RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: ANF-W04

Hunting for the Undefined Threat: Advanced Analytics & Visualization

Joshua Stevens

Enterprise Security Architect
Hewlett-Packard
Cyber Security Technology Office

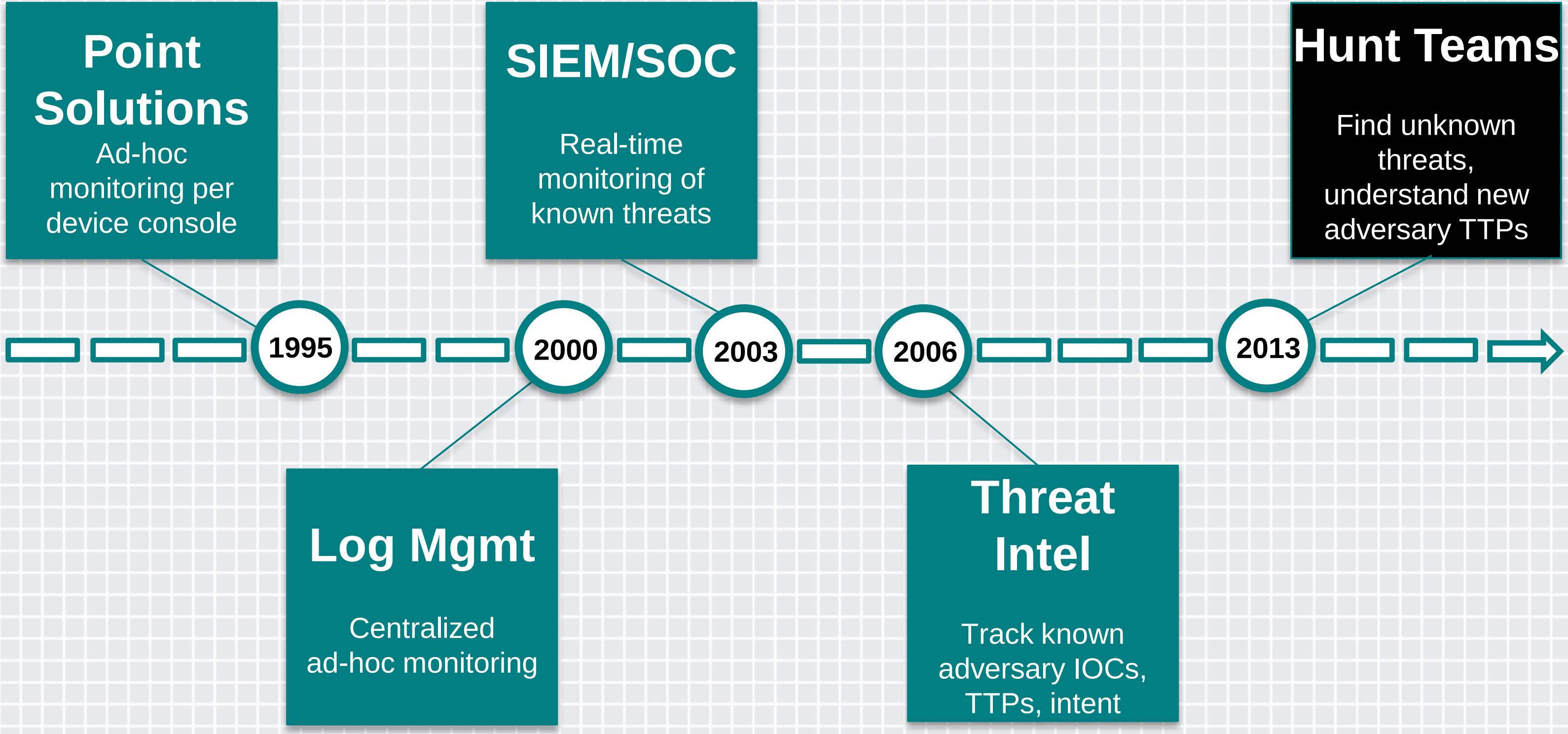
RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Defining the "Hunt Team"

Cyber Defense Evolution



1995

Point Solutions

Ad-hoc monitoring per device console

2000

Log Mgmt

Centralized ad-hoc monitoring

2003

SIEM/SOC

Real-time monitoring of known threats

2006

Threat Intel

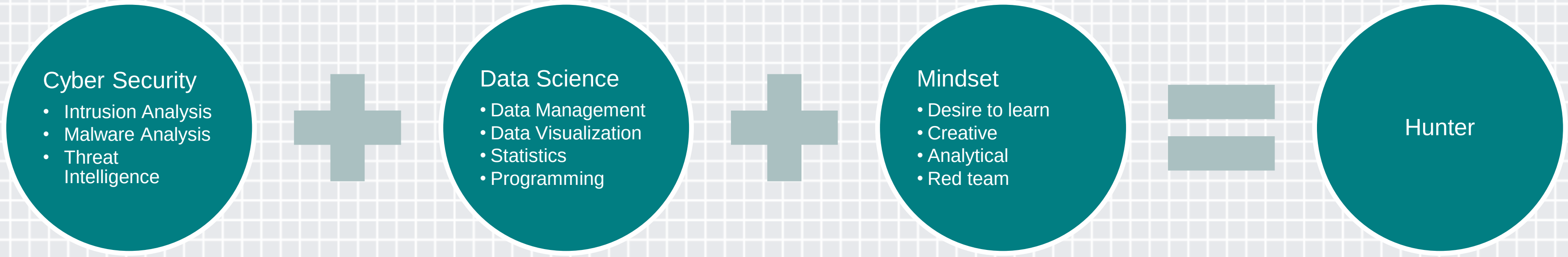
Track known adversary IOCs, TTPs, intent

2013

Hunt Teams

Find unknown threats, understand new adversary TTPs

‘Hunt’er Skillsets



Cyber Security

- Intrusion Analysis
- Malware Analysis
- Threat Intelligence

+

Data Science

- Data Management
- Data Visualization
- Statistics
- Programming

+

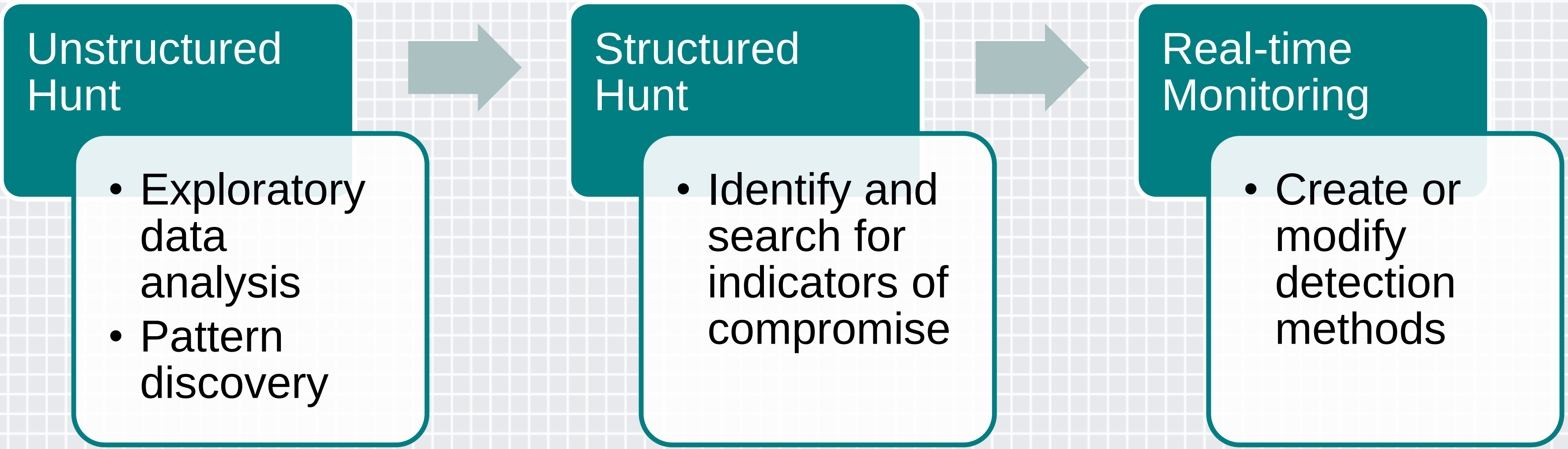
Mindset

- Desire to learn
- Creative
- Analytical
- Red team

=

Hunter

Hunt Processes



Unstructured Hunt

- Exploratory data analysis
- Pattern discovery

Structured Hunt

- Identify and search for indicators of compromise

Real-time Monitoring

- Create or modify detection methods

RSAConference2015

San Francisco | April 20-24 | Moscone Center

The Need for "Data" and Security Analytics

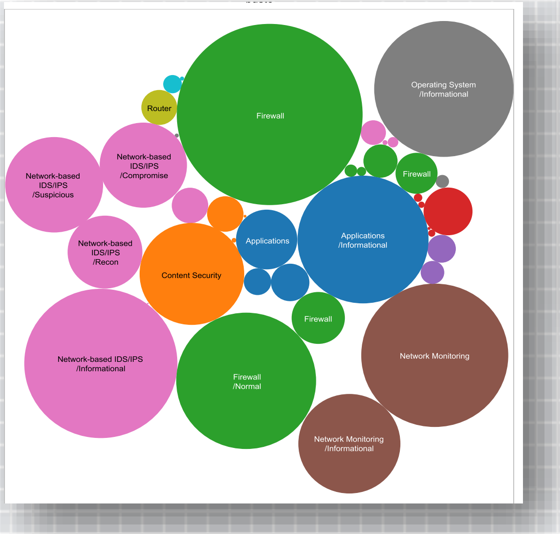
#RSAC

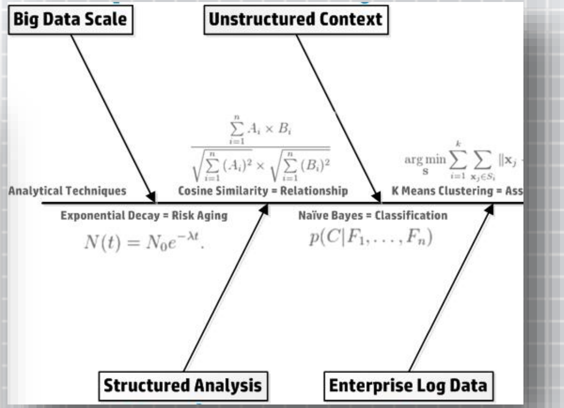
Hiding in Plain Sight

Known Threat	Unknown Threat
Matches a signature	New behavior
Goes to a bad place	Goes to an approved place
Works in the clear	Works encrypted
Unauthorized use	Authorized use
Outside of baseline	Inside of baseline
Within monitored infrastructure	Outside monitored infrastructure

Bad guys know how to stay inside the bell curve!

