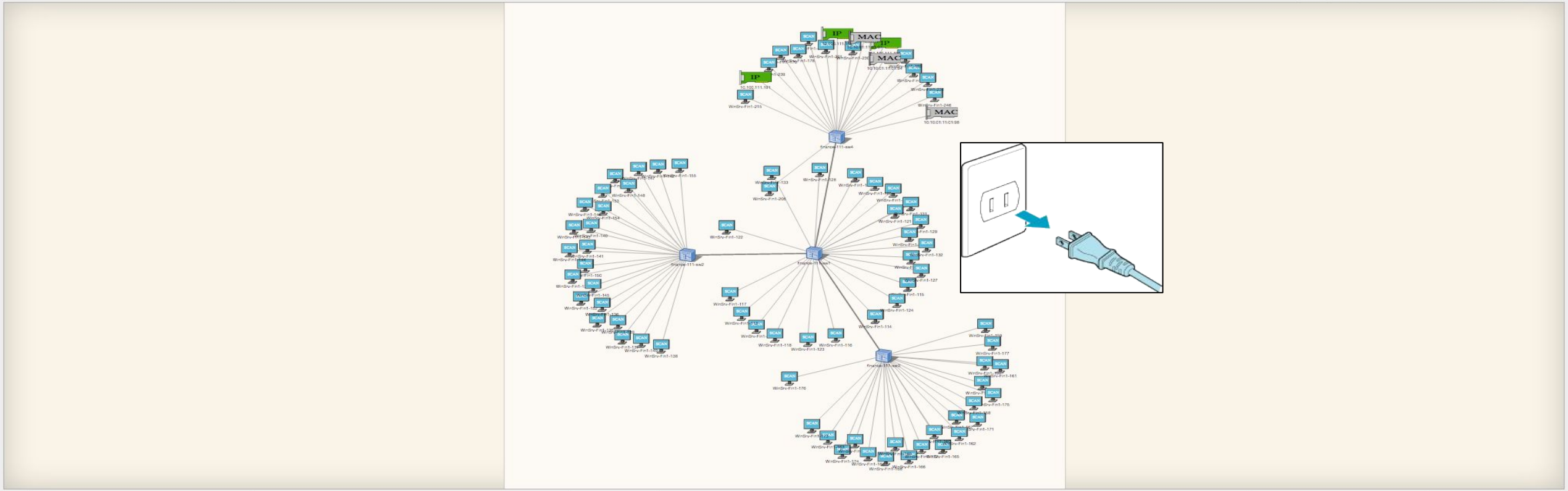
Launch Java App | Help | Logged in as: uladmin

Control Center | Network Map | Network Access | Threats | Vulnerabilities | Configuration Issues | Security Impact | Detailed Path | Incident Response

