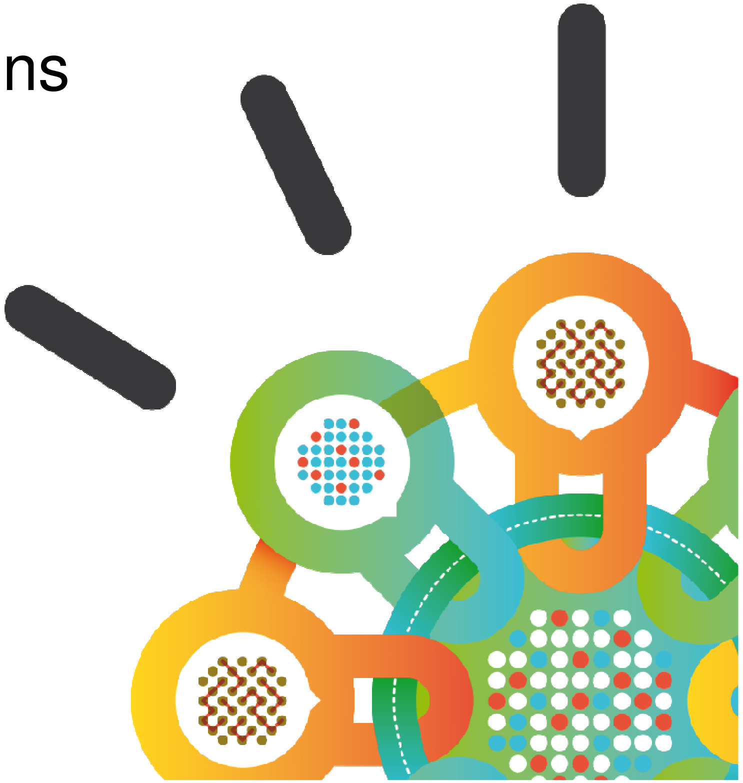
Security Intelligence.
Think Integrated.

QRadar Data Visualizations

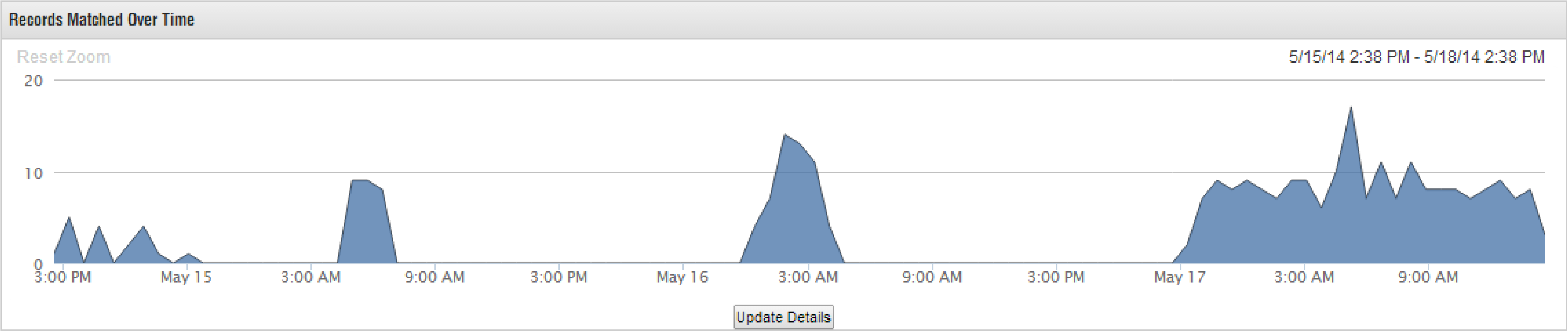
Better insight through better visualizations

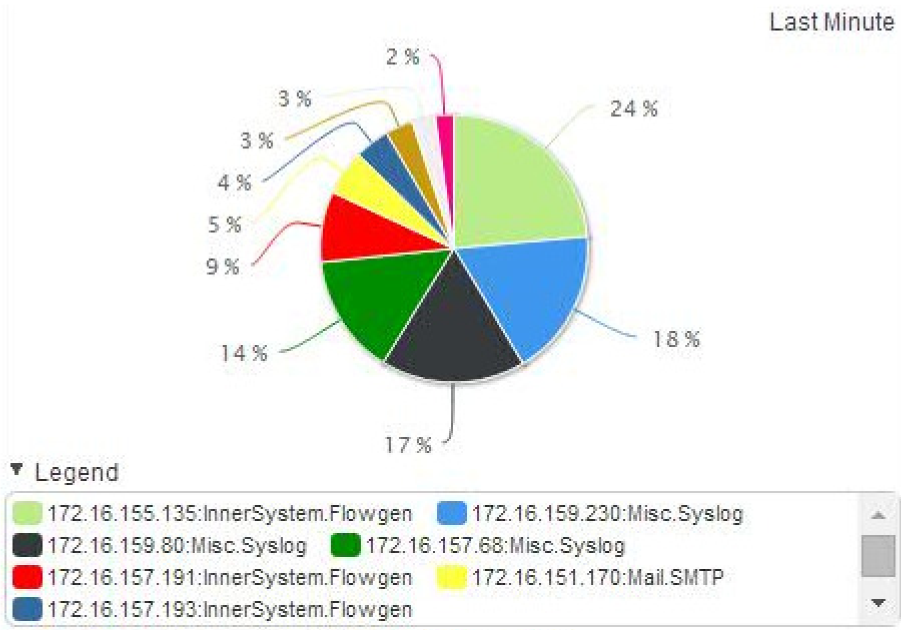
Rick McCaskill
User Experience Lead - ISS