Security Analytics Comes in Different Flavors





Big Data Scale

Unstructured Context

$$\frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} (A_i)^2} \times \sqrt{\sum_{i=1}^{n} (B_i)^2}}$$

$\arg\min_{\mathbf{S}} \sum_{i=1}^{k} \sum_{\mathbf{x}_j \in S_i} \|\mathbf{x}_j$

Analytical Techniques

Cosine Similarity = Relationship

K Means Clustering = Ass

Exponential Decay = Risk Aging

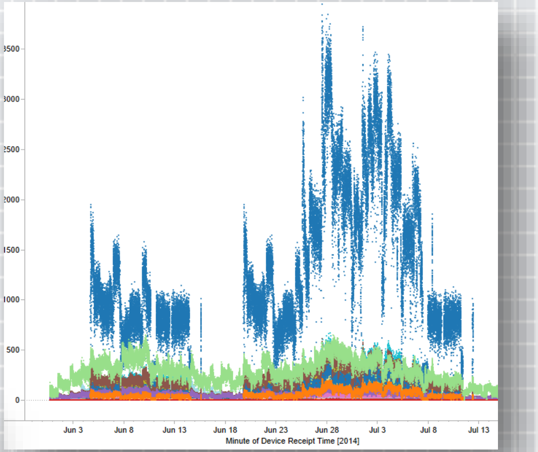
$$N(t) = N_0 e^{-\lambda t}.$$

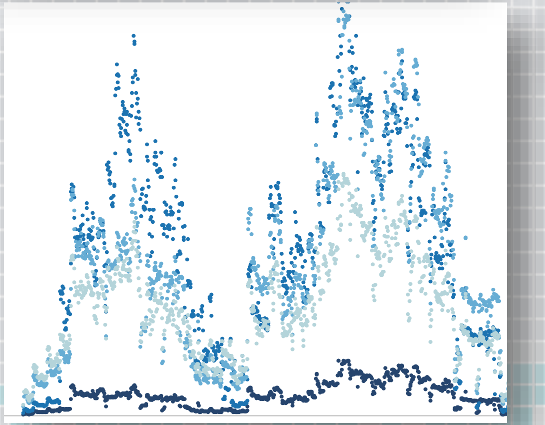
Naïve Bayes = Classification

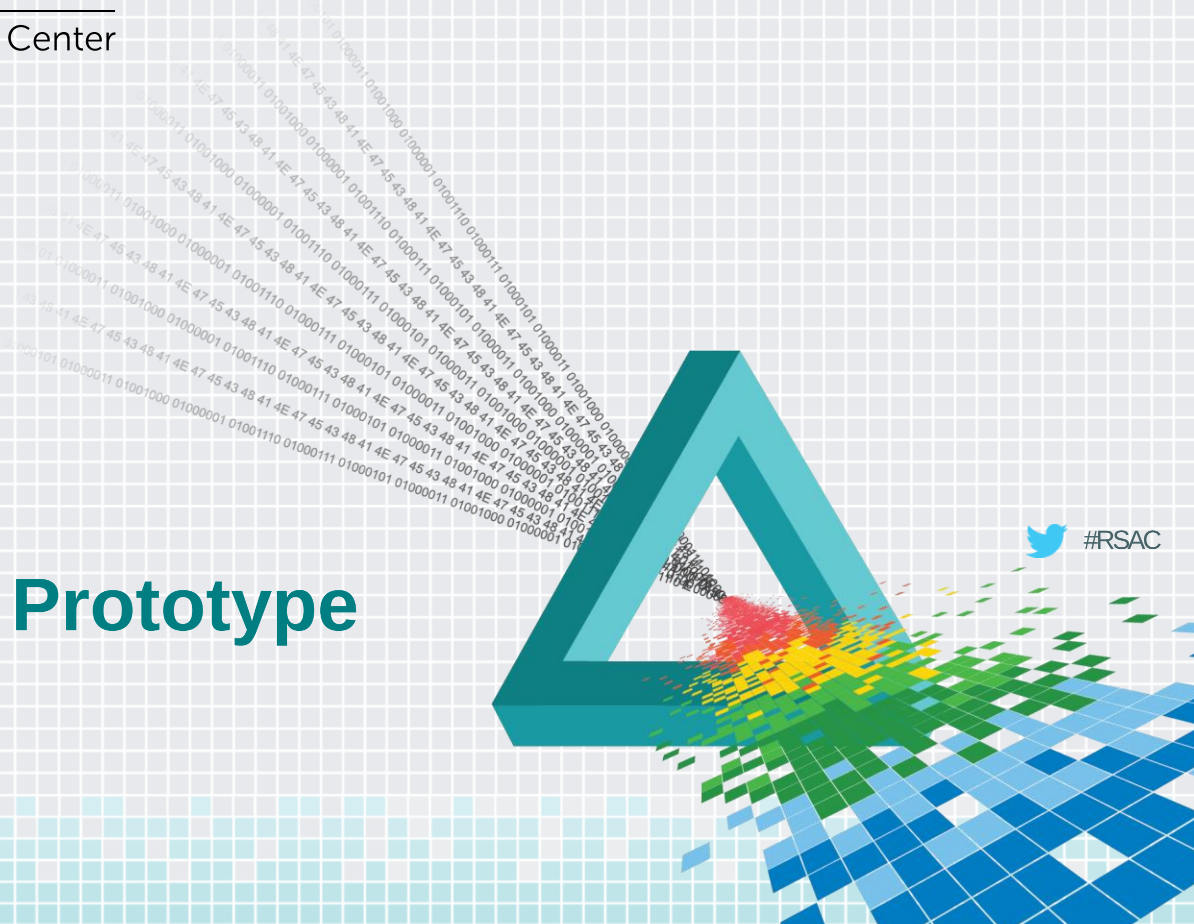
$$p(C|F_1, \ldots, F_n)$$

Structured Analysis

Enterprise Log Data

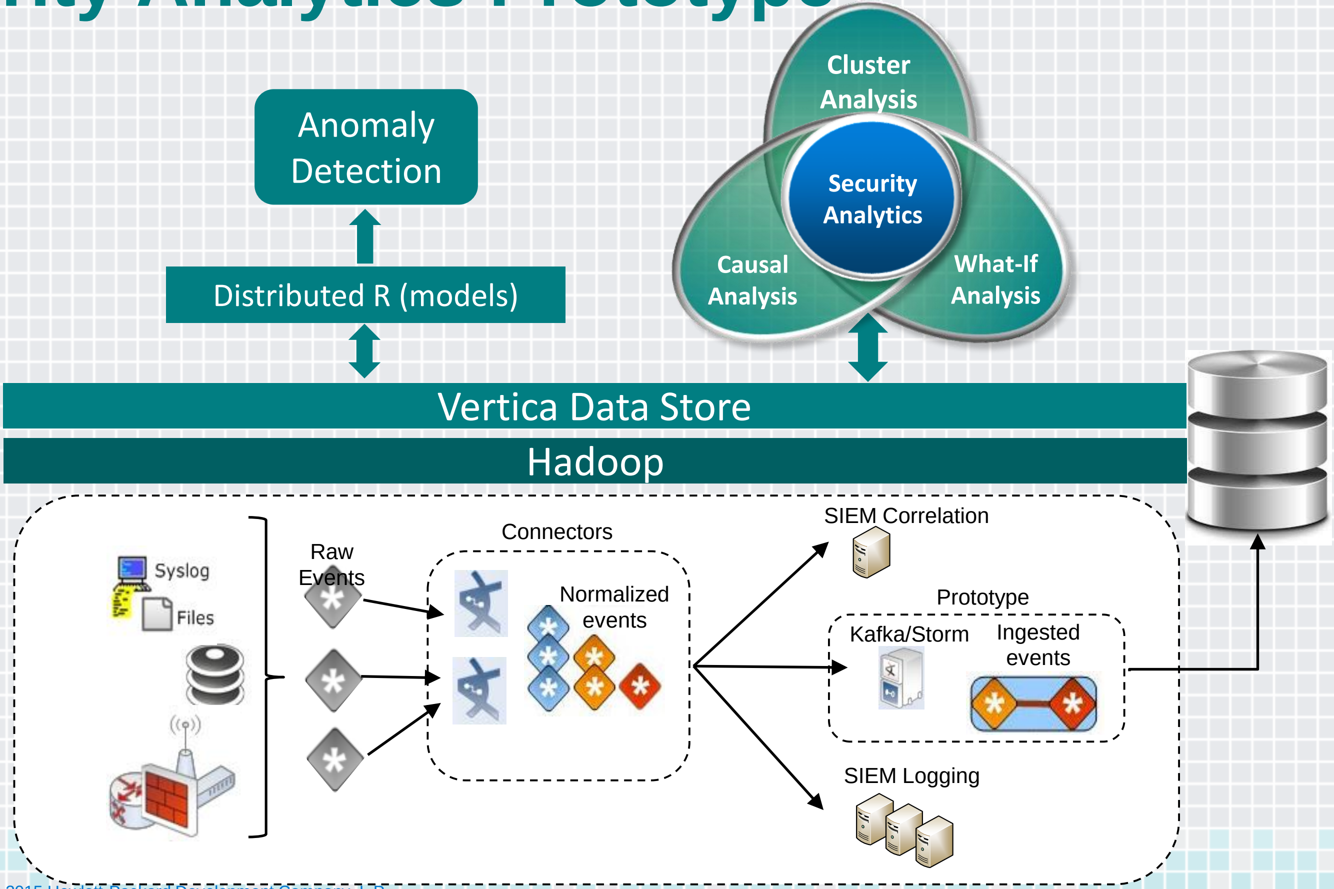






A 13-billion Event Prototype

Security Analytics Prototype



Anomaly Detection

Distributed R (models)

Cluster Analysis

Security Analytics

Causal Analysis

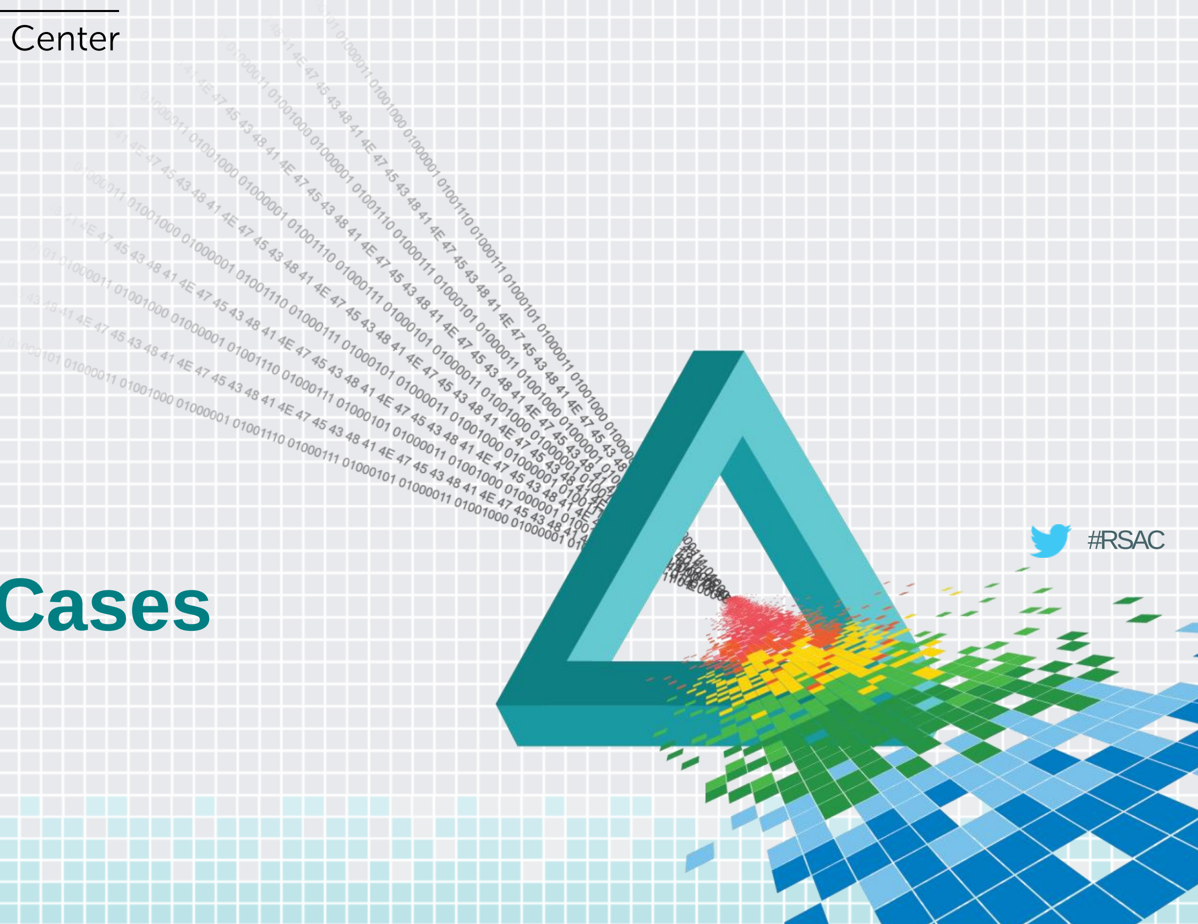
What-If Analysis

Vertica Data Store

Hadoop

RSAConference2015

San Francisco | April 20-24 | Moscone Center



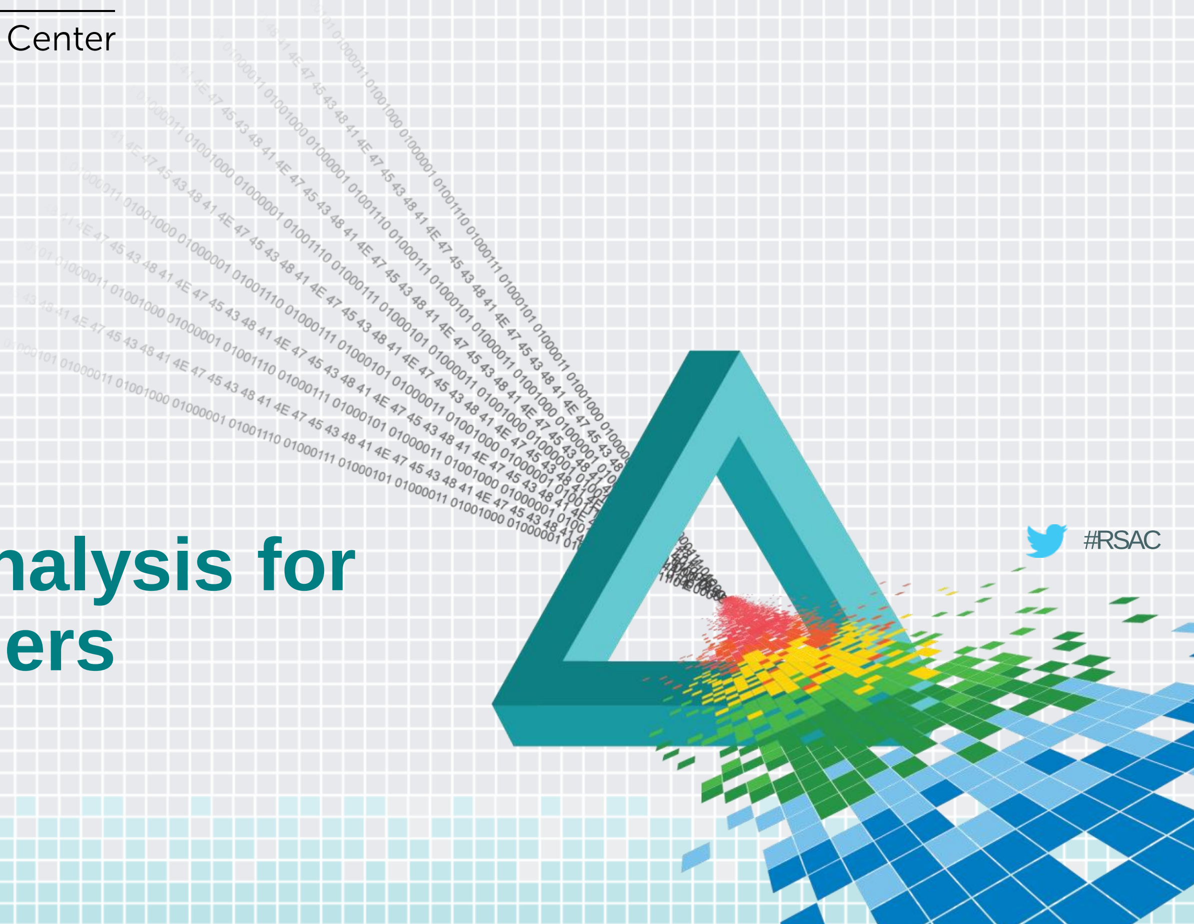
#RSAC

5 Hunt Team Use Cases

RSAConference2015

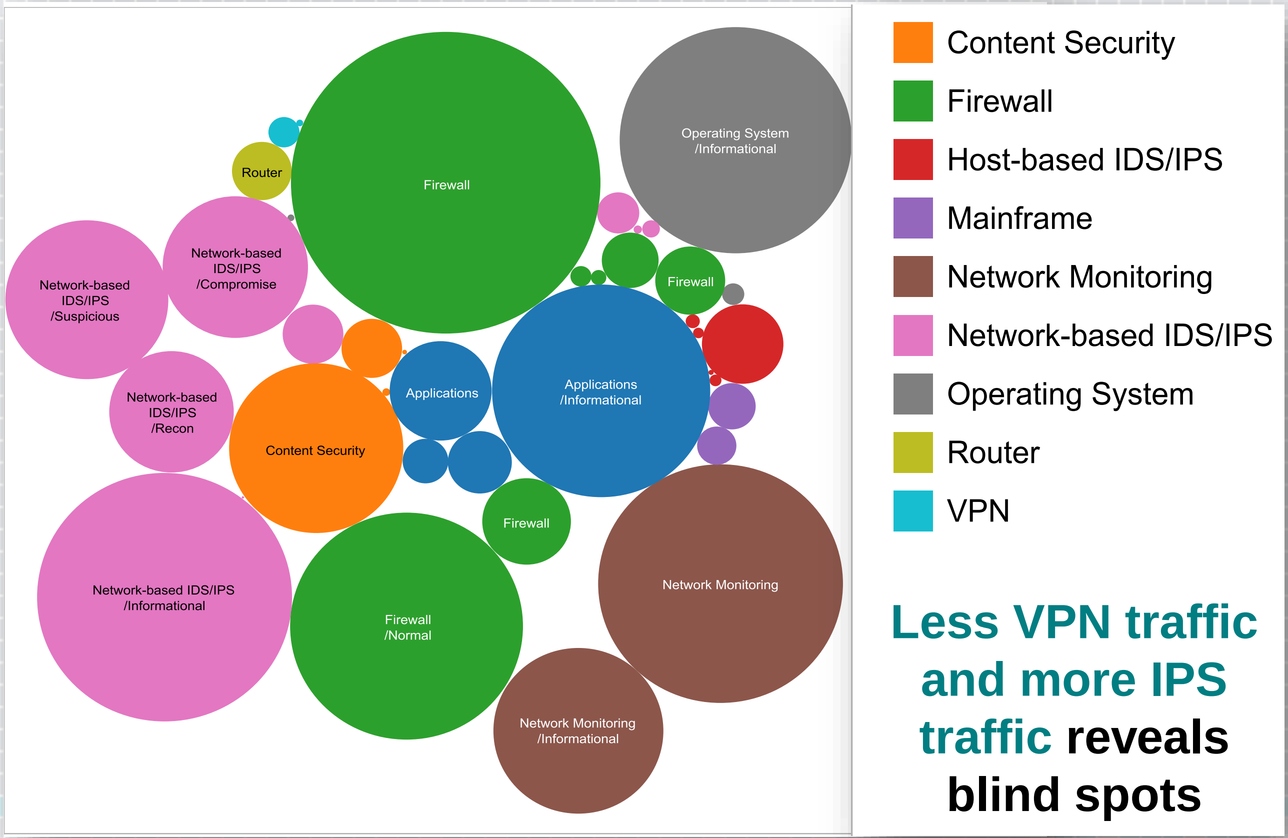
San Francisco | April 20-24 | Moscone Center

Case 1: Cluster Analysis for Hunt Team Managers



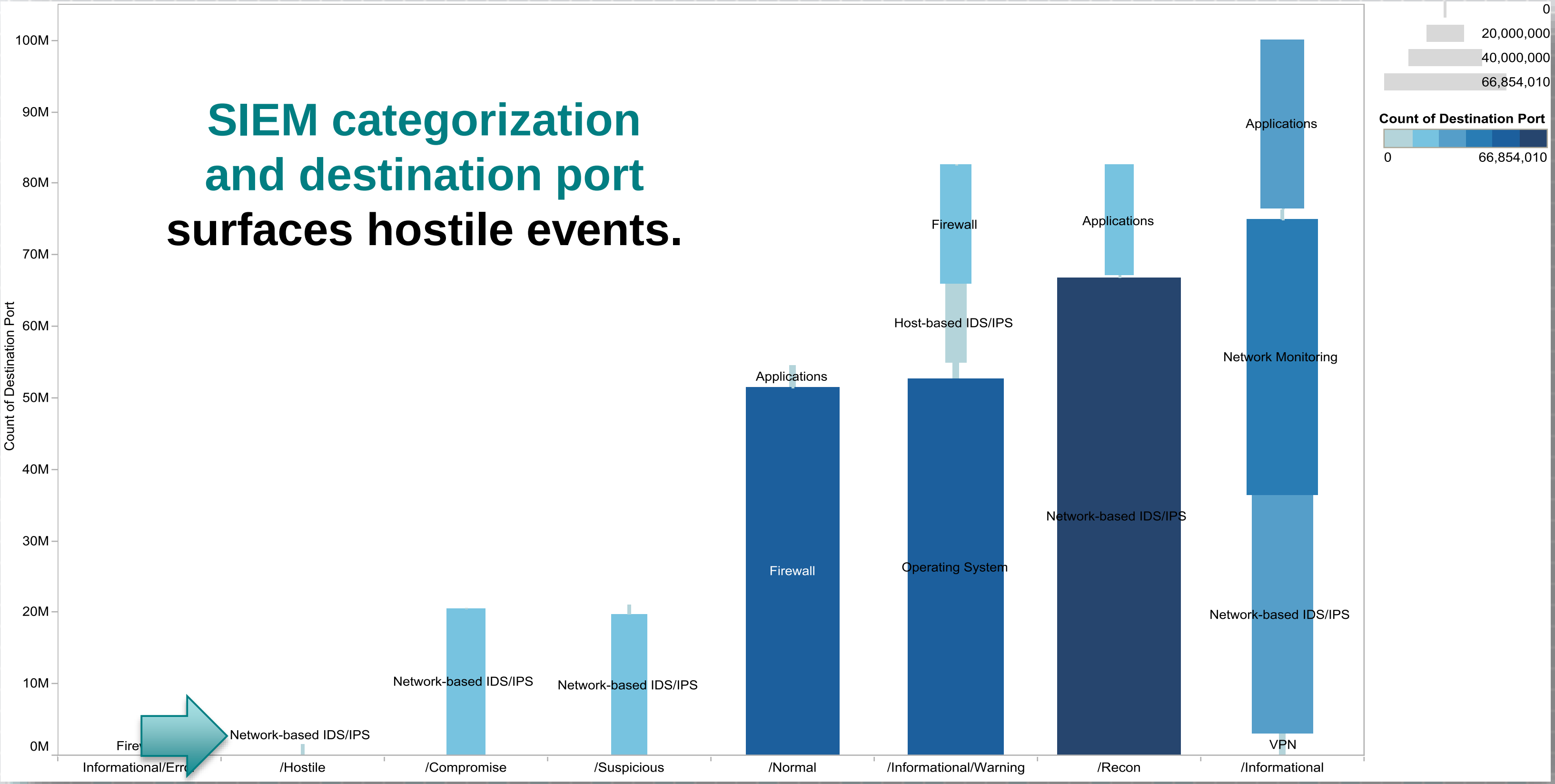
#RSAC

View: Proportional Relationships



Less VPN traffic and more IPS traffic reveals blind spots

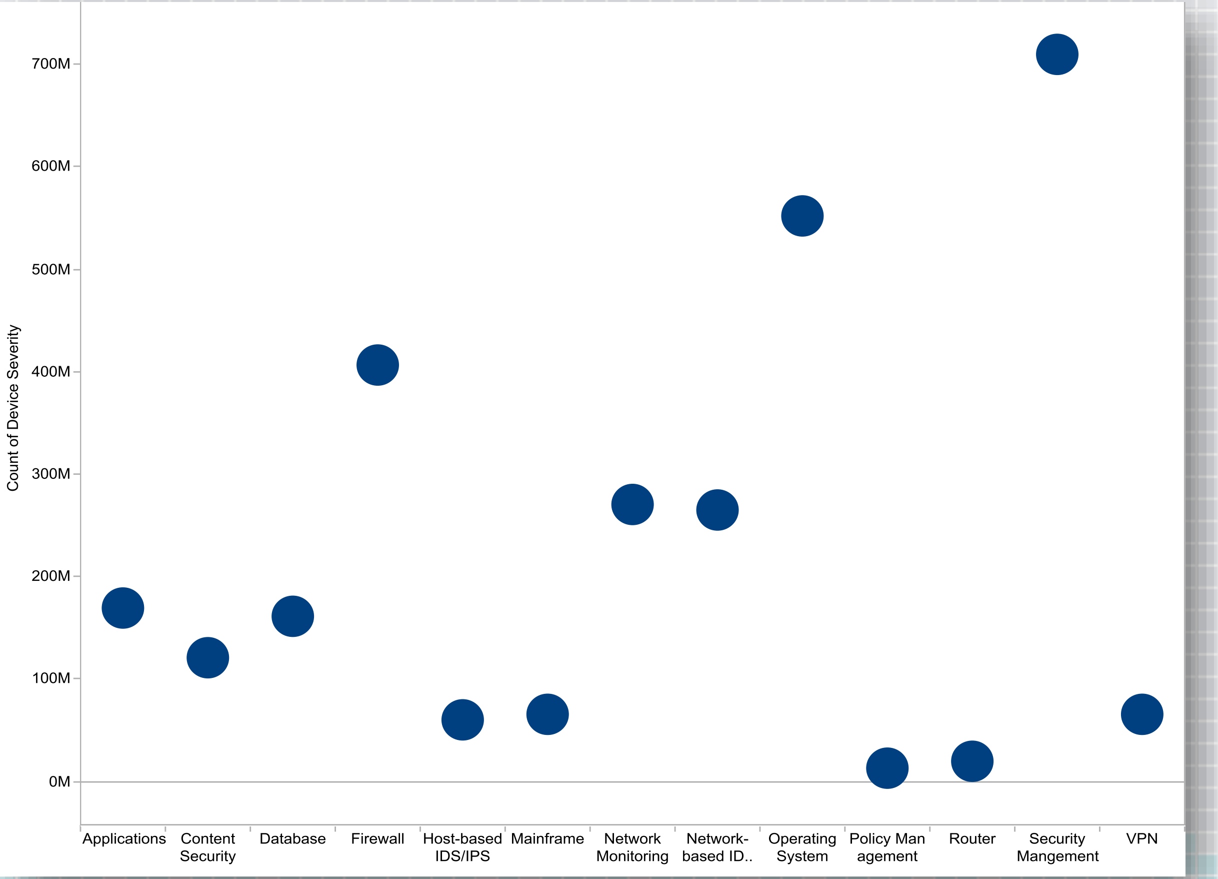
Apply Categorization



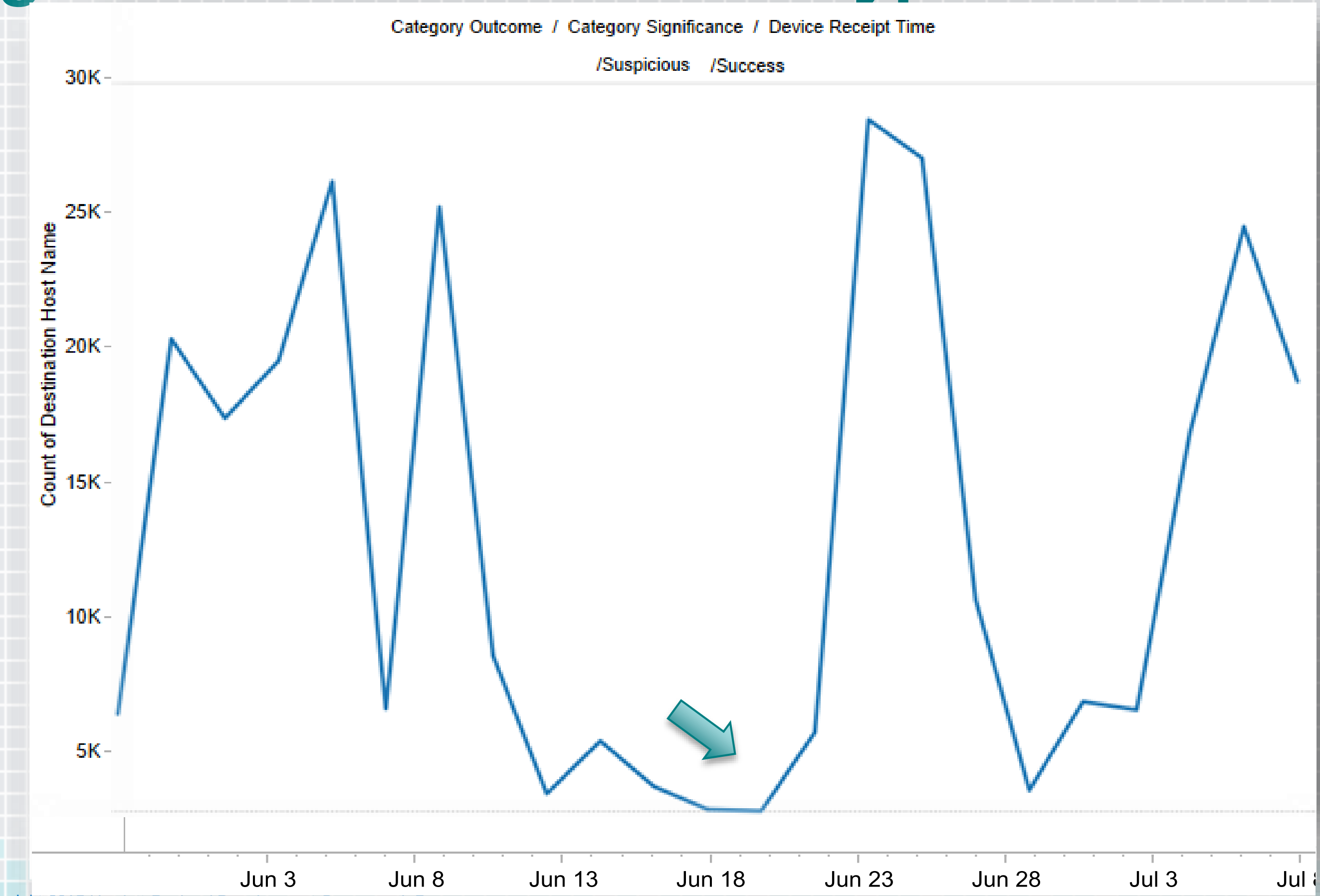
SIEM categorization and destination port surfaces hostile events.

Case 2: Track Anomalies for Security Analysts

View: Events by High Severity Rating and Volume

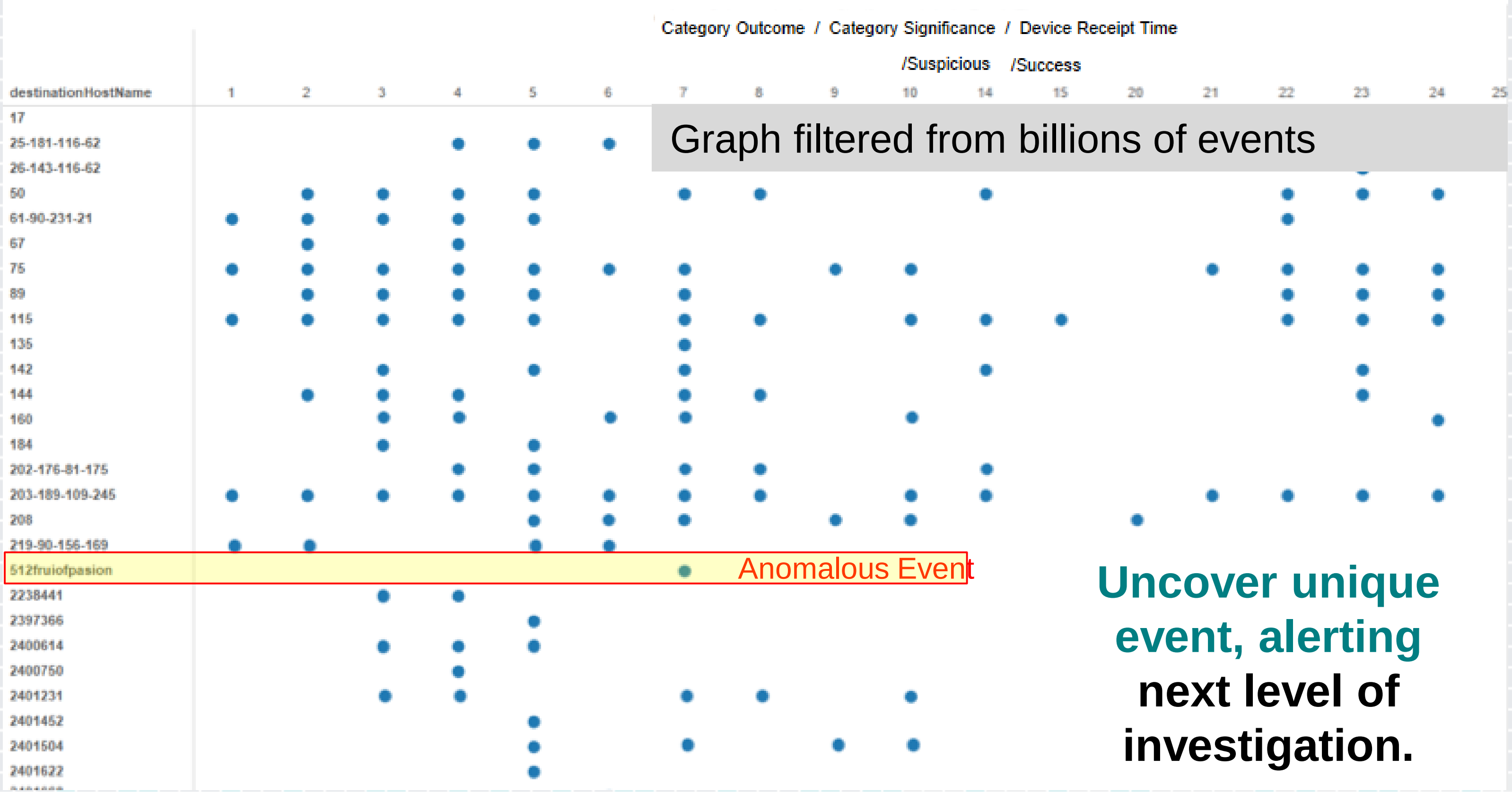


Change View to Destination Type



Display trend of unique destinations visited

Apply Anomaly Chart



Graph filtered from billions of events

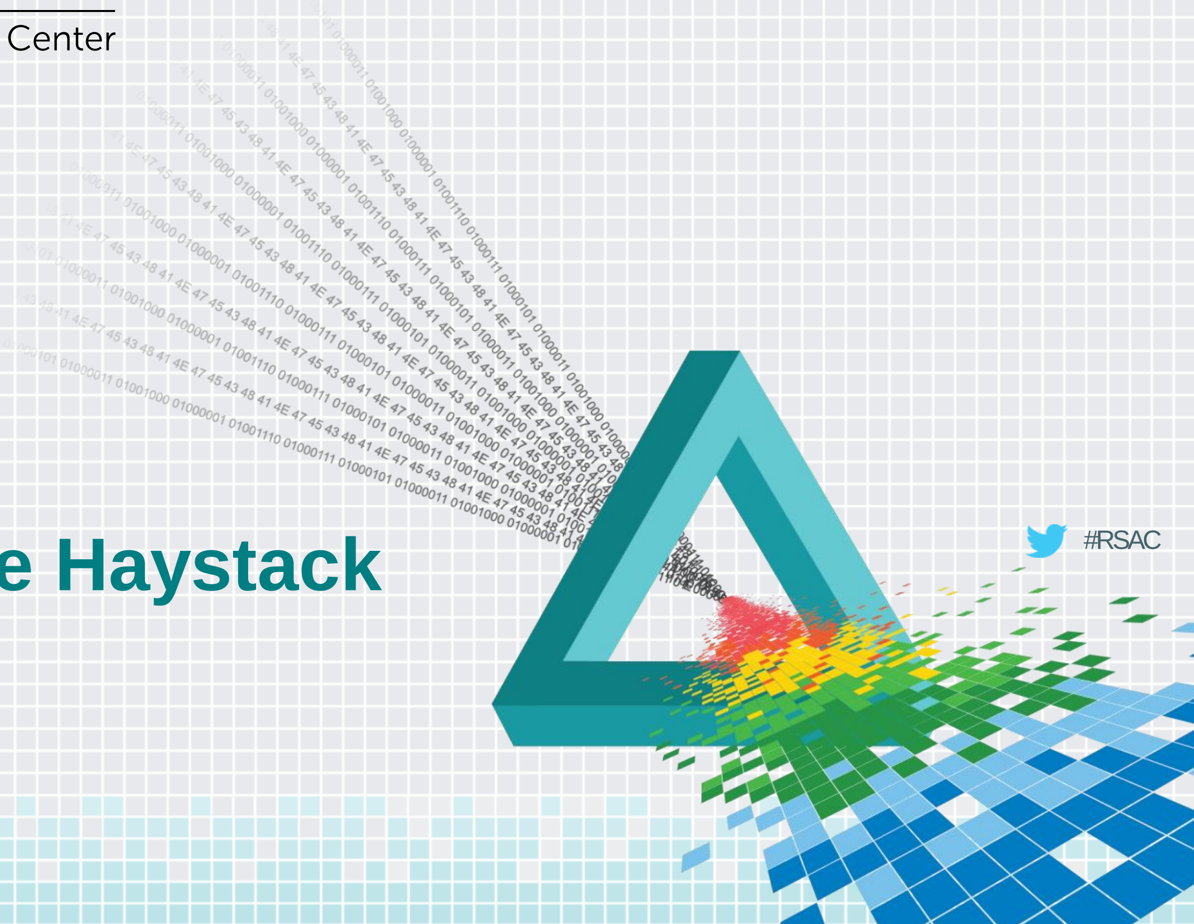
Anomalous Event

Uncover unique event, alerting next level of investigation.

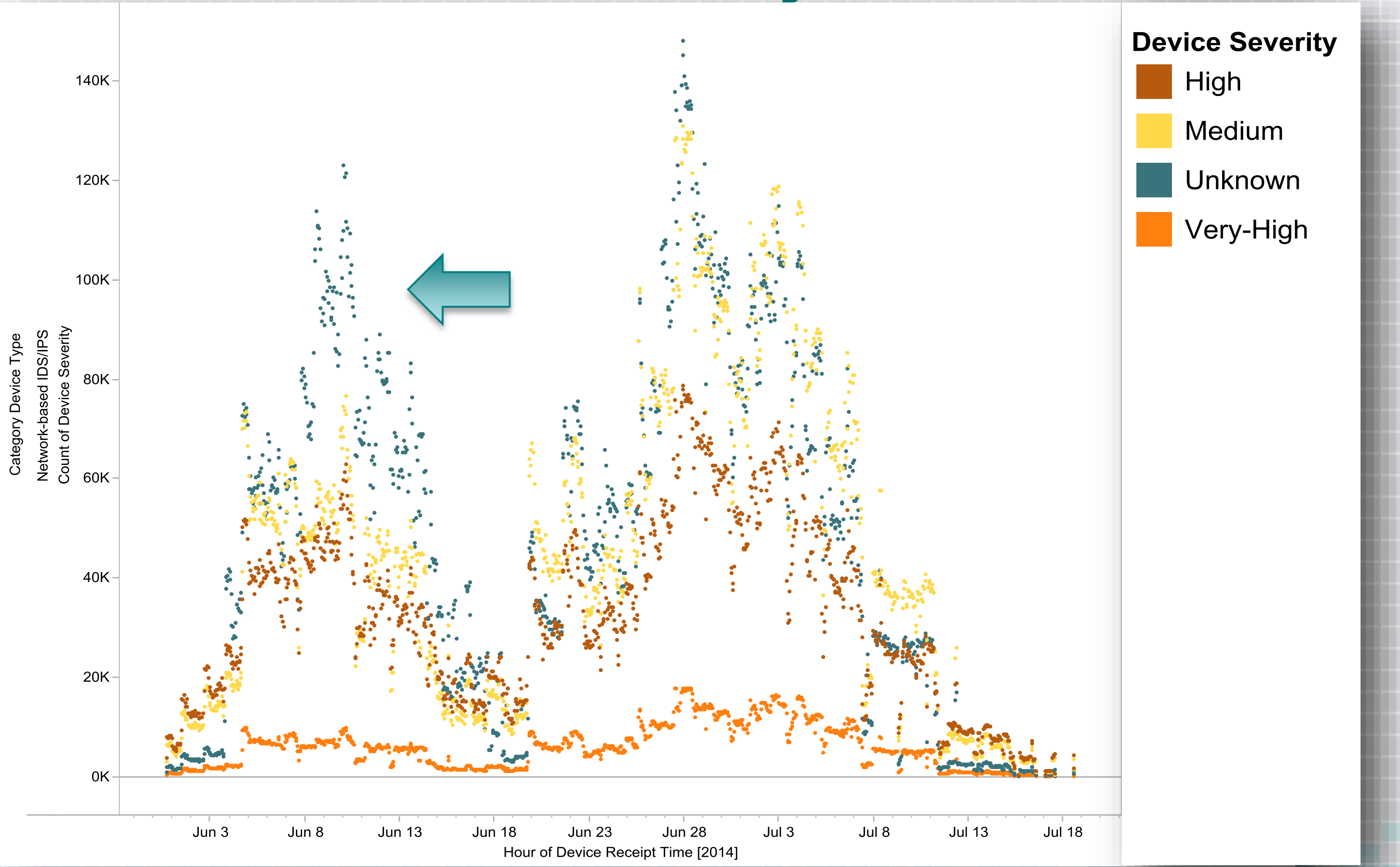
RSAConference2015

San Francisco | April 20-24 | Moscone Center

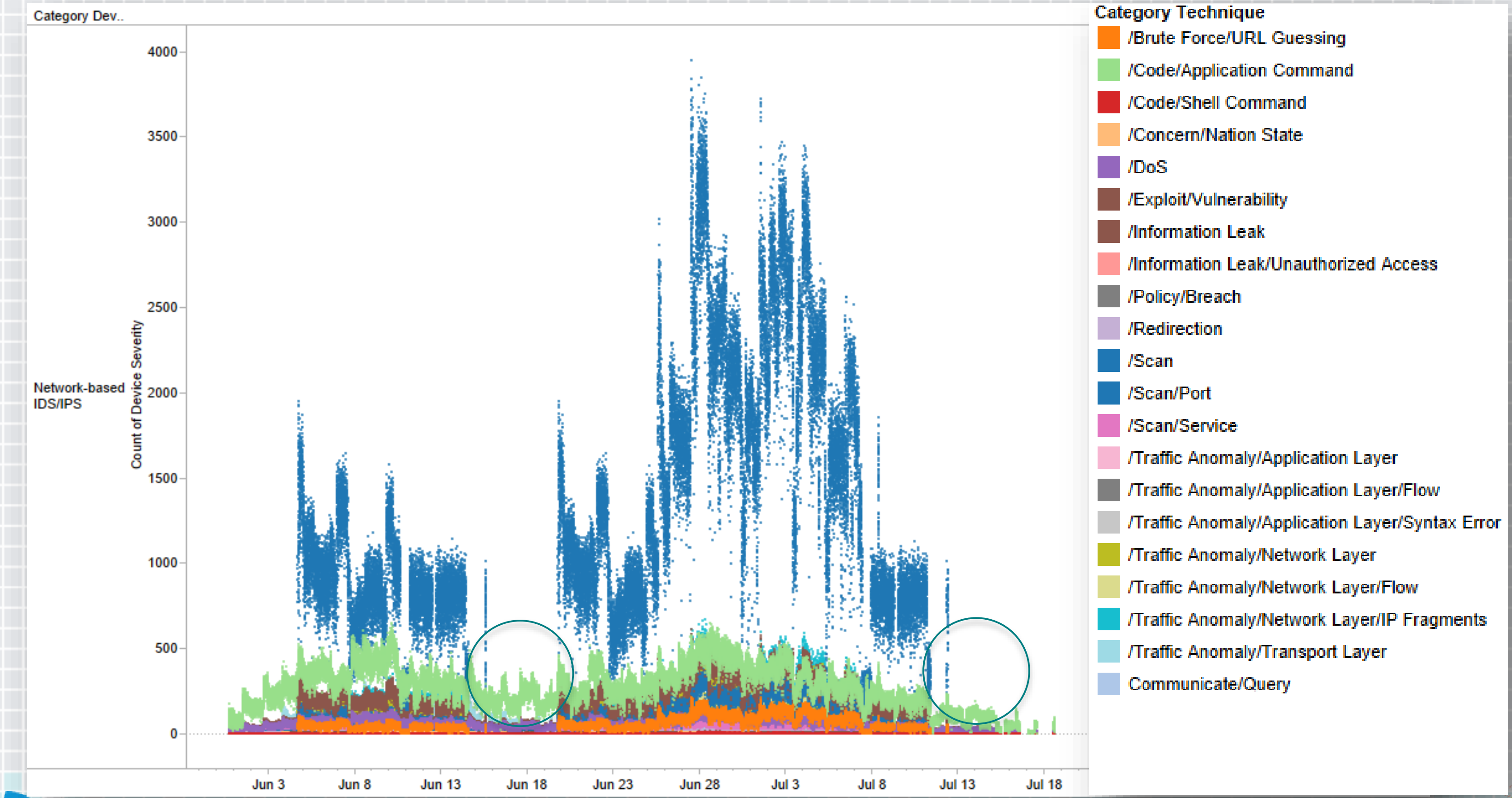
Case 3: Analyze the Haystack for the Hunt Team



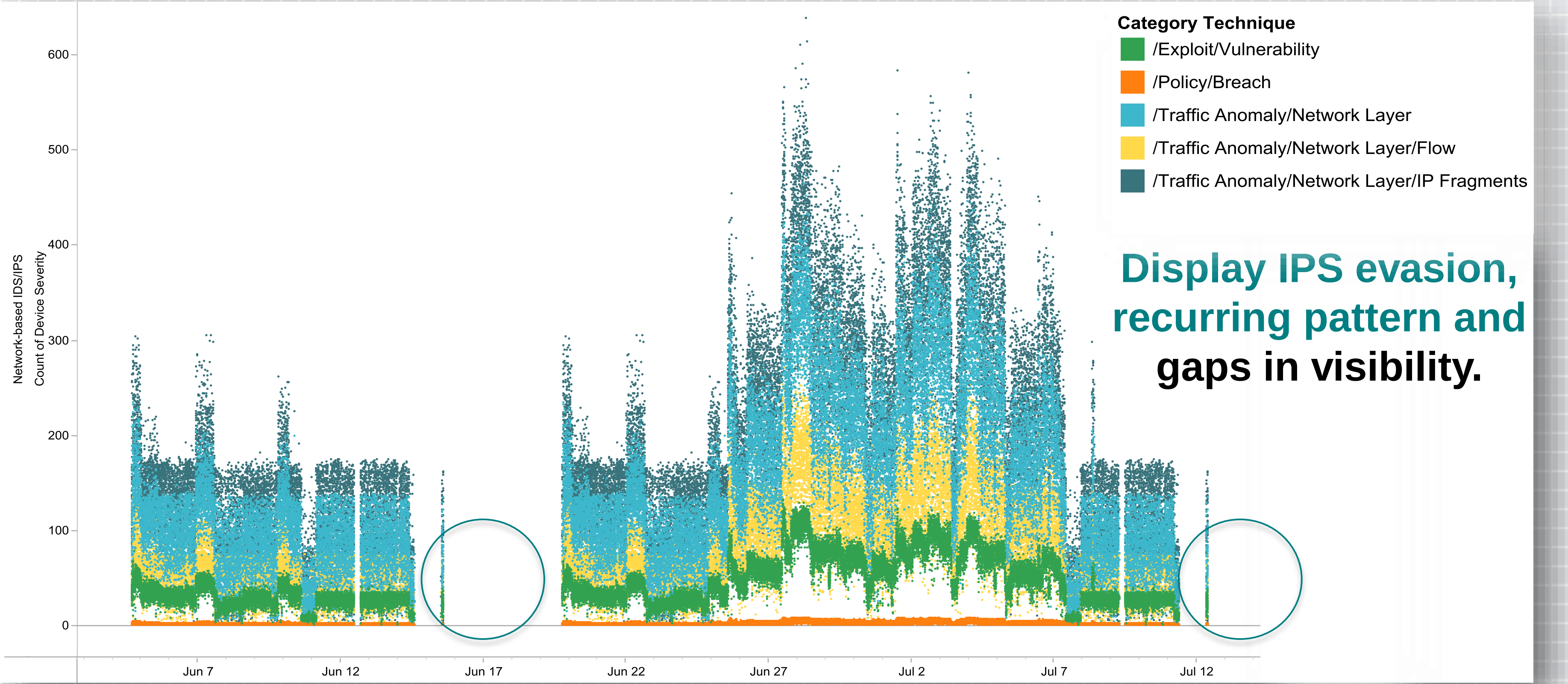
View: IPS Events for 45 days



Model IPS Events by Technique



Filter on the Return Traffic



Display IPS evasion, recurring pattern and gaps in visibility.

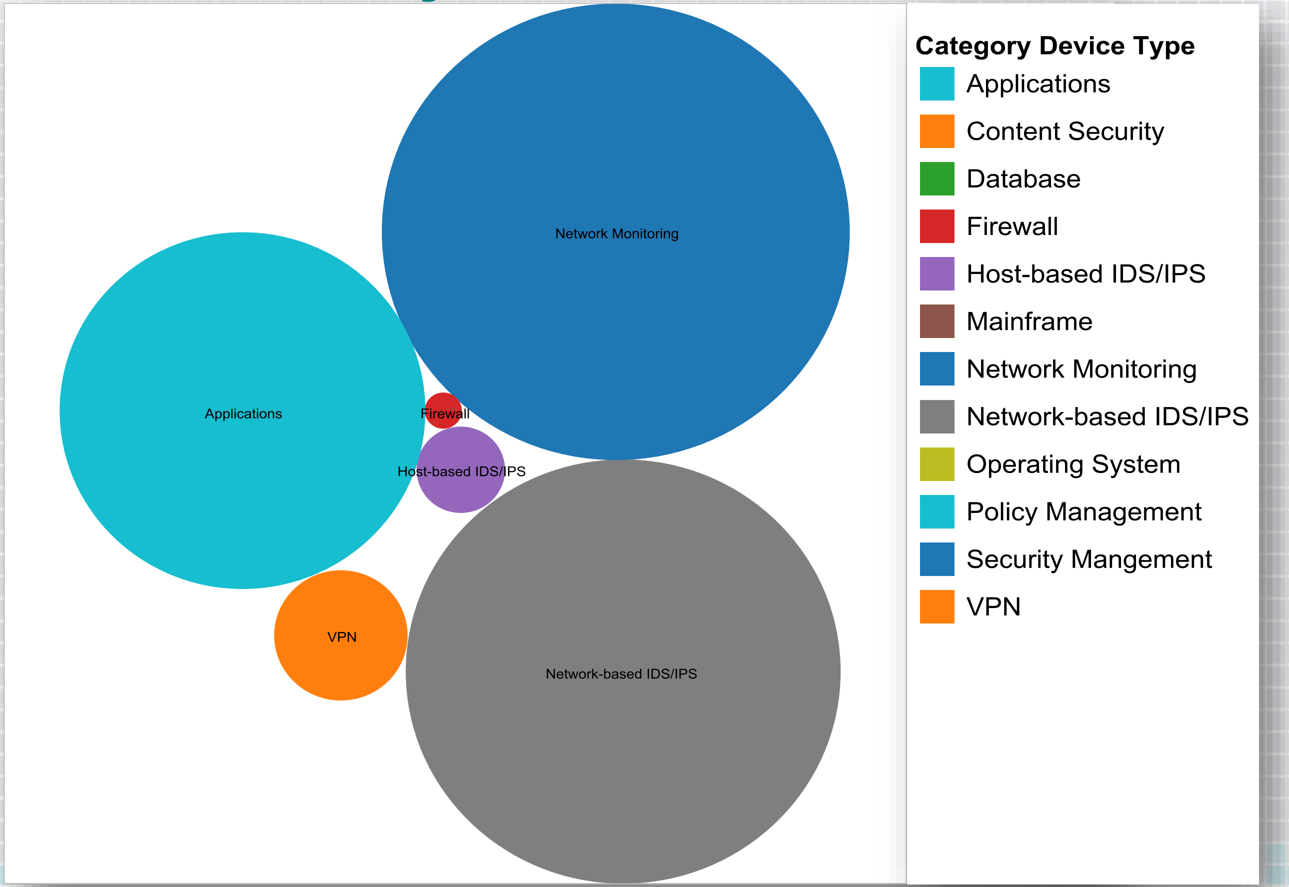
RSA Conference2015

San Francisco | April 20-24 | Moscone Center

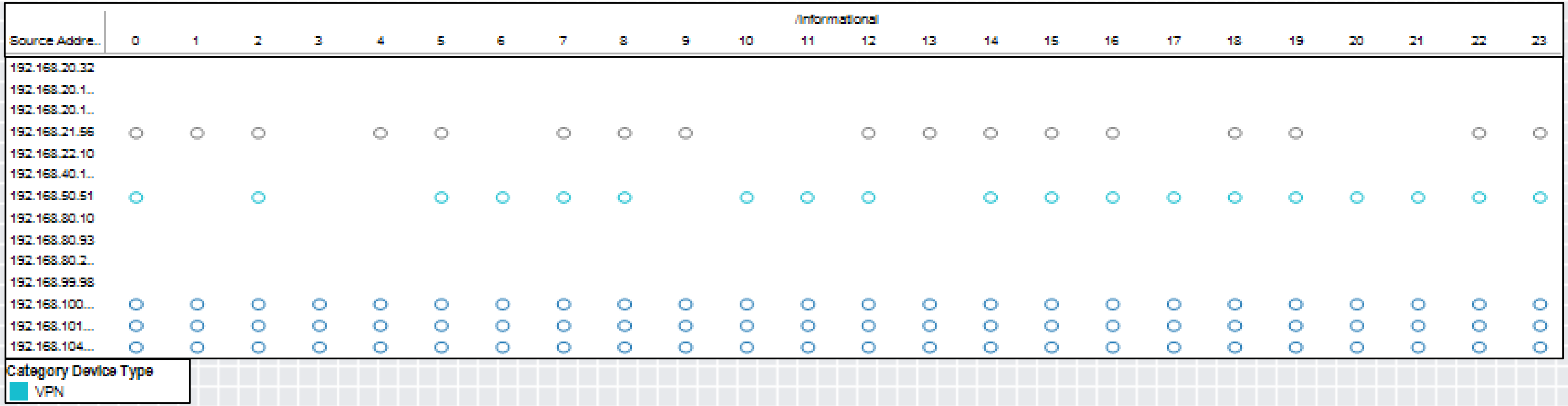
#RSAC

Case 4: Behavioral Analysis for the Hunt Team

View: Non-Security Events in the Environment



A Typical View of VPN Logging by Source

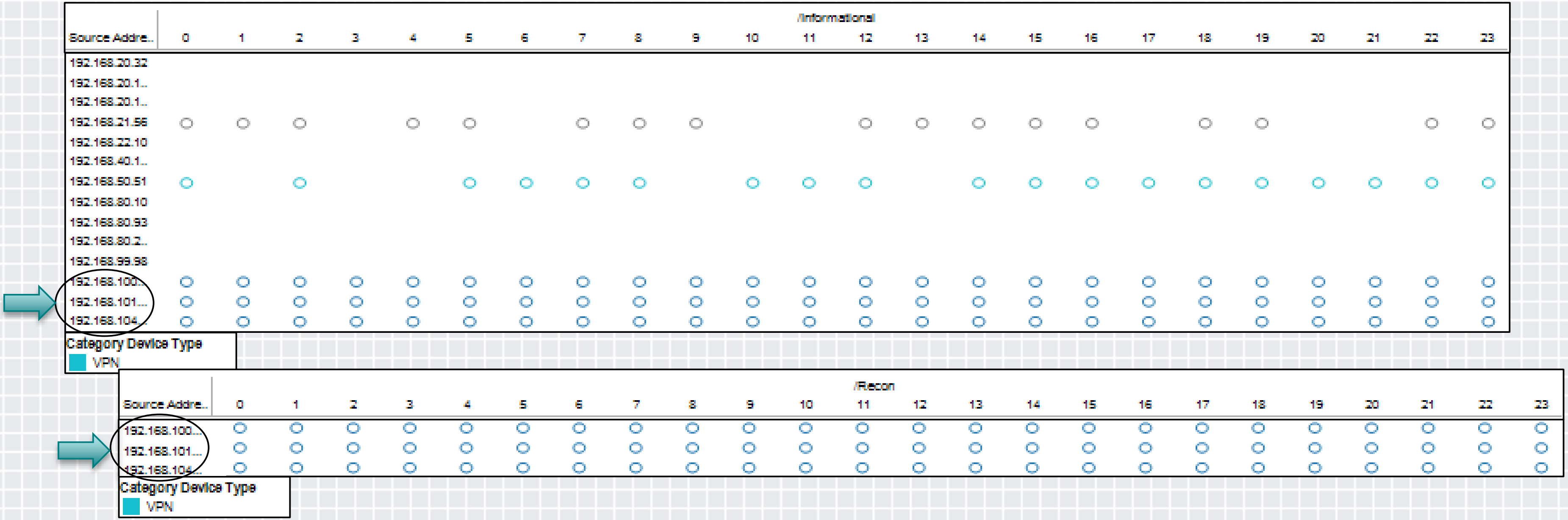


/Informational

Source Addre..	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
192.168.20.32																								
192.168.20.1..																								
192.168.20.1..																								
192.168.21.56	○	○	○		○	○		○	○	○			○	○	○	○	○		○	○			○	○
192.168.22.10																								
192.168.40.1..																								
192.168.50.51	○		○			○	○	○	○		○	○	○		○	○	○	○	○	○	○	○	○	○
192.168.80.10																								
192.168.80.93																								
192.168.80.2..																								
192.168.99.98																								
192.168.100....	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
192.168.101....	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
192.168.104....	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Category Device Type
🟦 VPN

Overlay VPN Source with Recon Events



Correlate two sources of information to identify atypical behavior

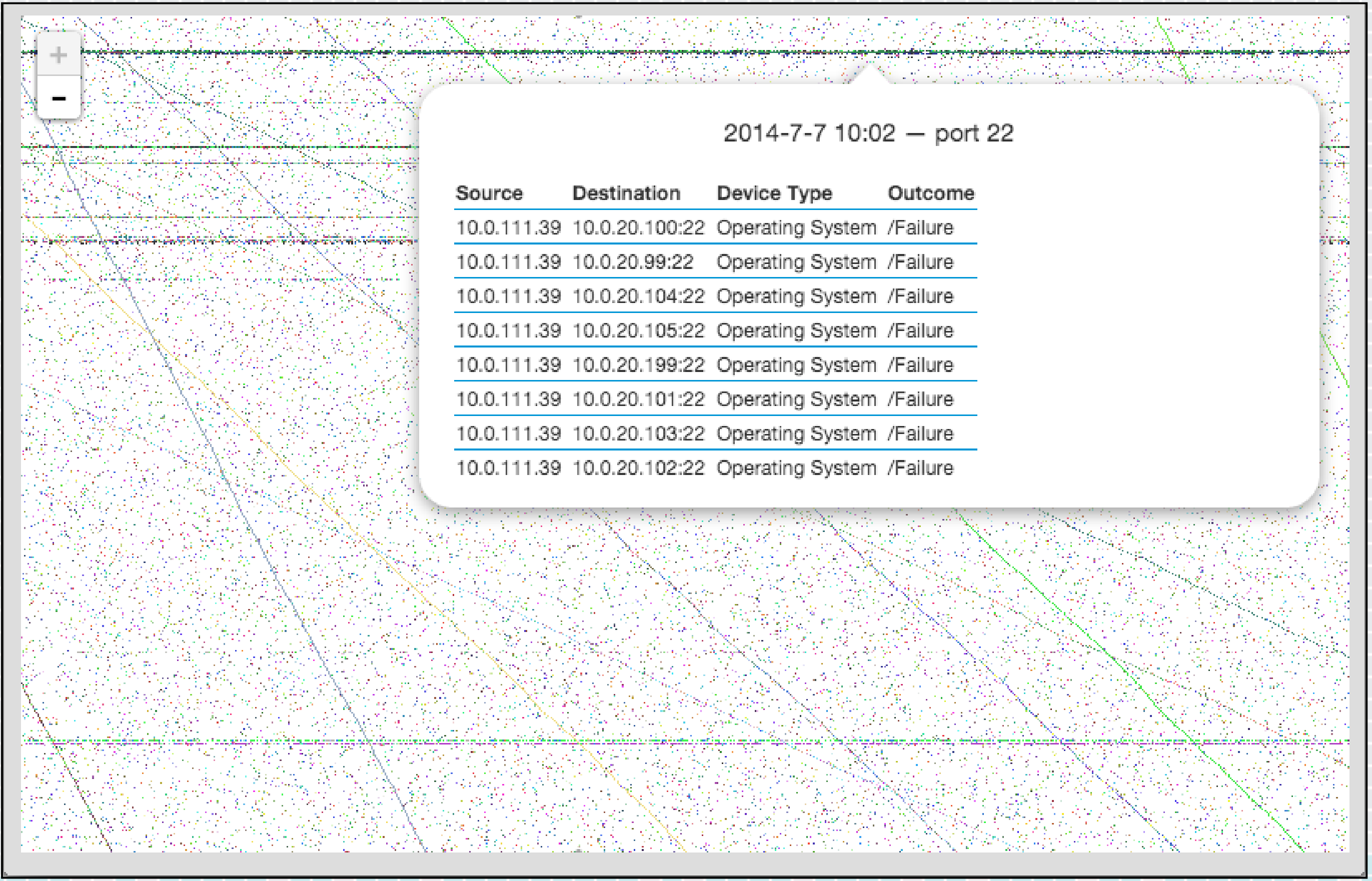
RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Case 5: Advanced Analysis for the Hunt Team

Drilldown Reveals Subtle Patterns



2014-7-7 10:02 — port 22

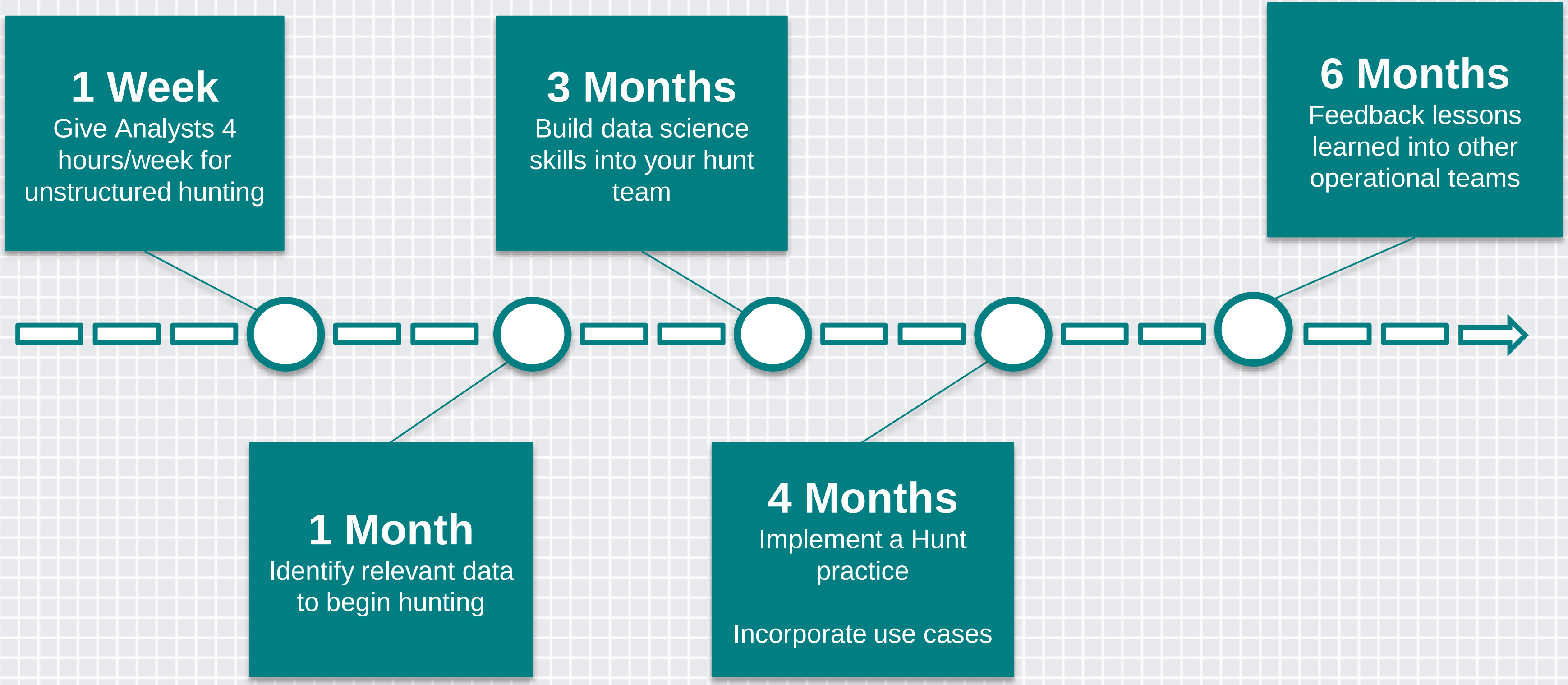
Source	Destination	Device Type	Outcome
10.0.111.39	10.0.20.100:22	Operating System	/Failure
10.0.111.39	10.0.20.99:22	Operating System	/Failure
10.0.111.39	10.0.20.104:22	Operating System	/Failure
10.0.111.39	10.0.20.105:22	Operating System	/Failure
10.0.111.39	10.0.20.199:22	Operating System	/Failure
10.0.111.39	10.0.20.101:22	Operating System	/Failure
10.0.111.39	10.0.20.103:22	Operating System	/Failure
10.0.111.39	10.0.20.102:22	Operating System	/Failure

Horizontal line denotes large scale brute force attempts

In Closing

- Defining the “Hunt Team”
- Leveraging “Data” and Security Analytics
- An internal analytics prototype
- Use cases for the hunt team

Apply What You Have Learned Today



1 Week
Give Analysts 4 hours/week for unstructured hunting

1 Month
Identify relevant data to begin hunting

3 Months
Build data science skills into your hunt team

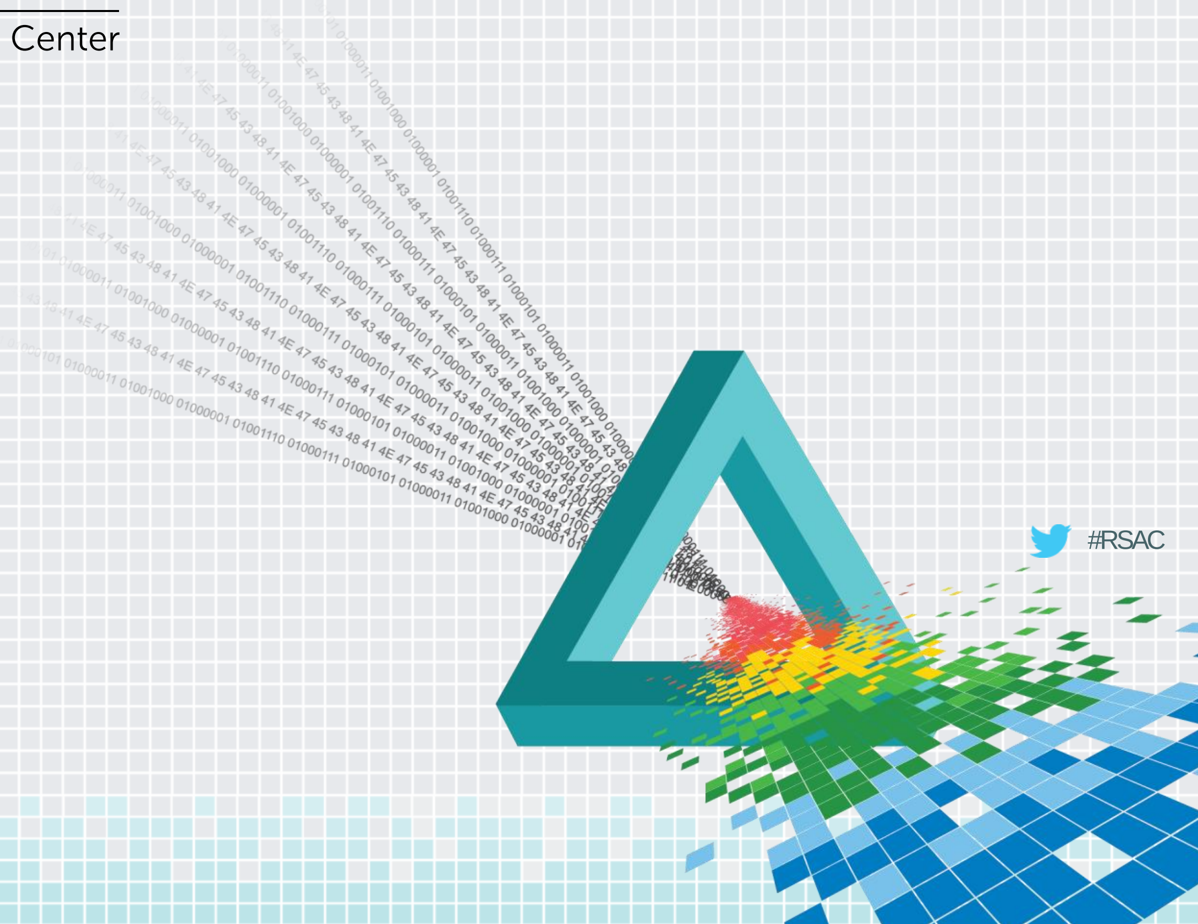
4 Months
Implement a Hunt practice

Incorporate use cases

6 Months
Feedback lessons learned into other operational teams

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Questions?