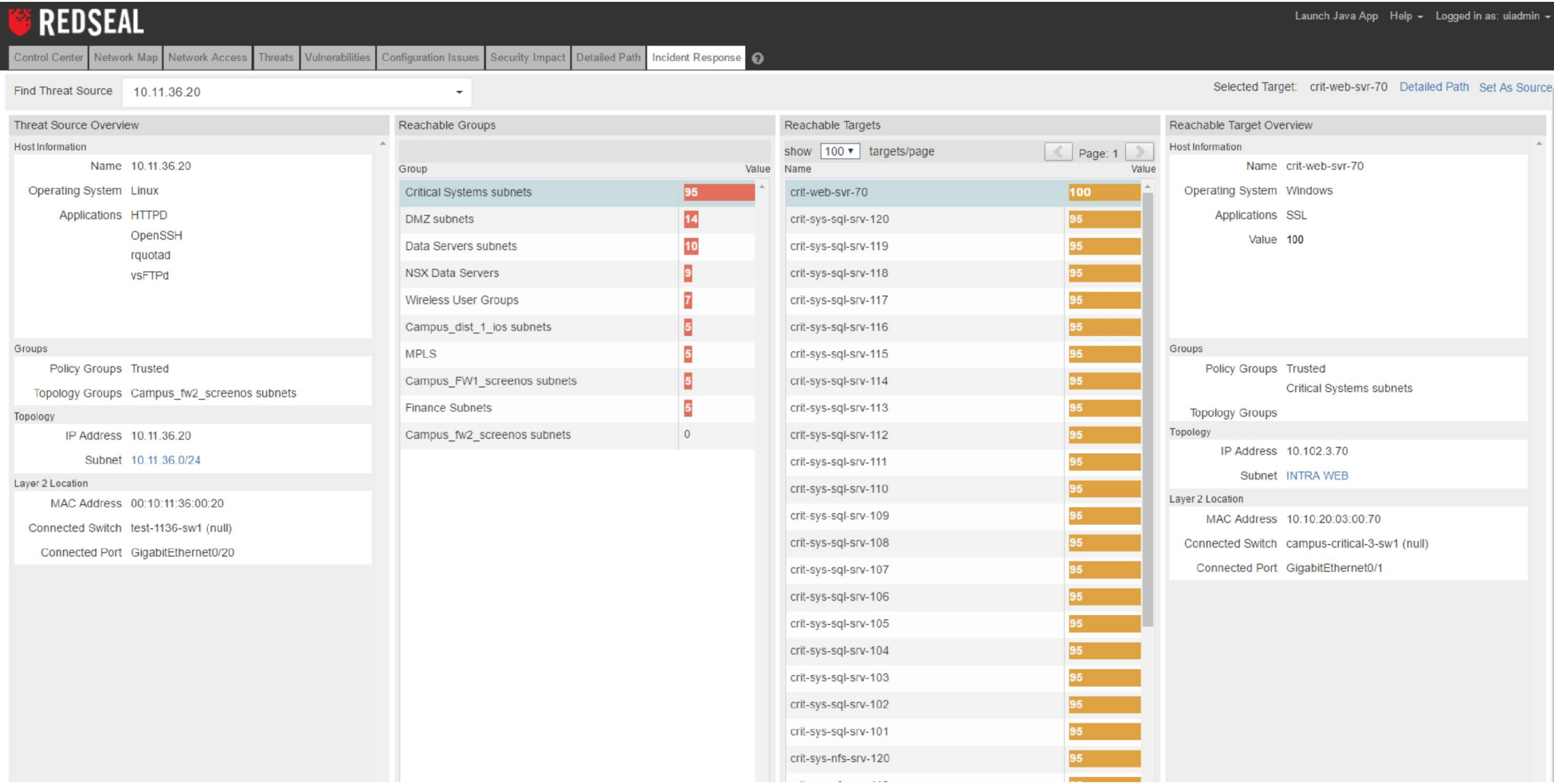
Layer 2 Network Map for subnet

10.100.111.0/24

Zoom: 57%



Switch	Port	Mode	Peer	Peer Interface	Peer IP Address	Peer MAC Address	Peer VLAN
finance-111-sw3	GigabitEthernet0/15	access	WinSrv-Fin1-170	WinSrv-Fin1-170		10:10:01:11:01:70	10
finance-111-sw4	GigabitEthernet0/7	access	WinSrv-Fin1-208	WinSrv-Fin1-208		10:10:01:11:02:08	10
finance-111-sw1	GigabitEthernet0/11	access	WinSrv-Fin1-122	WinSrv-Fin1-122		10:10:01:11:01:22	10
finance-111-sw4	GigabitEthernet0/6	access	WinSrv-Fin1-206	WinSrv-Fin1-206		10:10:01:11:02:06	10



REDSEAL

Launch Java App | Help | Logged in as: uiadmin

Control Center | Network Map | Network Access | Threats | Vulnerabilities | Configuration Issues | Security Impact | Detailed Path | Incident Response

Detailed Path Query

Sources: 10.11.36.20 | Destinations: crit-web-svr-70 | Protocols: Type Protocols, Protocol Range | Ports: Type Ports, Port Range | Query

Exhaustive Query

DETAILED PATH RESULT

Tools

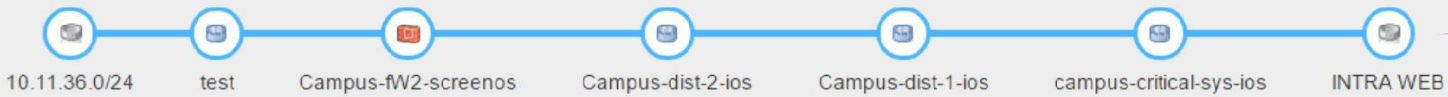
Fully Open Path

1 Path(s) Discovered:

Row count: 1

Result	Hops	Start	Finish
Not Filtered	5	10.11.36.0/24 (connected to test4)	10.102.3.0/24 INTRA WEB

Individual path with 5 hop(s)



How do they get there?

Path Details

Access Details

Access	Device	Interface	VRF Table	Protocol	Source IP	Source Port	Destination IP	Destination Port

splunk> .conf19

REDSEAL

Launch Java App | Help | Logged in as: uiadmin

Control Center | Network Map | Network Access | Threats | Vulnerabilities | Configuration Issues | Security Impact | Detailed Path | Incident Response

Detailed Path Query

Sources: 10.11.36.20 A

Destinations: crit-web-svr-70 B

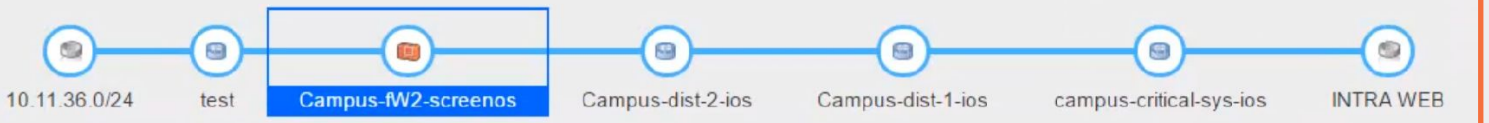
Protocols: Type Protocols, Protocol Range