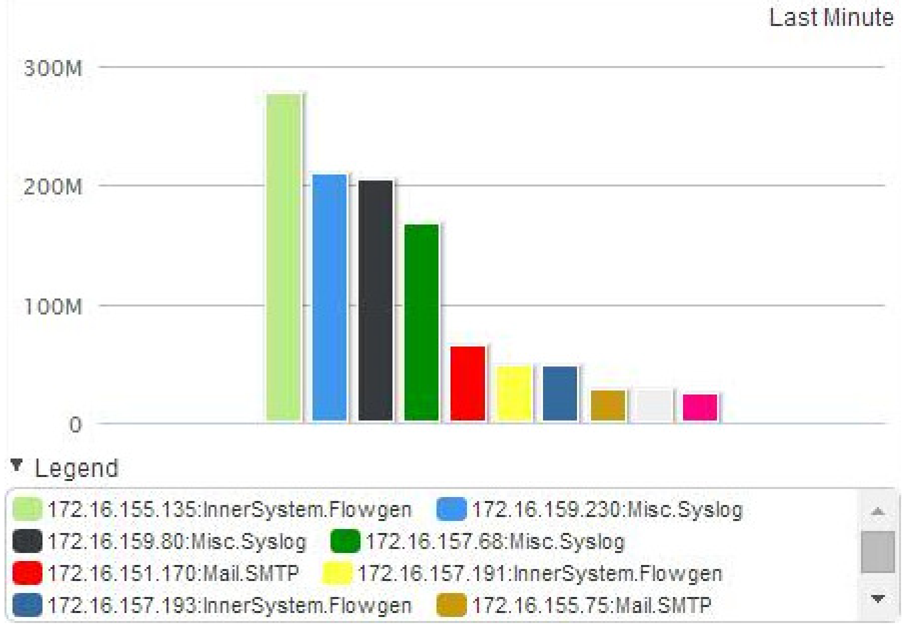
May, 2014

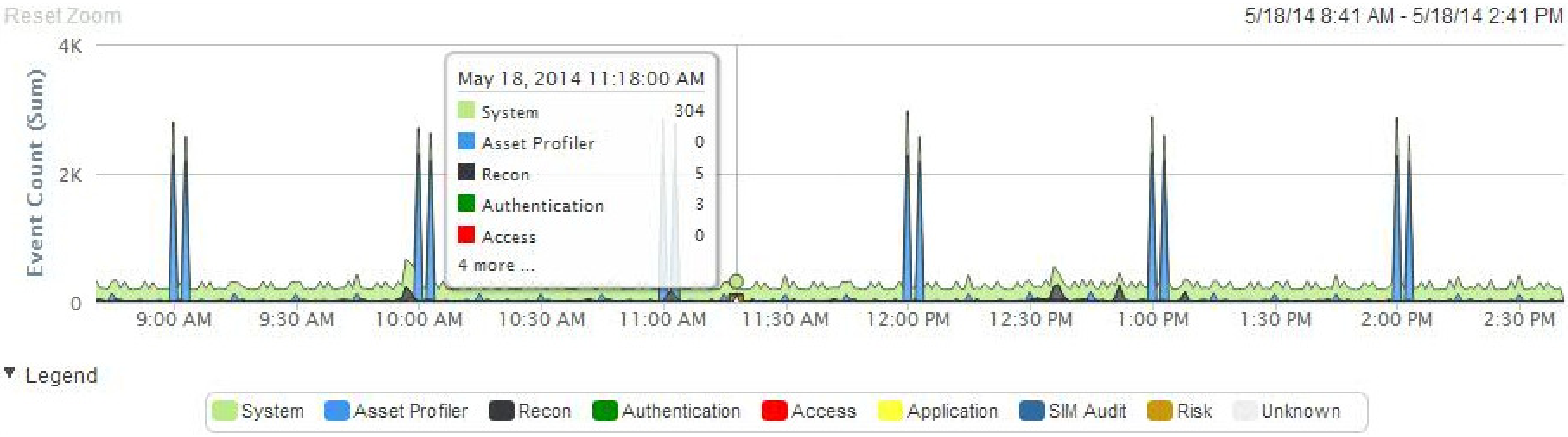


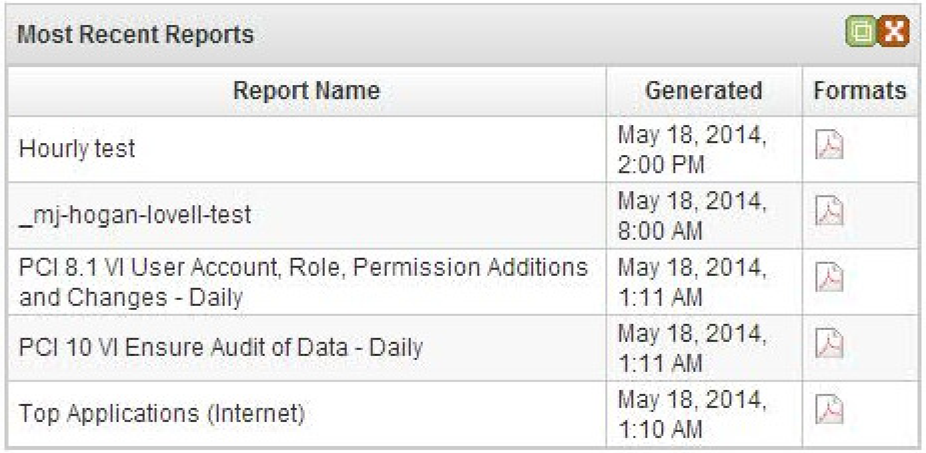
Any effort to help people
understand
the significance of data
by placing it in a
visual
context


Records Matched Over Time
Reset Zoom
5/15/14 2:38 PM - 5/18/14 2:38 PM
20
10
0
3:00 PM
May 15
3:00 AM
9:00 AM
3:00 PM
May 16
3:00 AM
9:00 AM
3:00 PM
May 17
3:00 AM
9:00 AM
Update Details


Last Minute
2 %
3 %
3 %
4 %
5 %
9 %
14 %
17 %
18 %
24 %
Legend
🟩 172.16.155.135:InnerSystem.Flowgen
🟦 172.16.159.230:Misc.Syslog
⬛ 172.16.159.80:Misc.Syslog
🟩 172.16.157.68:Misc.Syslog
🟥 172.16.157.191:InnerSystem.Flowgen
🟨 172.16.151.170:Mail.SMTP
🟦 172.16.157.193:InnerSystem.Flowgen


Last Minute
300M
200M
100M
0
Legend
🟩 172.16.155.135:InnerSystem.Flowgen
🟦 172.16.159.230:Misc.Syslog
⬛ 172.16.159.80:Misc.Syslog
🟩 172.16.157.68:Misc.Syslog
🟥 172.16.151.170:Mail.SMTP
🟨 172.16.157.191:InnerSystem.Flowgen
🟦 172.16.157.193:InnerSystem.Flowgen
🟫 172.16.155.75:Mail.SMTP





Most Recent Reports

Report Name	Generated	Formats
Hourly test	May 18, 2014, 2:00 PM	📄
_mj-hogan-lovell-test	May 18, 2014, 8:00 AM	📄
PCI 8.1 VI User Account, Role, Permission Additions and Changes - Daily	May 18, 2014, 1:11 AM	📄
PCI 10 VI Ensure Audit of Data - Daily	May 18, 2014, 1:11 AM	📄
Top Applications (Internet)	May 18, 2014, 1:10 AM	📄

Visualization Demo

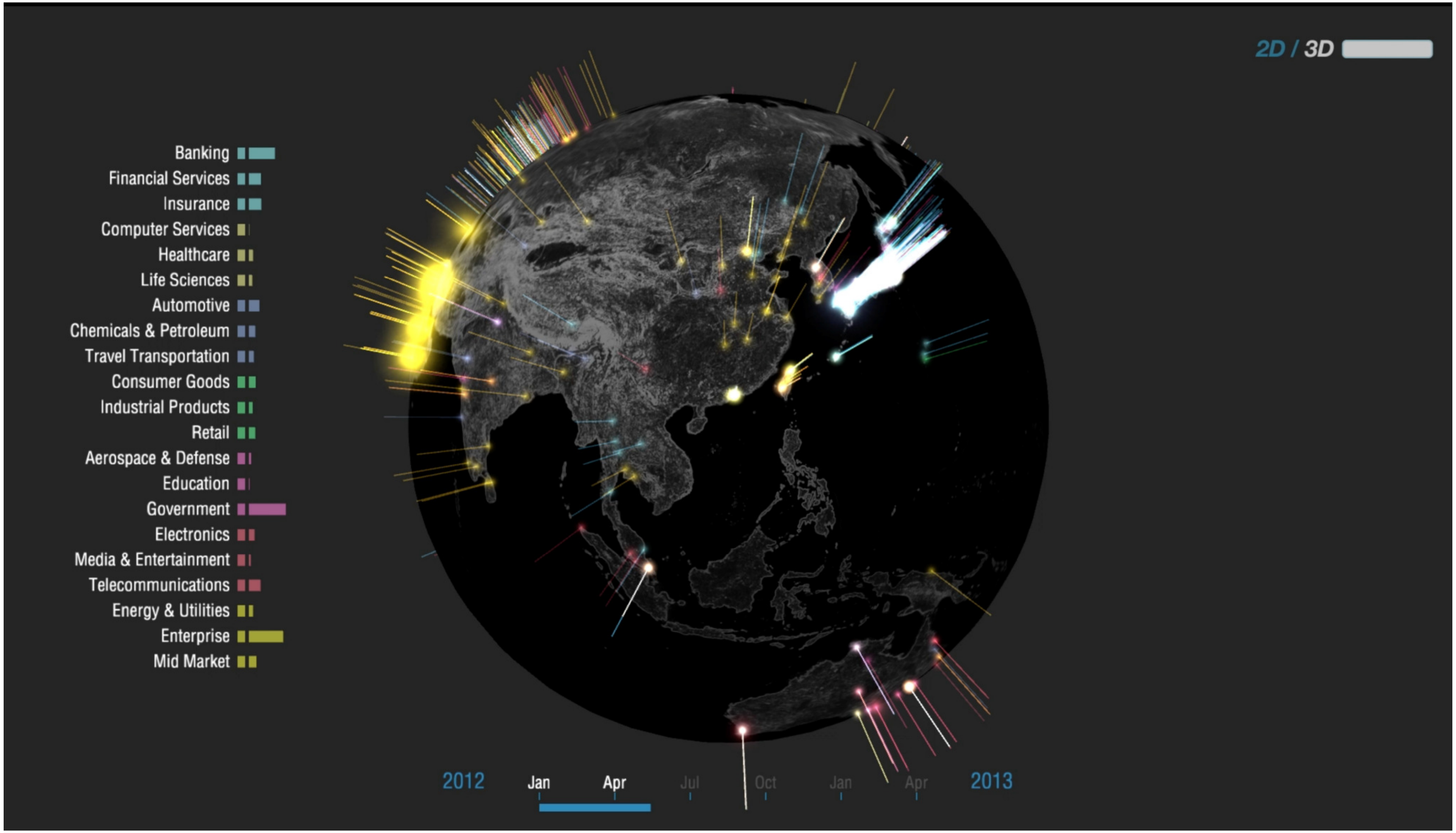
The good stuff

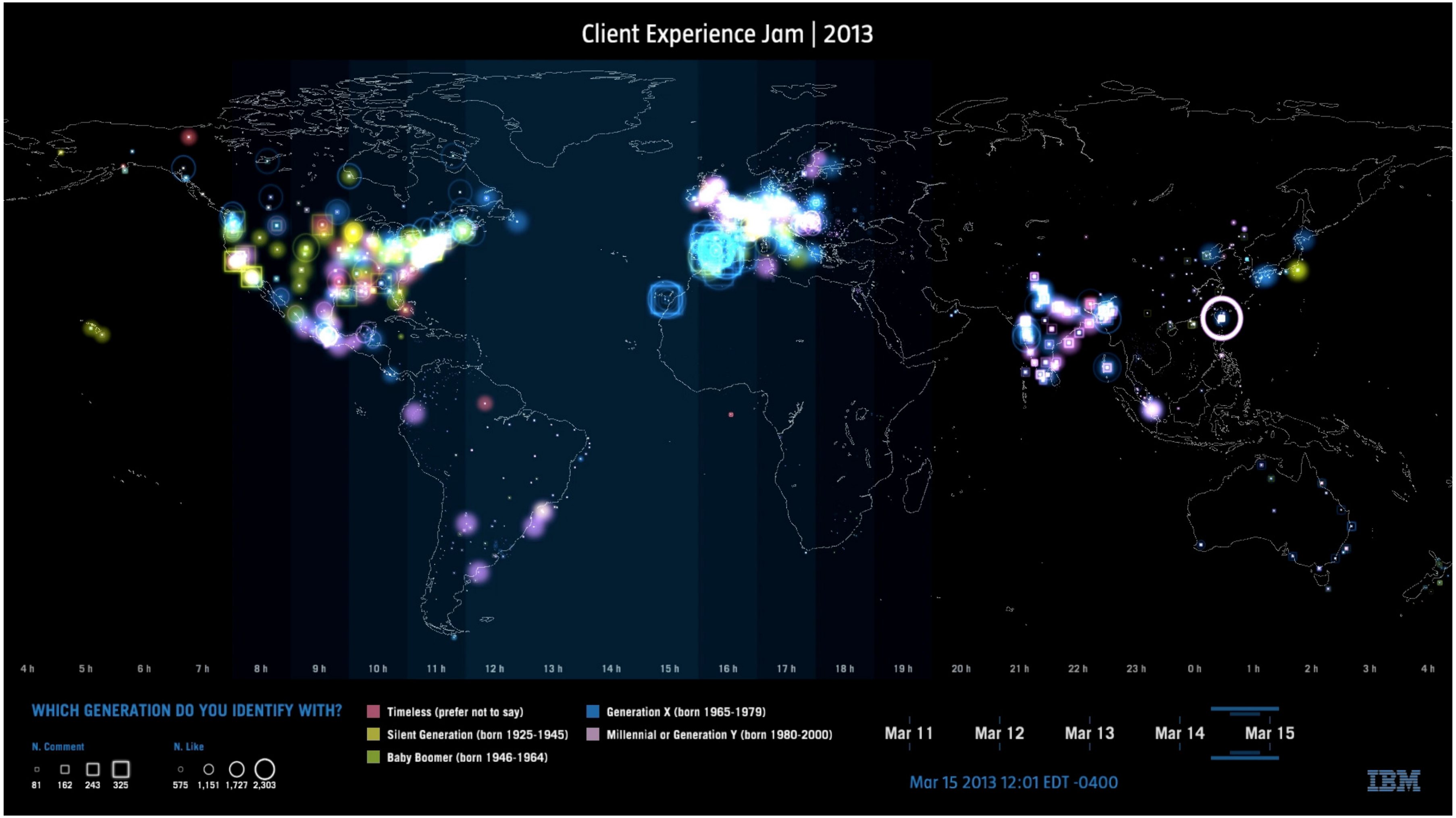
Visualizing Offenses

Visualizing Network Traffic

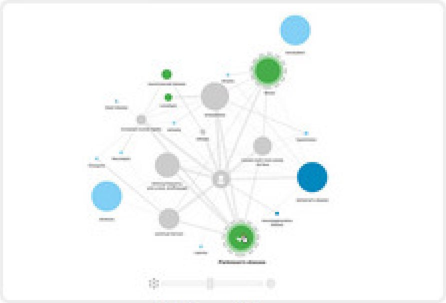
More Visualizations

Visualizations being explored in other areas of IBM

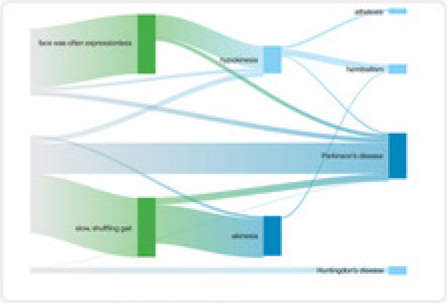

2D / 3D
Banking
Financial Services
Insurance
Computer Services
Healthcare
Life Sciences
Automotive
Chemicals & Petroleum
Travel Transportation
Consumer Goods
Industrial Products
Retail
Aerospace & Defense
Education
Government
Electronics
Media & Entertainment
Telecommunications
Energy & Utilities
Enterprise
Mid Market
2012
Jan
Apr
Jul
Oct
Jan
Apr
2013


Client Experience Jam | 2013
4 h
5 h
6 h
7 h
8 h
9 h
10 h
11 h
12 h
13 h
14 h
15 h
16 h
17 h
18 h
19 h
20 h
21 h
22 h
23 h
0 h
1 h
2 h
3 h
4 h
WHICH GENERATION DO YOU IDENTIFY WITH?
N. Comment
81
162
243
325
N. Like
575
1,151
1,727
2,303
Timeless (prefer not to say)
Silent Generation (born 1925-1945)
Baby Boomer (born 1946-1964)
Generation X (born 1965-1979)
Millennial or Generation Y (born 1980-2000)
Mar 11
Mar 12
Mar 13
Mar 14
Mar 15
Mar 15 2013 12:01 EDT -0400
IBM

Watson Paths



Network.jpg



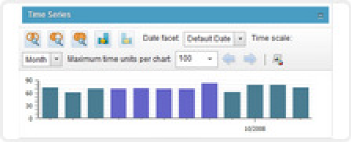
Sankey-Dia__.jpg

Hypotheses
Ewing's sarcoma
Osteoclastoma
Osteogenic sarcoma
Synovial sarcoma
Chondrosarcoma
HIGH
MED
LOW

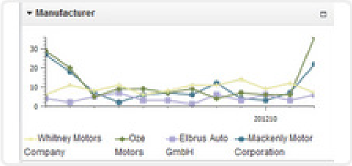
Sunburst.jpg

Watson Content Analytics

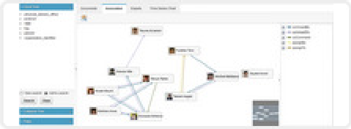
Bar.jpg



Column.jpg



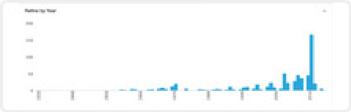
Line.jpg



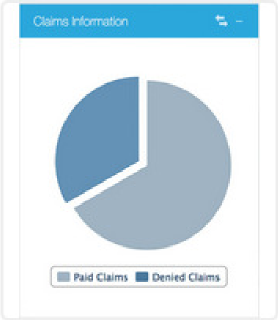
Network.jpg

Watson Explorer

Column.jpg

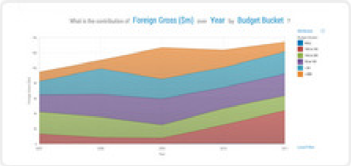


Histogram.jpg

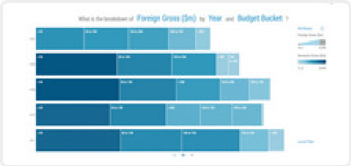


Pie.jpg

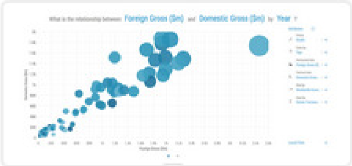
Watson Analytics


What is the distribution of Foreign Gross ($m) over Year by Budget Bucket ?

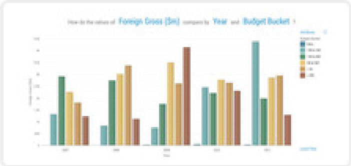
area.jpg


What is the breakdown of Foreign Gross ($m) by Year and Budget Bucket ?

Bar Treema__.jpg


What is the relationship between Foreign Gross ($m) and Domestic Gross ($m) by Year ?

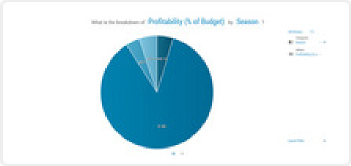
Bubble.jpg


How do the values of Foreign Gross ($m) compare by Year and Budget Bucket ?

Column.jpg

What is the trend of Foreign Gross ($m) over Year by Budget Bucket ?

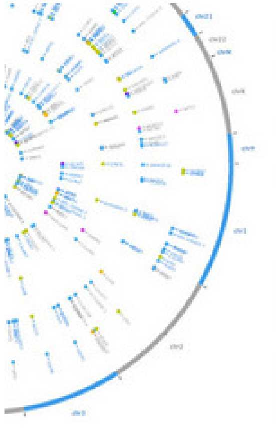
Line.jpg

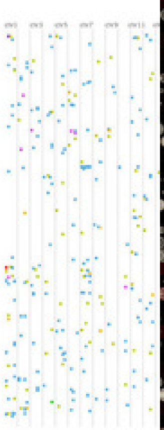

What is the breakdown of Profitability (% of Budget) by Season ?

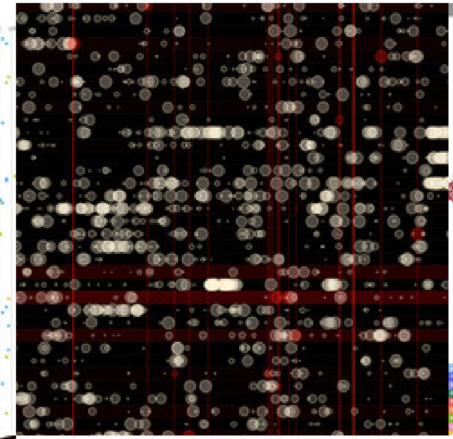
Pie.jpg

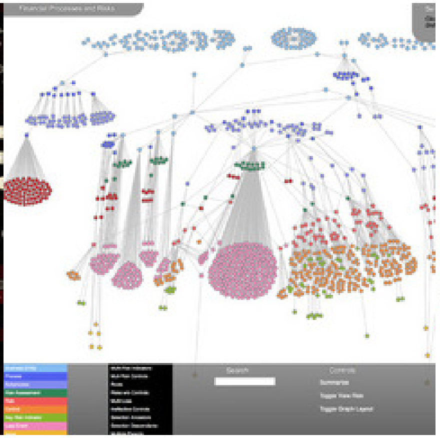
scatter-pl__.jpg

table.jpg



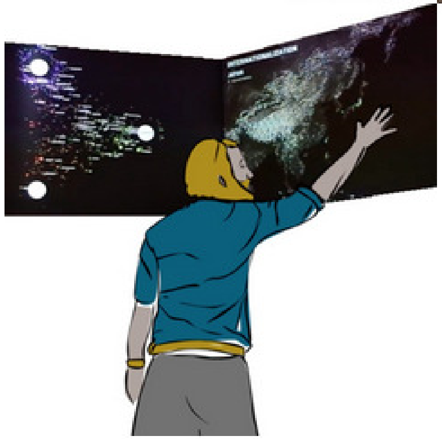






Financial Processes and Risks
Search
Controls

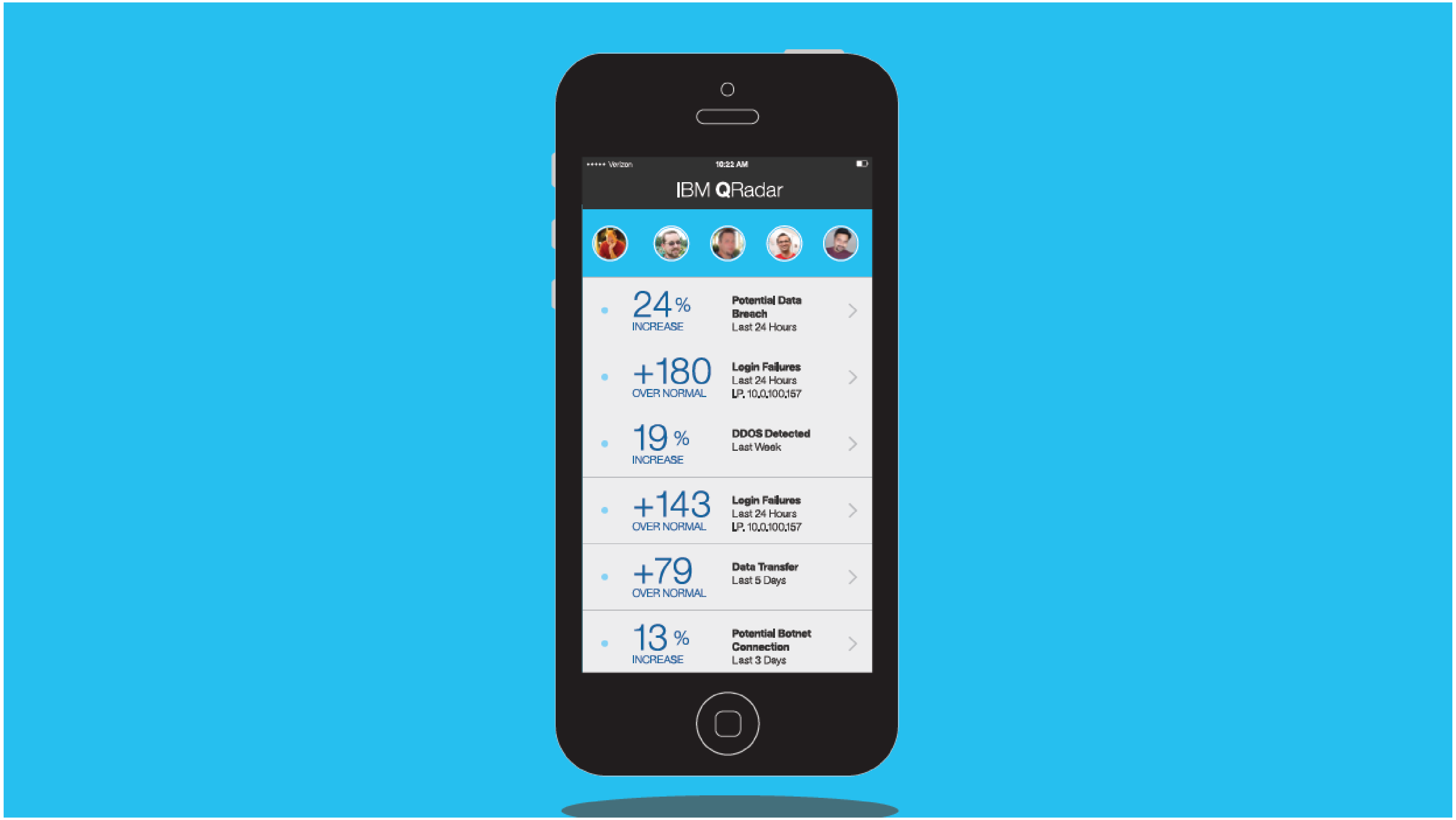
Authors
Bonnie John Brad Myers
Stuart Card
Papers
Applications
Lab Reports
Multimodal UI
Web



INTERNATIONALIZATION

QRadar Reimagined

IBM Design Thinking Exercise with the Austin Design Studio



••••• Verizon 10:22 AM

IBM QRadar

24 % INCREASE — Potential Data Breach, Last 24 Hours

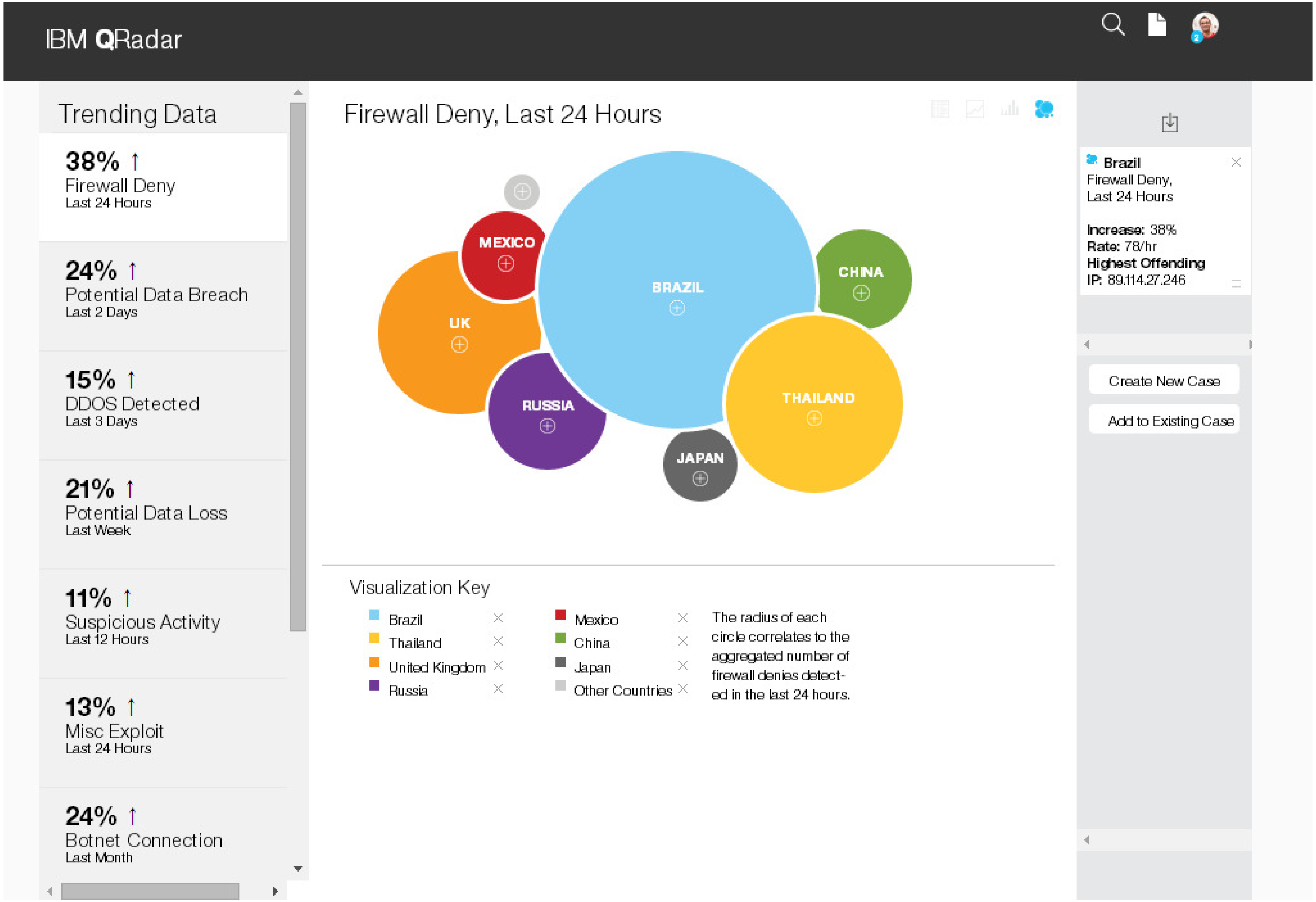
+180 OVER NORMAL — Login Failures, Last 24 Hours, I.P. 10.0.100.157

19 % INCREASE — DDOS Detected, Last Week

+143 OVER NORMAL — Login Failures, Last 24 Hours, I.P. 10.0.100.157

+79 OVER NORMAL — Data Transfer, Last 5 Days

13 % INCREASE — Potential Botnet Connection, Last 3 Days



IBM QRadar

Trending Data

38% ↑
Firewall Deny
Last 24 Hours

24% ↑
Potential Data Breach
Last 2 Days

15% ↑
DDOS Detected
Last 3 Days

21% ↑
Potential Data Loss
Last Week

11% ↑
Suspicious Activity
Last 12 Hours

13% ↑
Misc Exploit
Last 24 Hours

24% ↑
Botnet Connection
Last Month

Firewall Deny, Last 24 Hours

Visualization Key

🟦 Brazil ×
🟨 Thailand ×
🟧 United Kingdom ×
🟪 Russia ×
🟥 Mexico ×
🟩 China ×
⬛ Japan ×
⬜ Other Countries ×

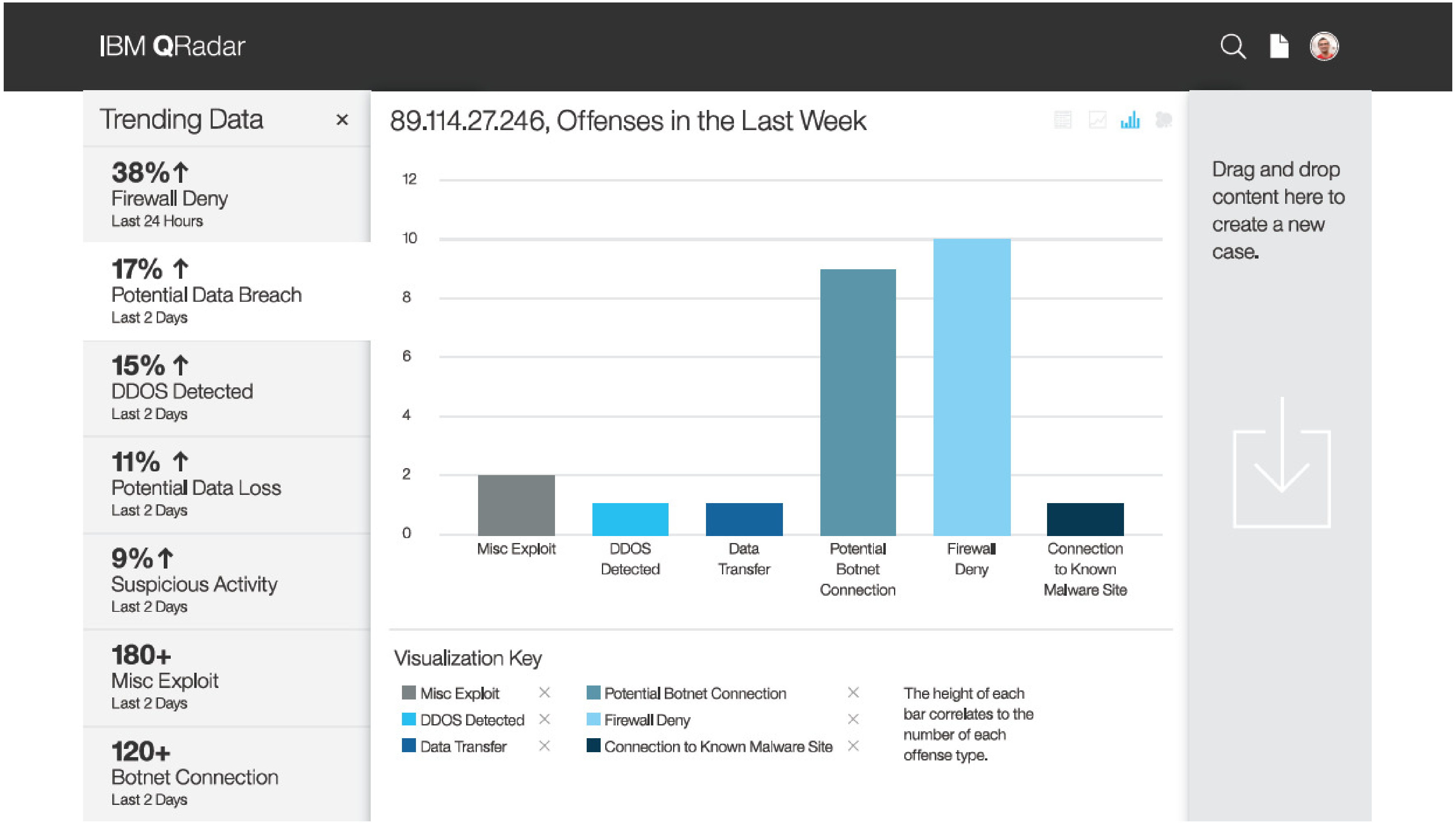
The radius of each circle correlates to the aggregated number of firewall denies detected in the last 24 hours.

Brazil
Firewall Deny,
Last 24 Hours

Increase: 38%
Rate: 78/hr
Highest Offending IP: 89.114.27.246

Create New Case

Add to Existing Case



IBM QRadar

Trending Data ×

38%↑ Firewall Deny
Last 24 Hours

17% ↑ Potential Data Breach
Last 2 Days

15% ↑ DDOS Detected
Last 2 Days

11% ↑ Potential Data Loss
Last 2 Days

9%↑ Suspicious Activity
Last 2 Days

180+ Misc Exploit
Last 2 Days

120+ Botnet Connection
Last 2 Days

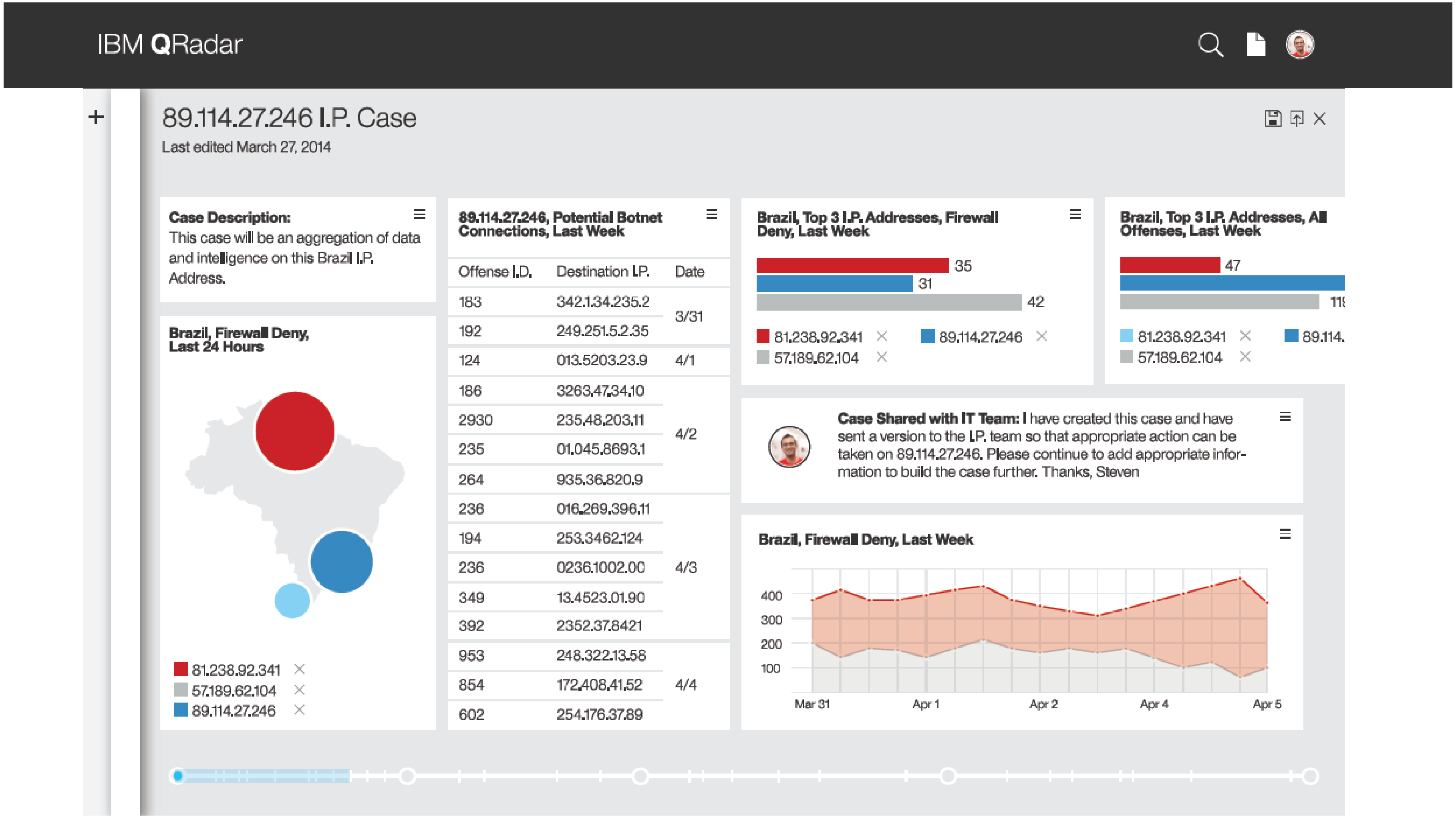
89.114.27.246, Offenses in the Last Week

Visualization Key

- ■ Misc Exploit ×
- ■ DDOS Detected ×
- ■ Data Transfer ×
- ■ Potential Botnet Connection ×
- ■ Firewall Deny ×
- ■ Connection to Known Malware Site ×

The height of each bar correlates to the number of each offense type.

Drag and drop content here to create a new case.



89.114.27.246 I.P. Case

Last edited March 27, 2014

Case Description: This case will be an aggregation of data and intelligence on this Brazil I.P. Address.

89.114.27.246, Potential Botnet Connections, Last Week

Offense I.D.	Destination I.P.	Date
183	342.1.34.235.2	3/31
192	249.251.5.2.35	
124	013.5203.23.9	4/1
186	3263.47.34.10	4/2
2930	235.48.203.11	
235	01.045.8693.1	
264	935.36.820.9	
236	016.269.396.11	4/3
194	253.3462.124	
236	0236.1002.00	
349	13.4523.01.90	
392	2352.37.8421	
953	248.322.13.58	4/4
854	172.408.41.52	
602	254.176.37.89	

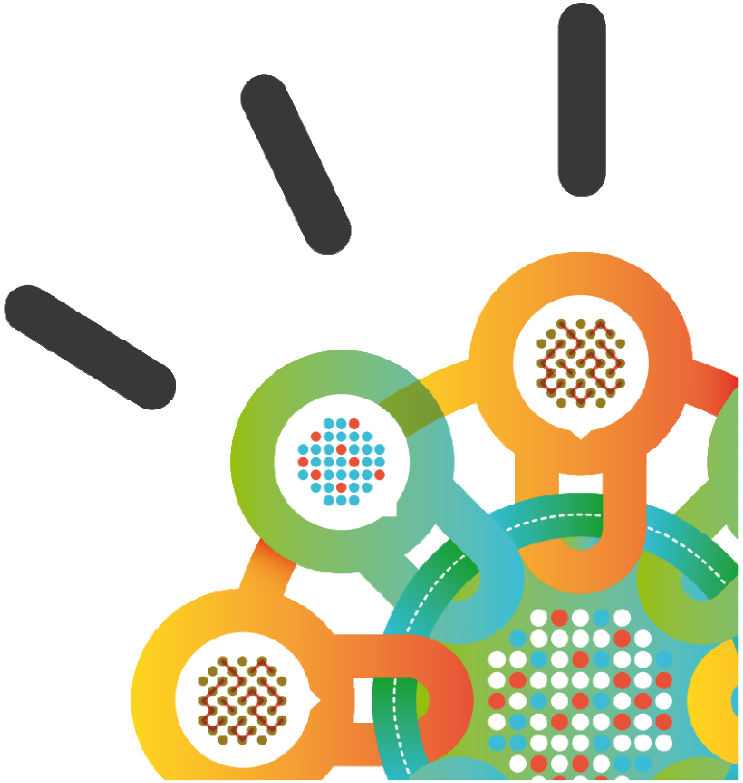
Case Shared with IT Team: I have created this case and have sent a version to the I.P. team so that appropriate action can be taken on 89.114.27.246. Please continue to add appropriate information to build the case further. Thanks, Steven

Security Intelligence.
Think Integrated.

Come and find me,

Rick McCaskill.

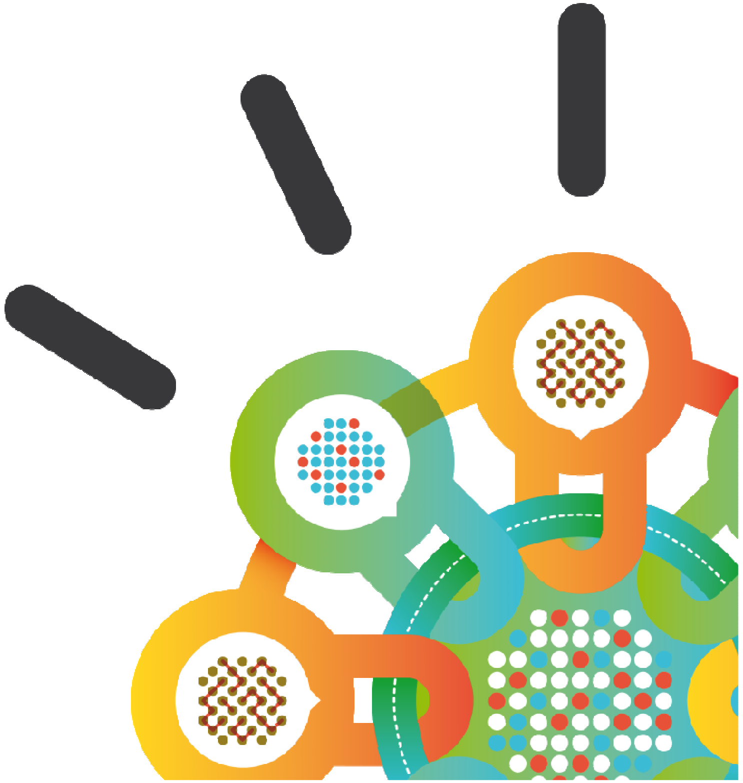
Let's talk about what visualizations can make your work easier.



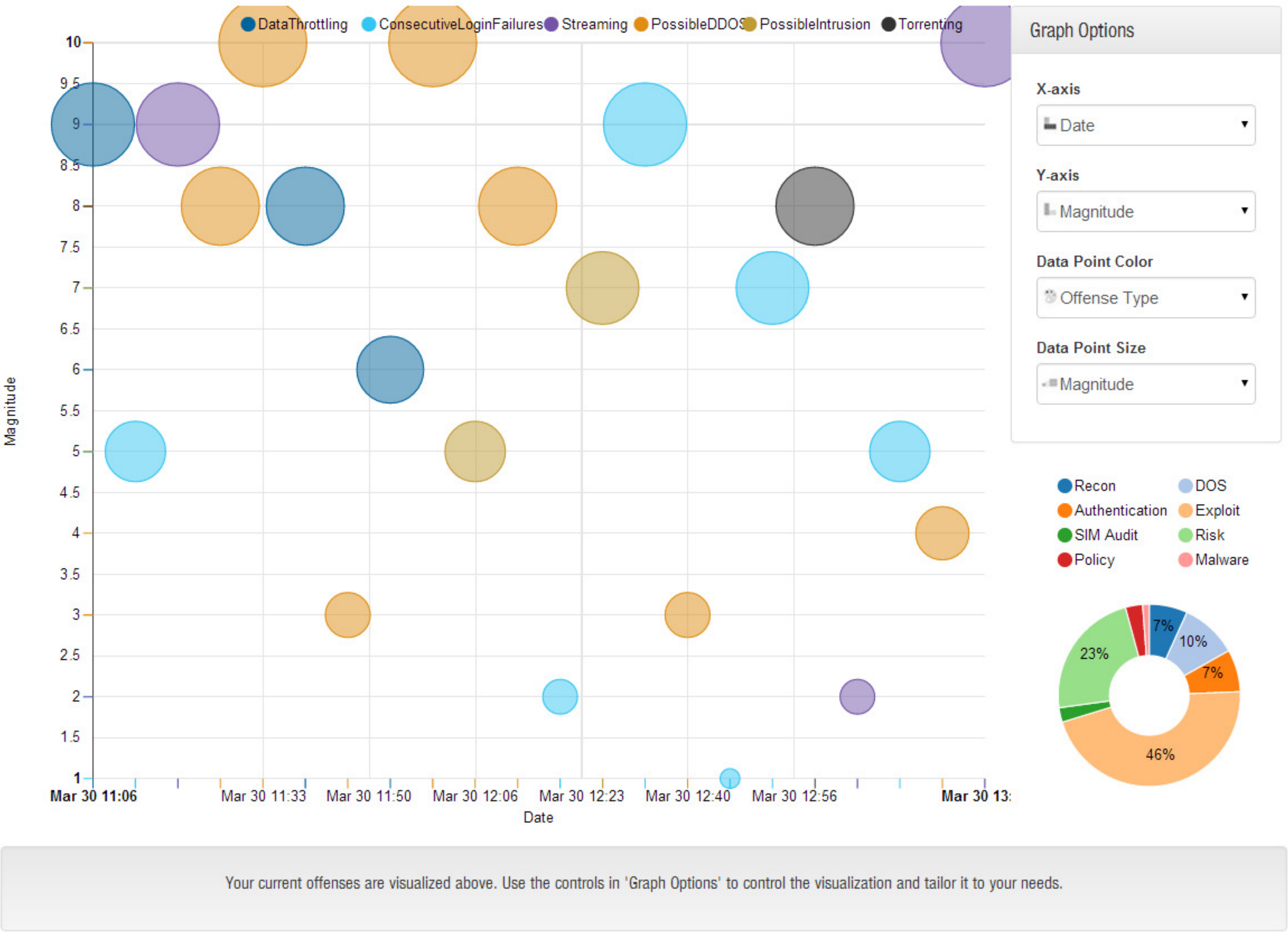
ibm.com/security

Security Intelligence.
Think Integrated.

Back-up slides
(in case of demo issues)



Offenses



Graph Options

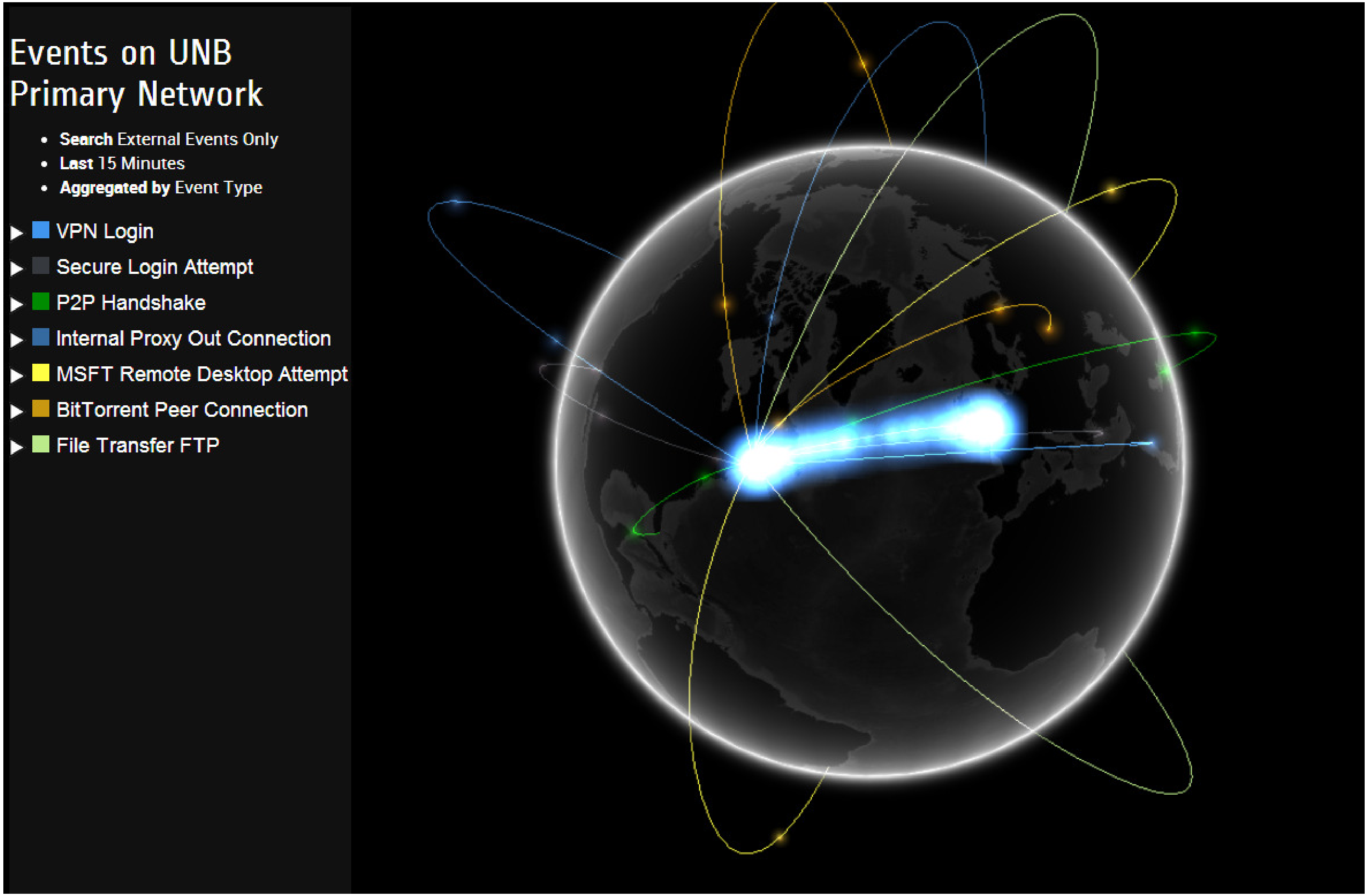
X-axis
Date

Y-axis
Magnitude

Data Point Color
Offense Type

Data Point Size
Magnitude

Your current offenses are visualized above. Use the controls in 'Graph Options' to control the visualization and tailor it to your needs.



Events on UNB Primary Network

- **Search** External Events Only
- **Last** 15 Minutes
- **Aggregated by** Event Type

▶ 🟦 VPN Login

▶ ⬛ Secure Login Attempt

▶ 🟩 P2P Handshake

▶ 🟦 Internal Proxy Out Connection

▶ 🟨 MSFT Remote Desktop Attempt

▶ 🟧 BitTorrent Peer Connection

▶ 🟩 File Transfer FTP