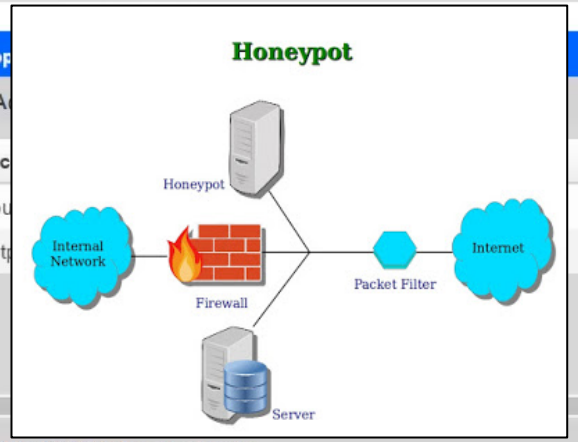
Ports: Type Ports, Port Range

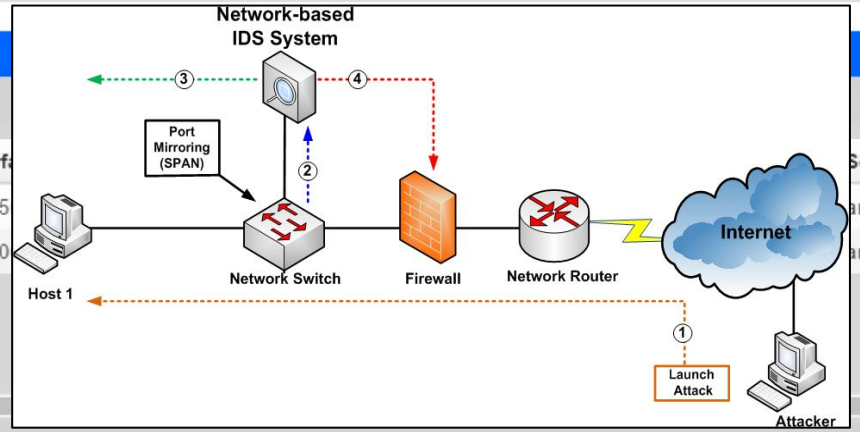
Query

Exhaustive Query

Individual path with 5 hop(s)







Acc	Interf	Source Port	Destination IP	Destination Port
Inpu	10.15	any	10.102.3.70	any
Outp	10.10	any	10.102.3.70	any

Filter/NAT Rules and Routes

Row count: 2

Search

Device	Type	Config	First Line
Campus-fW2-screenos	Filter Rule	set policy id 3 from "Test" to "dist" "Any" "Any" "Any" permit	config:111
Campus-fW2-screenos	Filter Rule	(implicit) deny all	

splunk> .conf19

REDSEAL

Launch Java App | Help | Logged in as: uiadmin

Control Center | Network Map | Network Access | Threats | Vulnerabilities

Detailed Path Query

Sources: 10.11.36.20

Exhaustive Query

Ports: Type Ports, Port Range | Query

10.11.36.0/24 — test — Campus-fW2-screenos

Config File Viewer: config

```
111 set policy id 3 from "Test" to "dist" "Any" "Any" "Any" permit
112 exit
113 set policy id 4 from "KE" to "dist" "Any" "Any" "Any" permit
114 exit
115 set policy id 5 from "dist" to "Dev" "Any" "Any" "Any" deny
116 exit
117 set policy id 6 from "dist" to "Product" "Any" "ANY" "Any" deny
118 exit
119 set policy id 7 from "dist" to "Test" "Any" "10.11.36.0/24" "Any" permit
120 exit
121 set policy id 8 from "dist" to "KE" "Any" "Any" "Any" deny
122 exit
123 set policy id 9 from "dist" to "Test" "Any" "172.16.30.0/24" "Any" permit
124 exit
125 set policy id 10 from "dist" to "Test" "Any" "172.16.0.0/24" "Any" permit
```

Export | OK

Hop Details: Campus-fW2-screenos

Access Details

Access	Device						Destination IP	Destination Port
Input	Campus-fW2-screenos	10.150.103.1 (ethernet4)	trust-vr	any	10.11.36.20	any	10.102.3.70	any
Output	Campus-fW2-screenos	10.100.150.130 (ethernet1)	trust-vr	any	10.11.36.20	any	10.102.3.70	any

Filter/NAT Rules and Routes

Row count: 2 | Search

Device	Type	Config	First Line
Campus-fW2-screenos	Filter Rule	set policy id 3 from "Test" to "dist" "Any" "Any" "Any" permit	config:111
Campus-fW2-screenos	Filter Rule	(implicit) deny all	

splunk> .conf19

Integration with RedSeal

Observe
Point Products → Orient
Analytics → Decision Making → Acting

Understand your network terrain

Valuable Threat Source Data

Where is it located?
Both logically and physically?
What other assets can it reach?
What is the access path and the source to the target?

Accelerate Containment

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION