IBM Security

State of NC QRadar Workshop

Threat Hunting, Advanced Analytics, Augmented Intelligence, and Automated Response

Michael Melore, CISSP
IBM Cyber Security Advisor

Follow us on Twitter **@MichaelMelore**

October 2017

IBM

A tremendous amount of security knowledge is created for human consumption **but most of it is untapped**

- Security events and alerts
- Logs and configuration data
- User and network activity
- Threat and vulnerability feeds

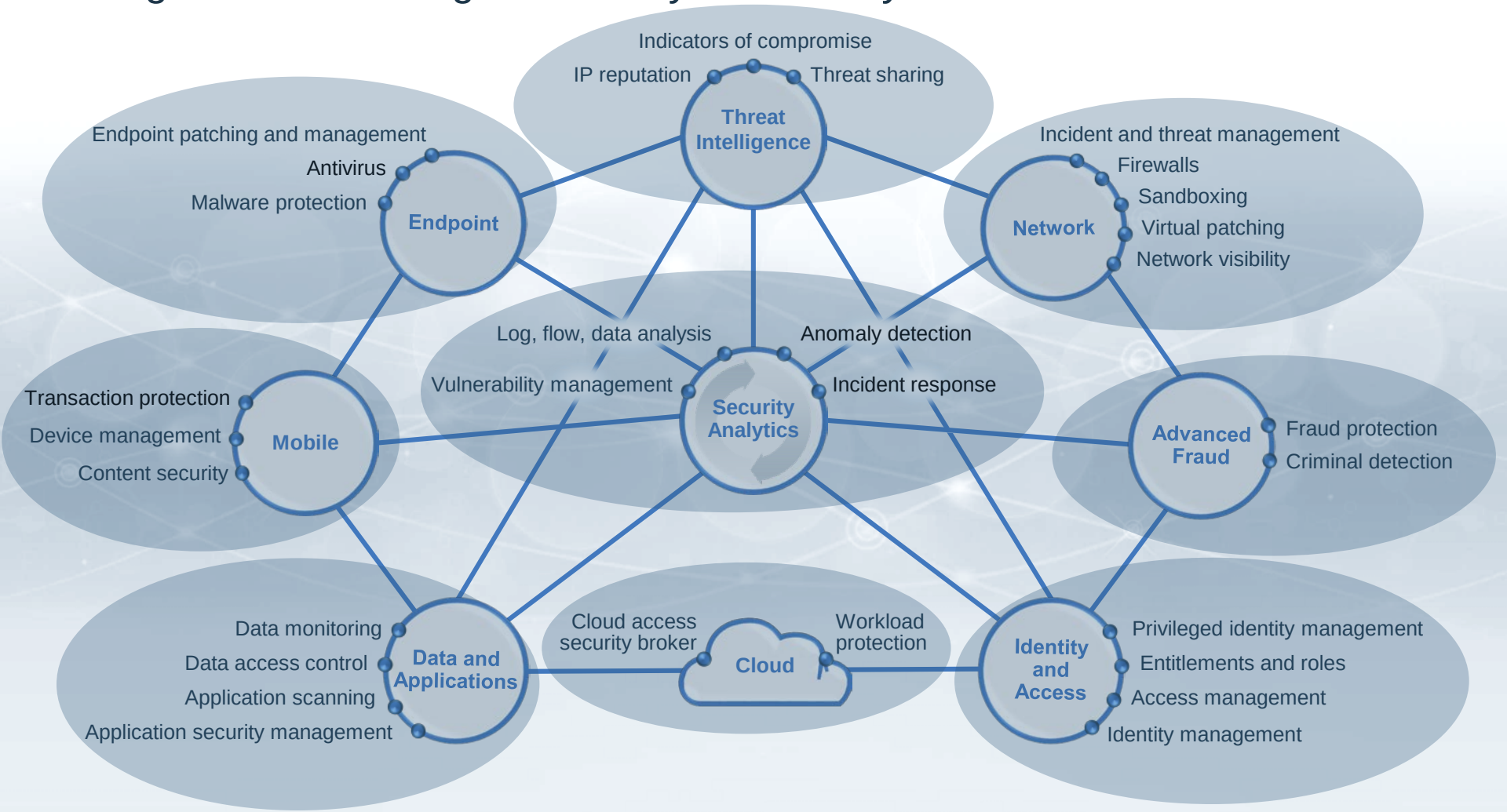
A universe of security knowledge Dark to your defenses

Typical organizations leverage only 8% of this content*

Examples include:

- Research documents
- Industry publications
- Forensic information
- Threat intelligence commentary
- Conference presentations
- Analyst reports
- Webpages
- Wikis
- Blogs
- News sources
- Newsletters
- Tweets

Integrated and intelligent security immune system



Today’s challenges

Escalating Attacks

- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

Increasing Complexity

- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

Resource Constraints

- Struggling security teams
- Too much data with limited manpower and skills to manage it all
- Managing and monitoring increasing compliance demands

Workflow

Advanced Analytics

DETECT

Cognitive

ENRICH

Threat Hunting

INVESTIGATE

ORCHESTRATE

What is Needed to Conduct Threat Hunting

Known Indicators

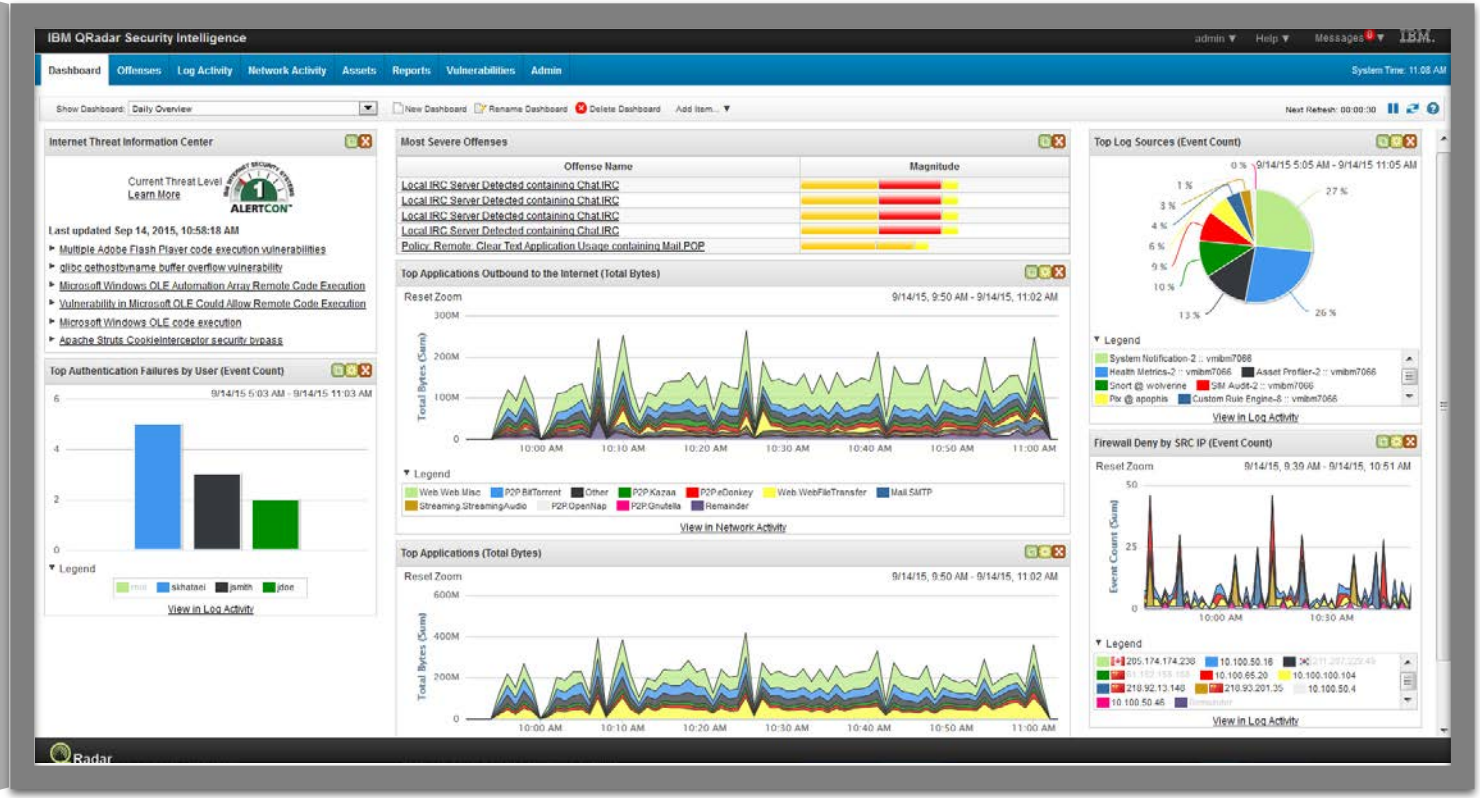
Foundational Data

Anomaly Detection

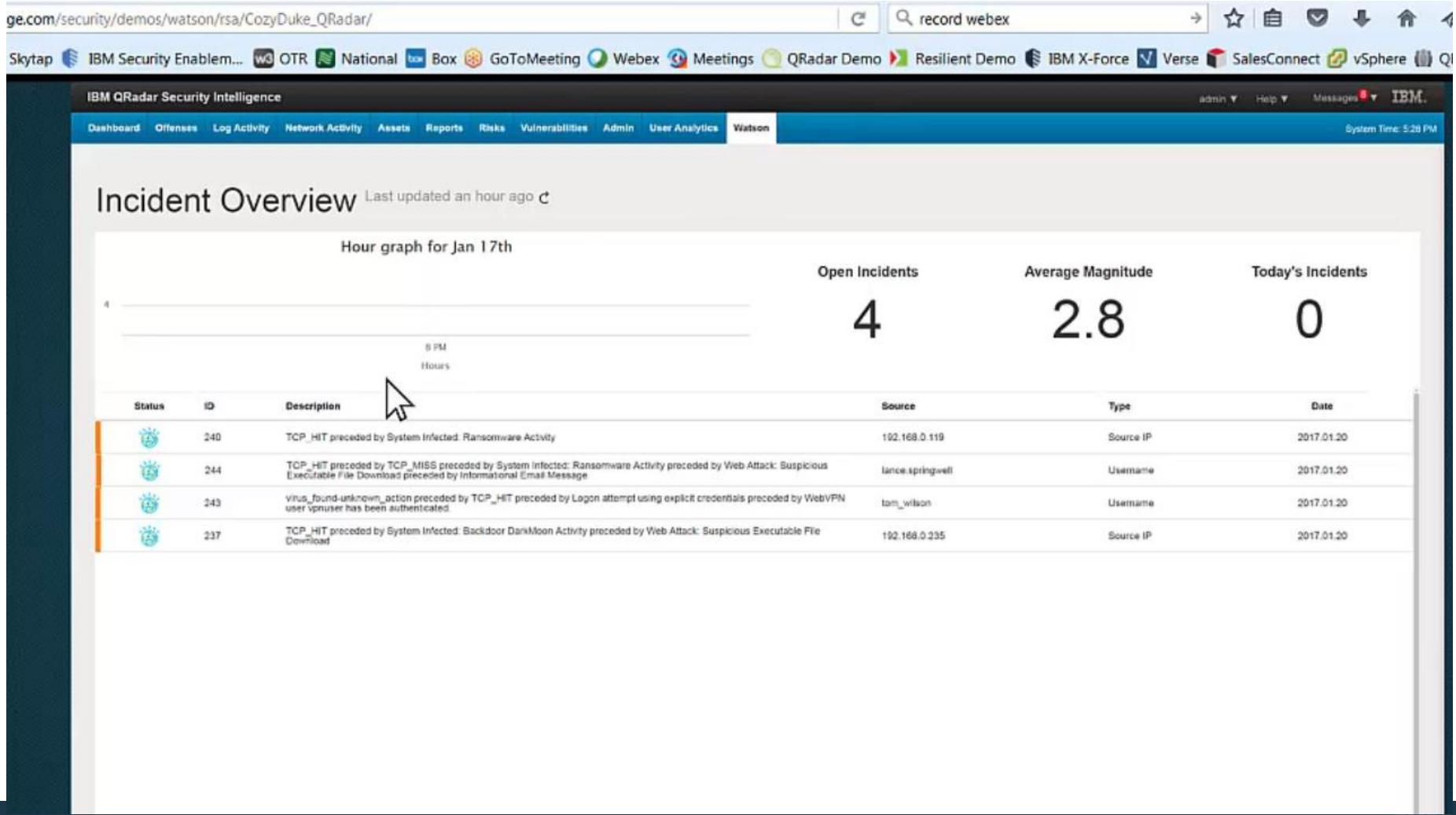
Organization + Discovery

QRadar: An integrated, unified architecture in a single web-based console

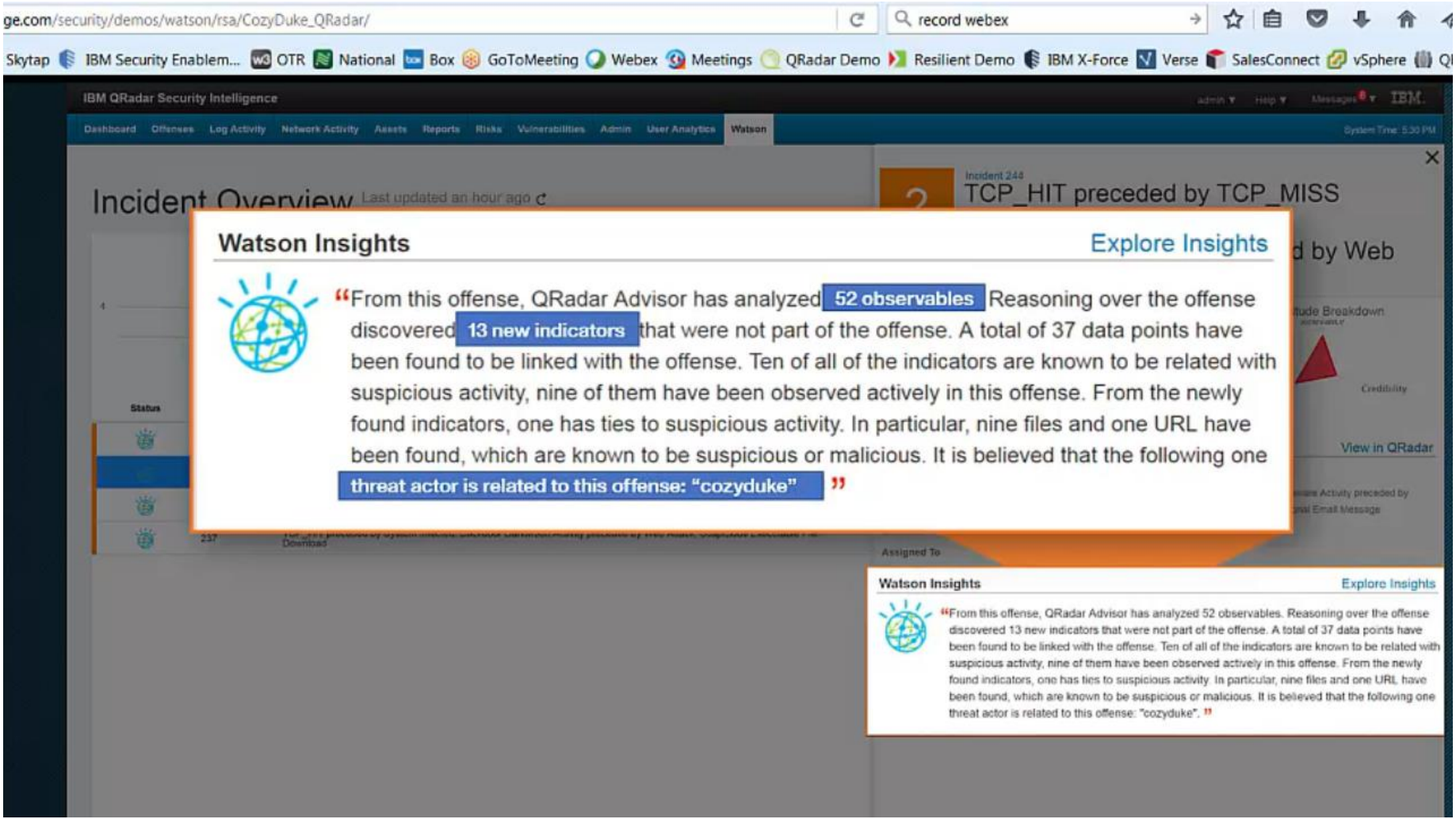
- Log Management
- Security Intelligence and Sense Analytics
- Network Activity Monitoring
- Vulnerability and Risk Management
- Network Forensics
- Incident Response



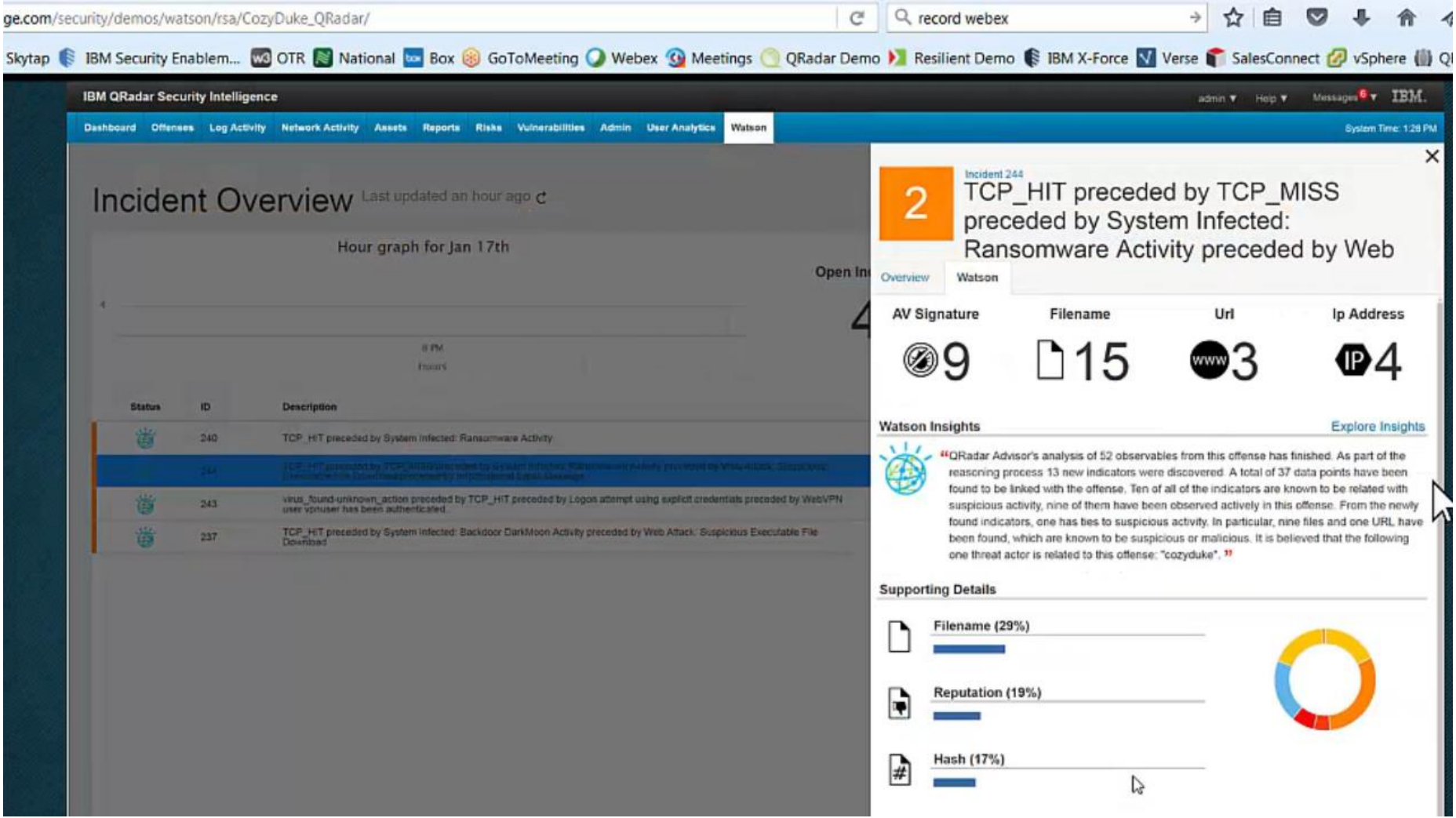
QRadar: Watson Advisor



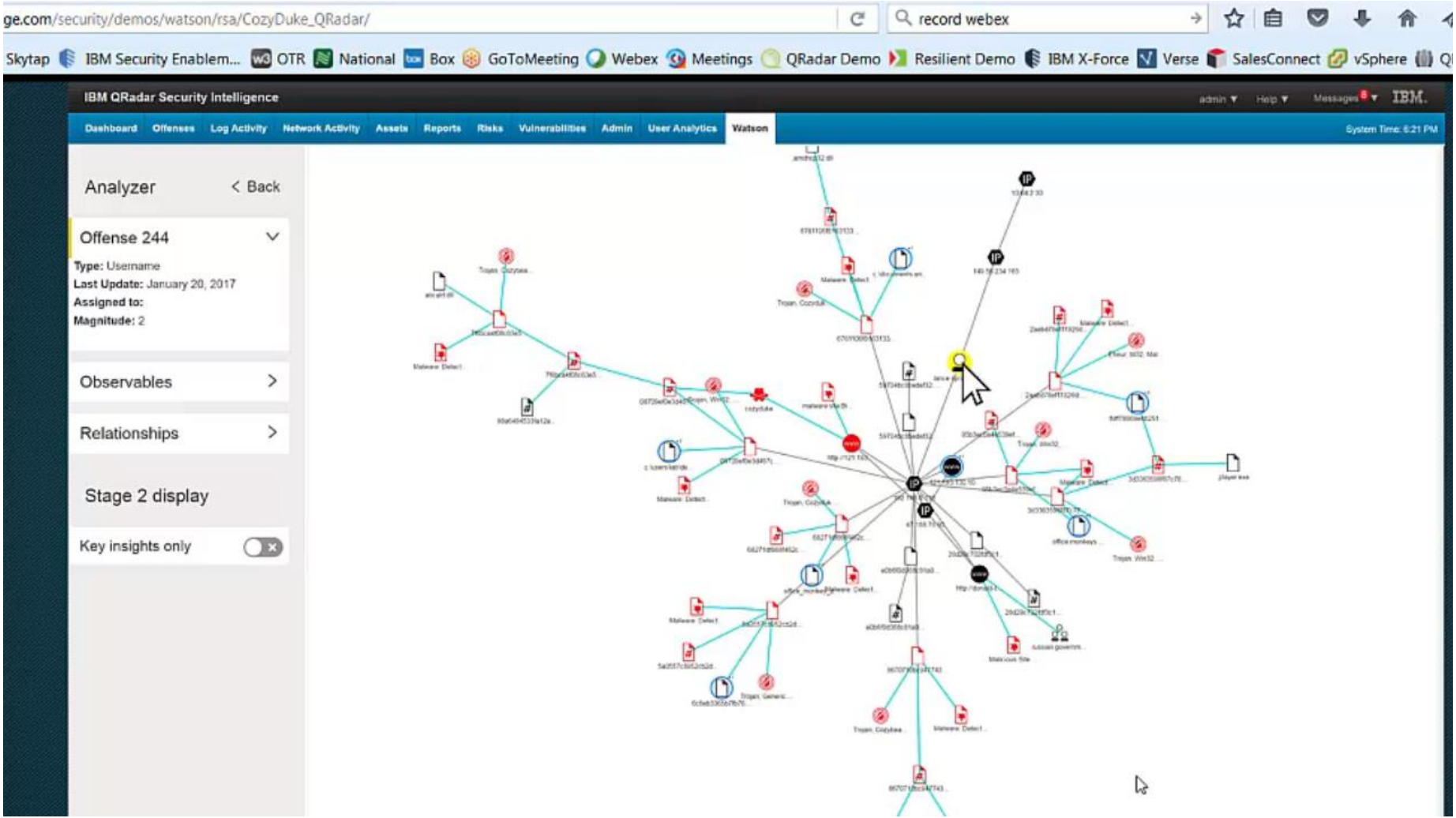
QRadar: Watson Advisor



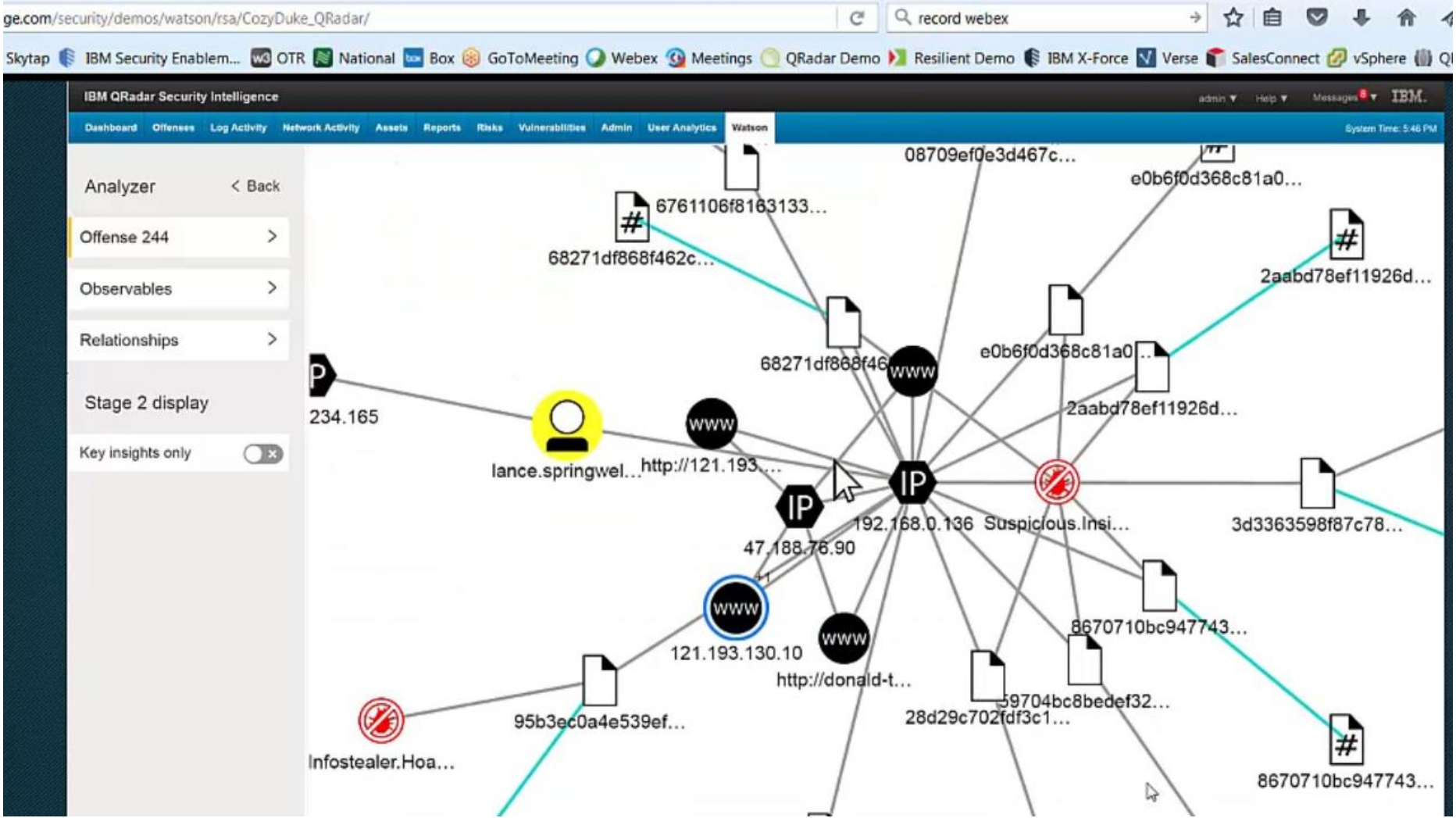
QRadar: Watson Advisor



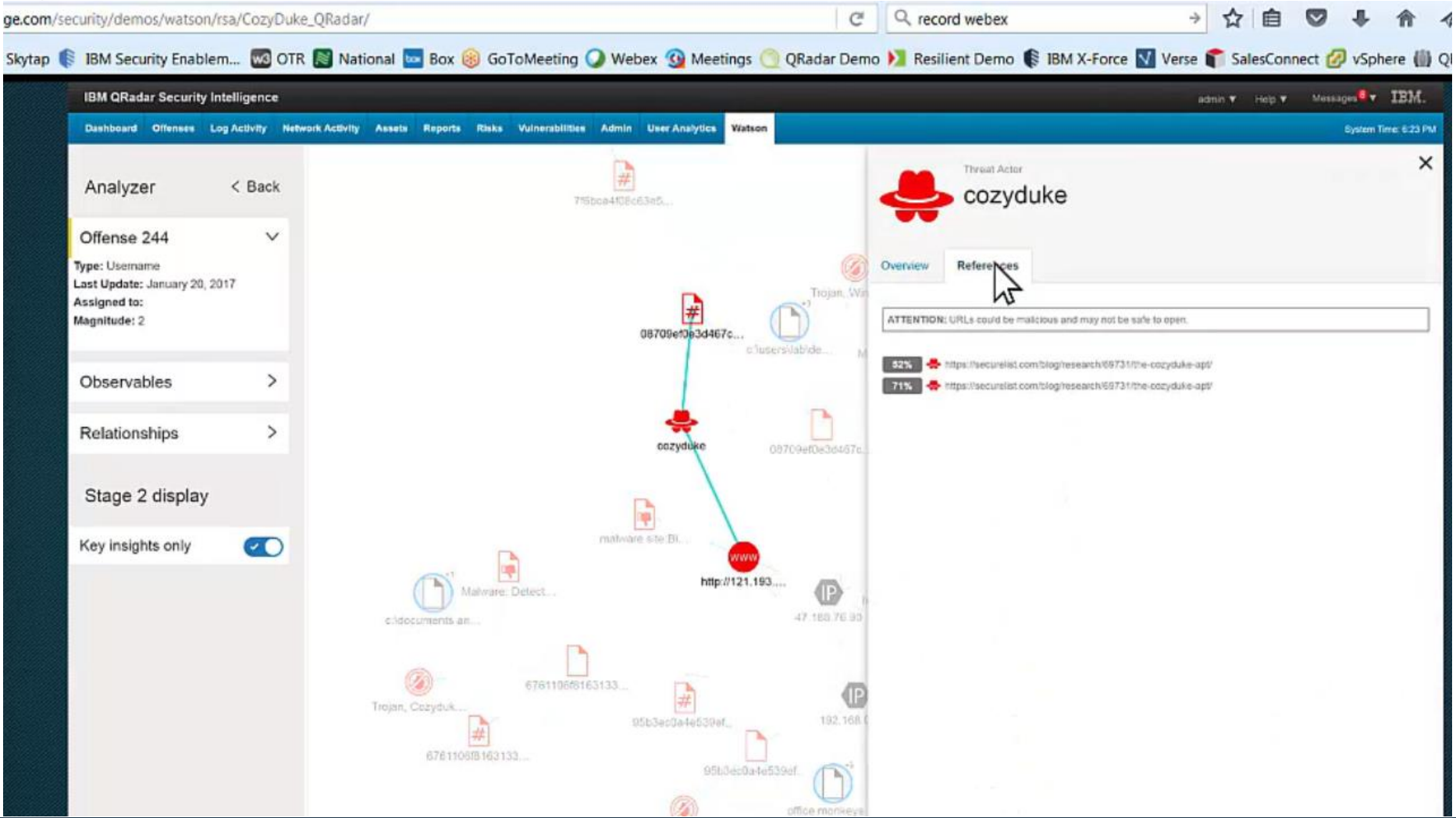
QRadar: Watson Advisor – Patient 0



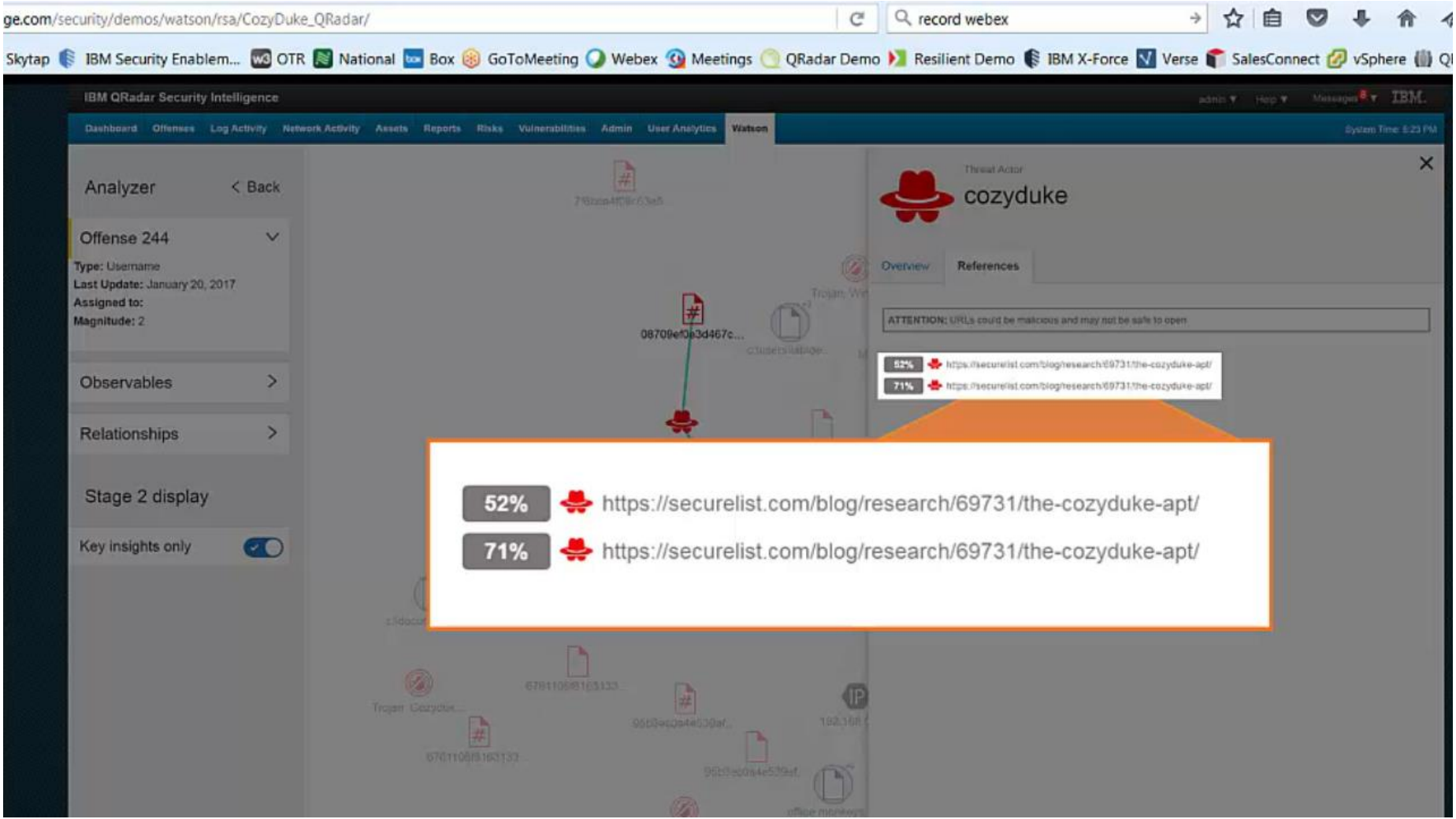
QRadar: Watson Advisor – Patient 0



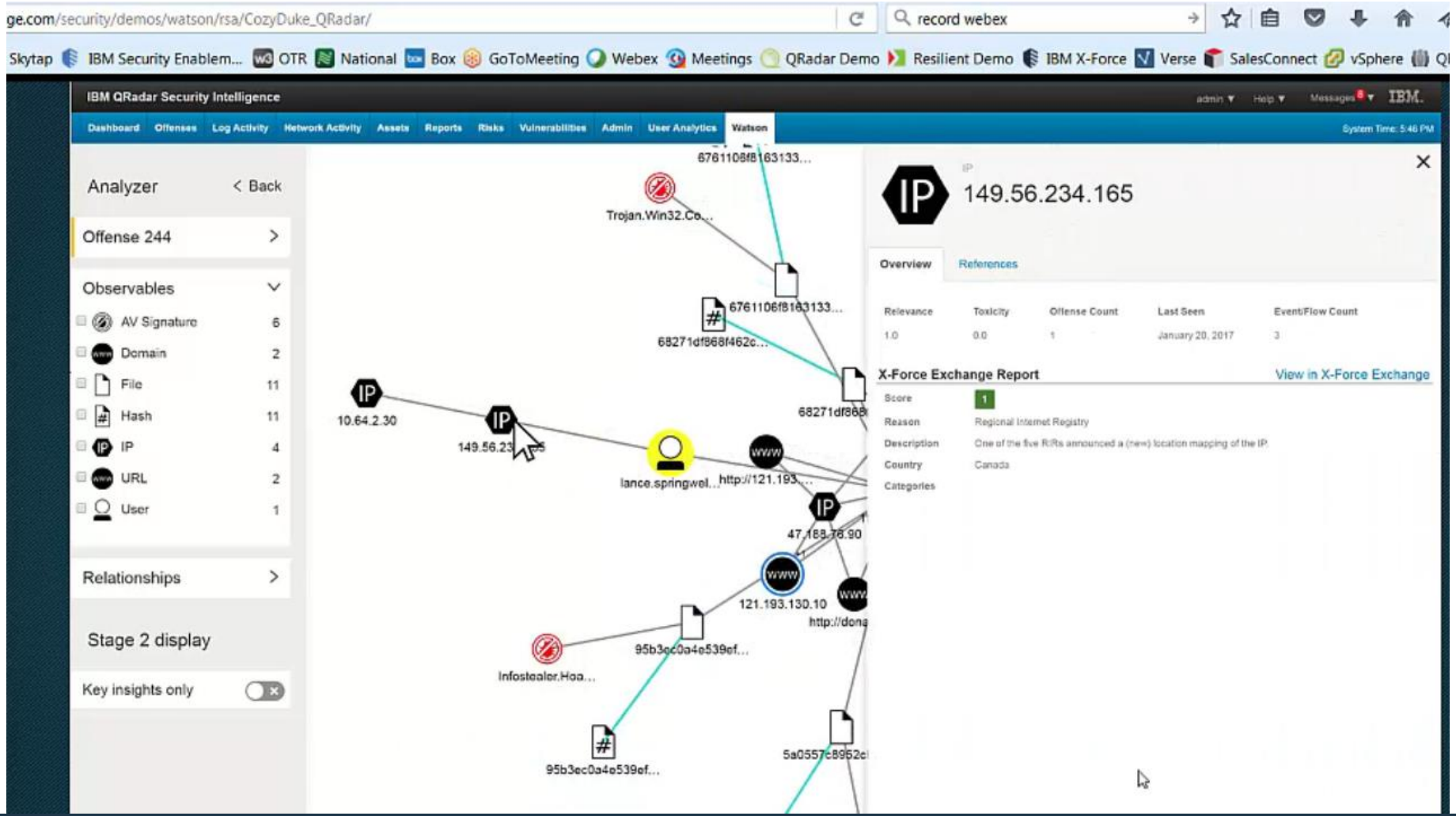
QRadar: Watson Advisor – Threat References



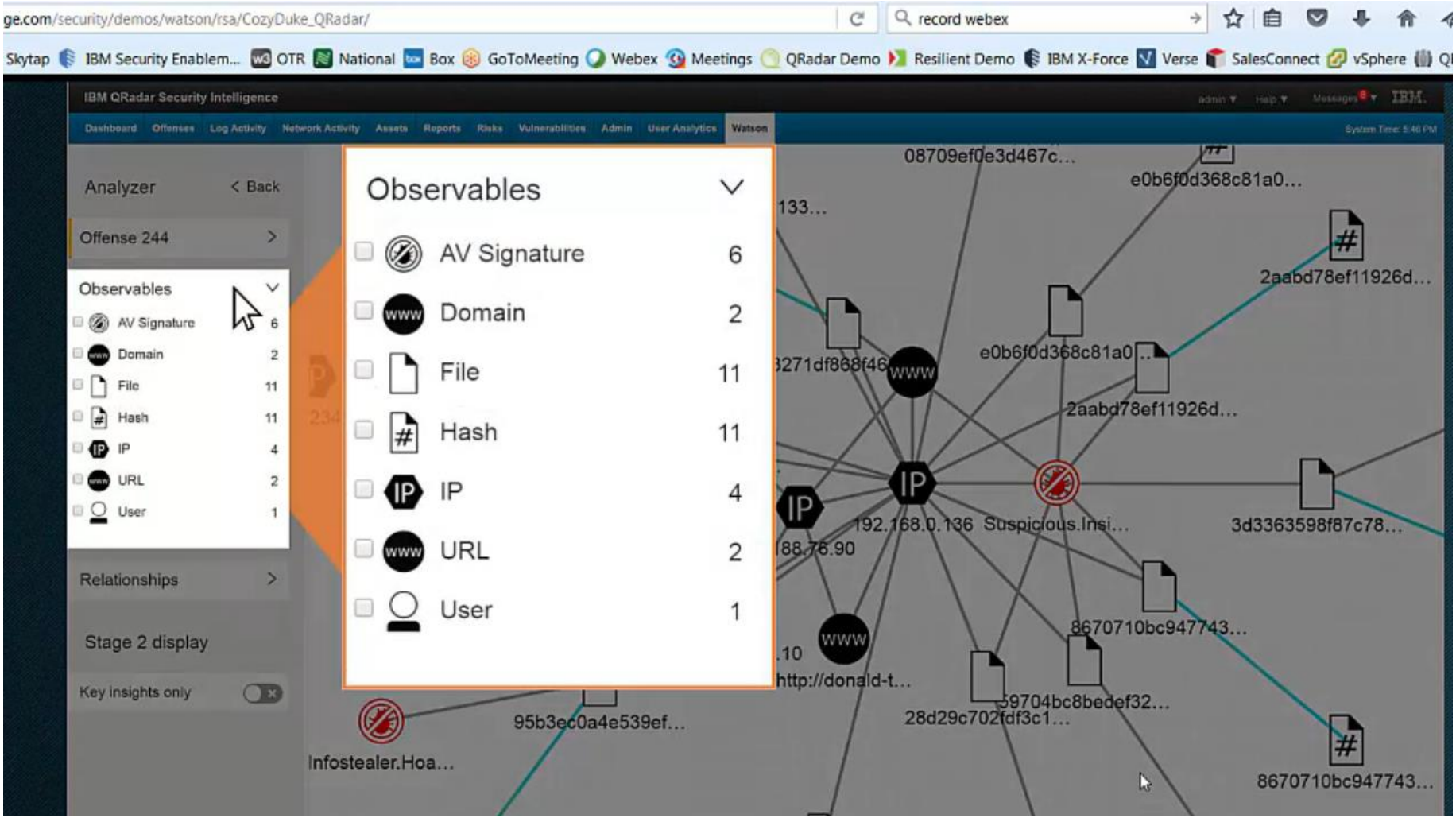
QRadar: Watson Advisor – Threat Information



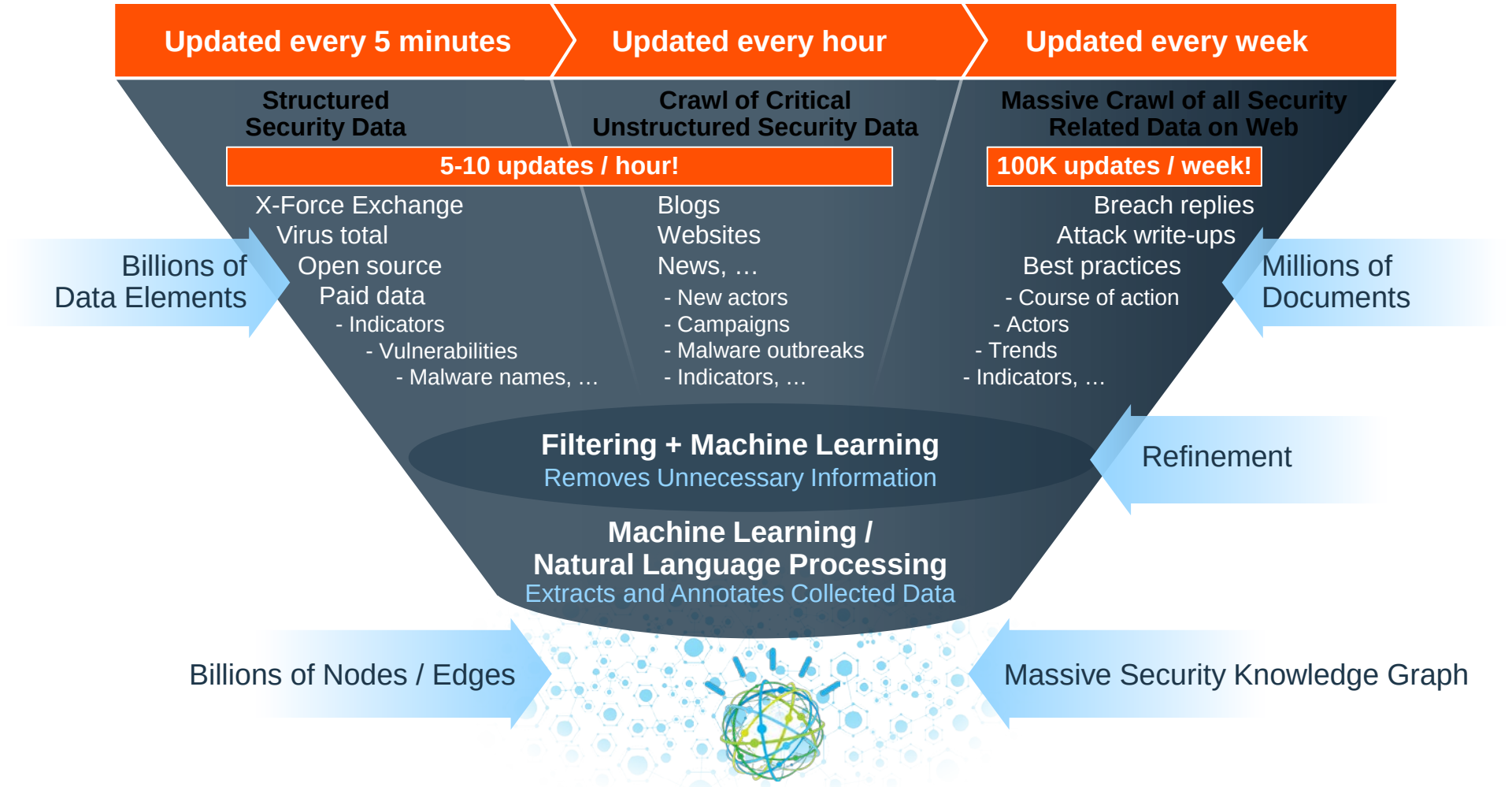
QRadar: Watson Advisor – X-Force Exchange



QRadar: Watson Advisor – Quick Fliters



Building the Foundation of Cognitive Security



Find, fix, and secure endpoints

Prevent advanced network attacks

Use analytics to discover and eliminate threats

Hunt for and investigate threats

Coordinate response activity

Understand the latest threat actors

Get help from security experts

Build deep understanding of threats targeting your business through cyber analysis

IBM i2 Enterprise Insight Analysis

IT and Non-traditional Information Feeds

- PCAP
- Alerts
- System logs
- SIEM
- SSO / AD
- Vulnerability scans
- HR data
- Reviews
- Behavioral data
- Badge logs
- Access logs
- Account creation

External Information Feeds

- Hacker forums
- Intel vendors
- Threat indicators
- Social media
- Government alerts
- Community info

Personal Data
Security / Threat Intelligence

CYBER ANALYSIS

Focused Monitoring and Threat Mitigation

- Integrated data feeds
- Enterprise awareness
- Compliance monitoring
- Threat discovery
- Risk management
- Enable decisions

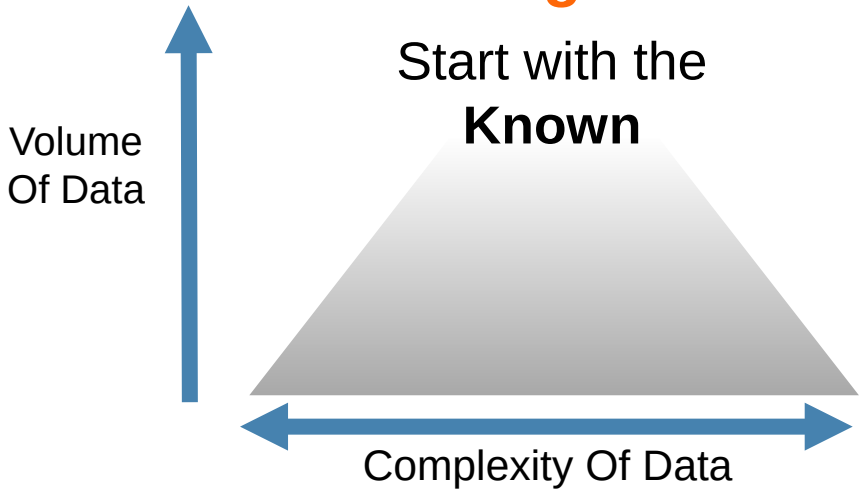
Key Differentiators of i2 vs. Other IBM Security Products

For Advanced Users
Tier 3, Threat Hunters

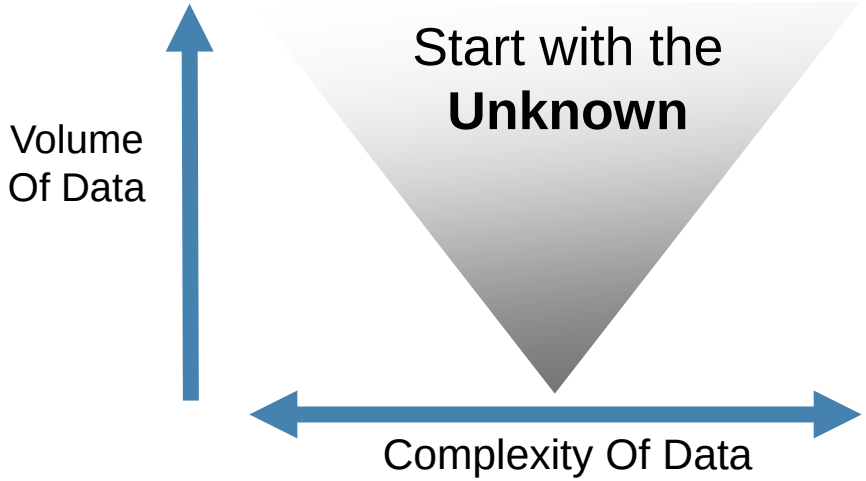
We Do Investigations
Human in the Loop

Non-Cyber Datasets
Physical, HR, Dark Web

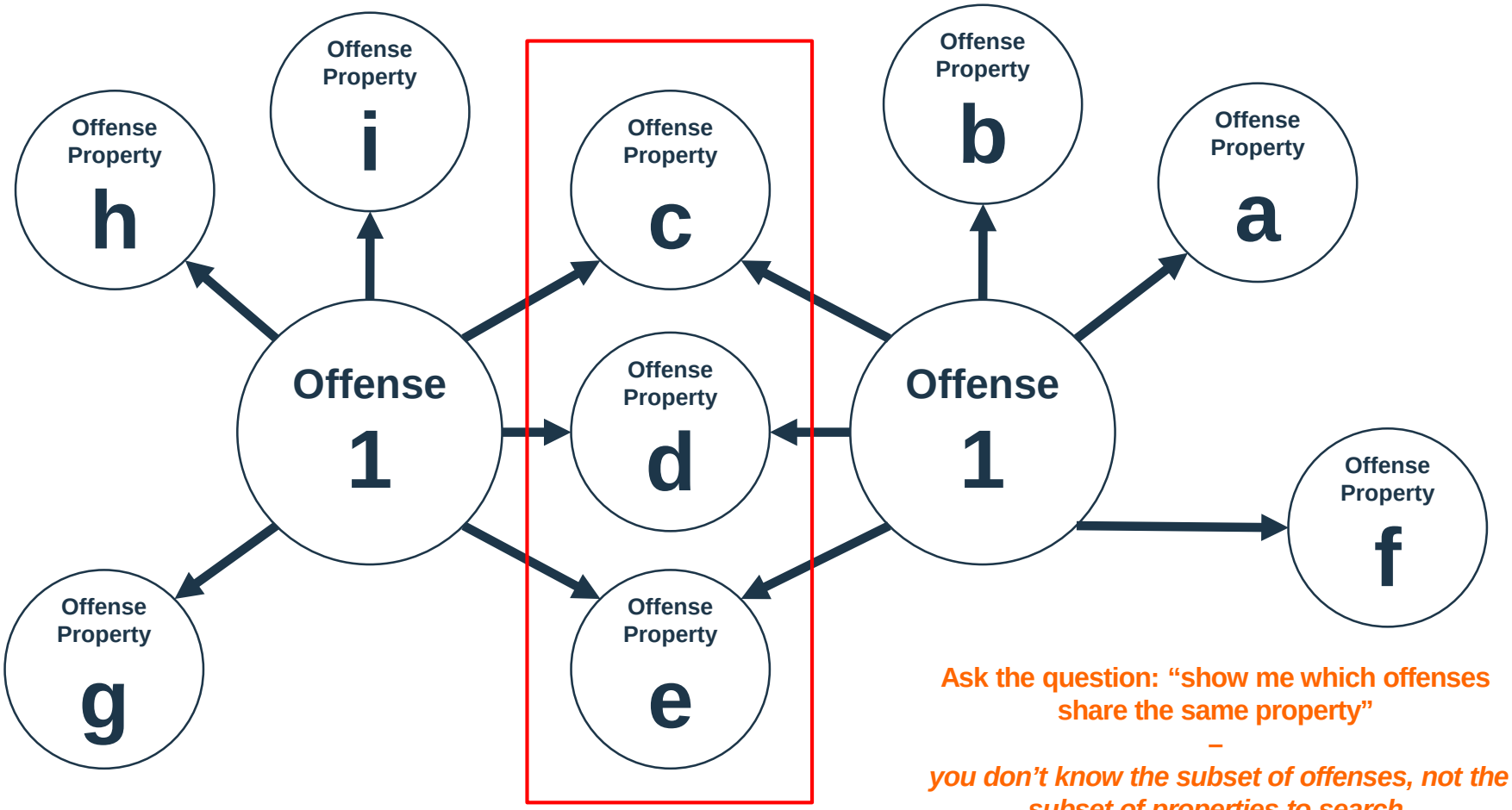
Investigations



Hunting



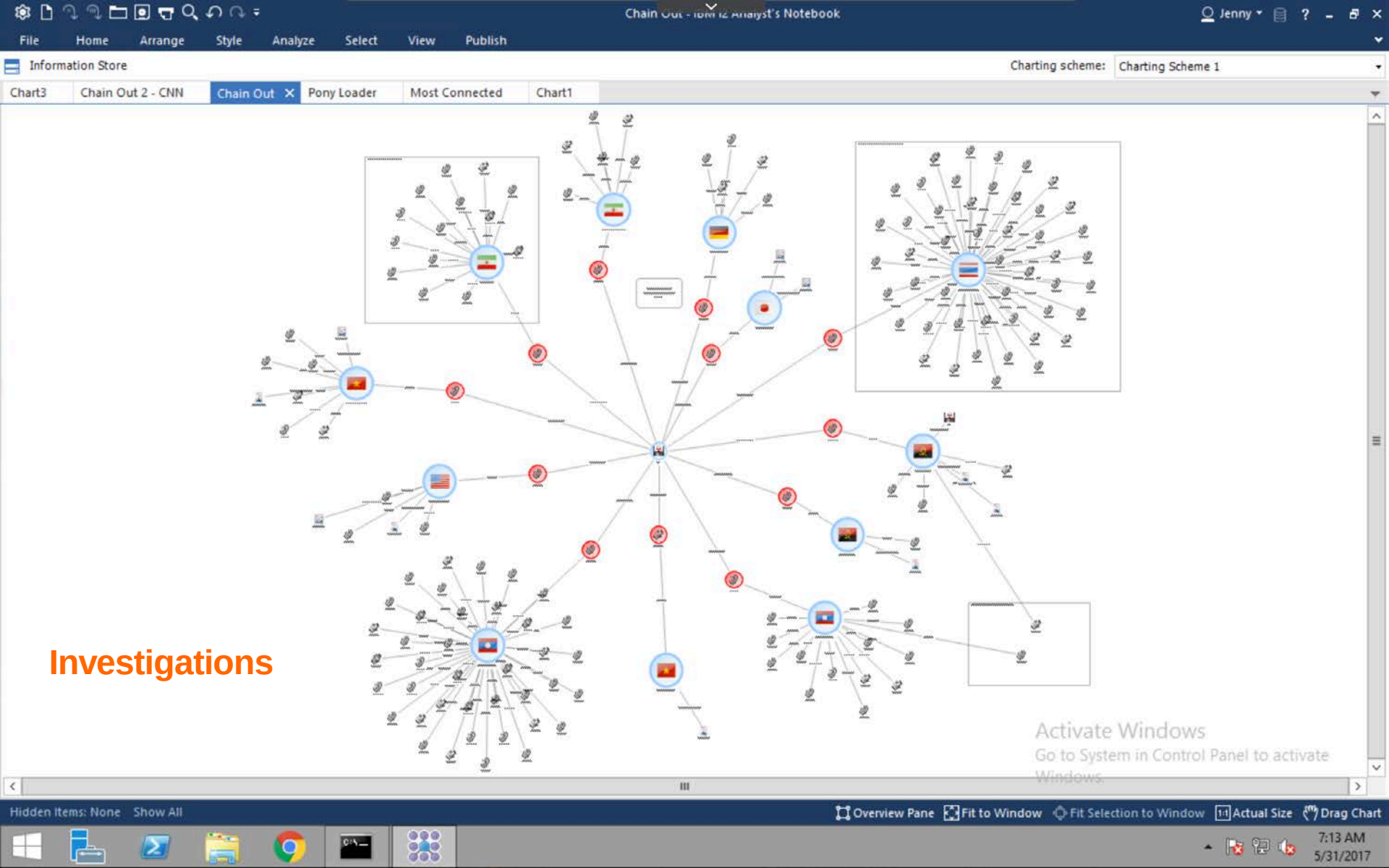
What is an Unknown Unknown Search



Ask the question: "show me which offenses share the same property"

–

you don't know the subset of offenses, not the subset of properties to search


Chain Out - IBM i2 Analyst's Notebook
Jenny
File
Home
Arrange
Style
Analyze
Select
View
Publish
Information Store
Charting scheme:
Charting Scheme 1
Chart3
Chain Out 2 - CNN
Chain Out
Pony Loader
Most Connected
Chart1
Investigations
Activate Windows
Go to System in Control Panel to activate Windows.
Hidden Items: None
Show All
Overview Pane
Fit to Window
Fit Selection to Window
Actual Size
Drag Chart
7:13 AM
5/31/2017

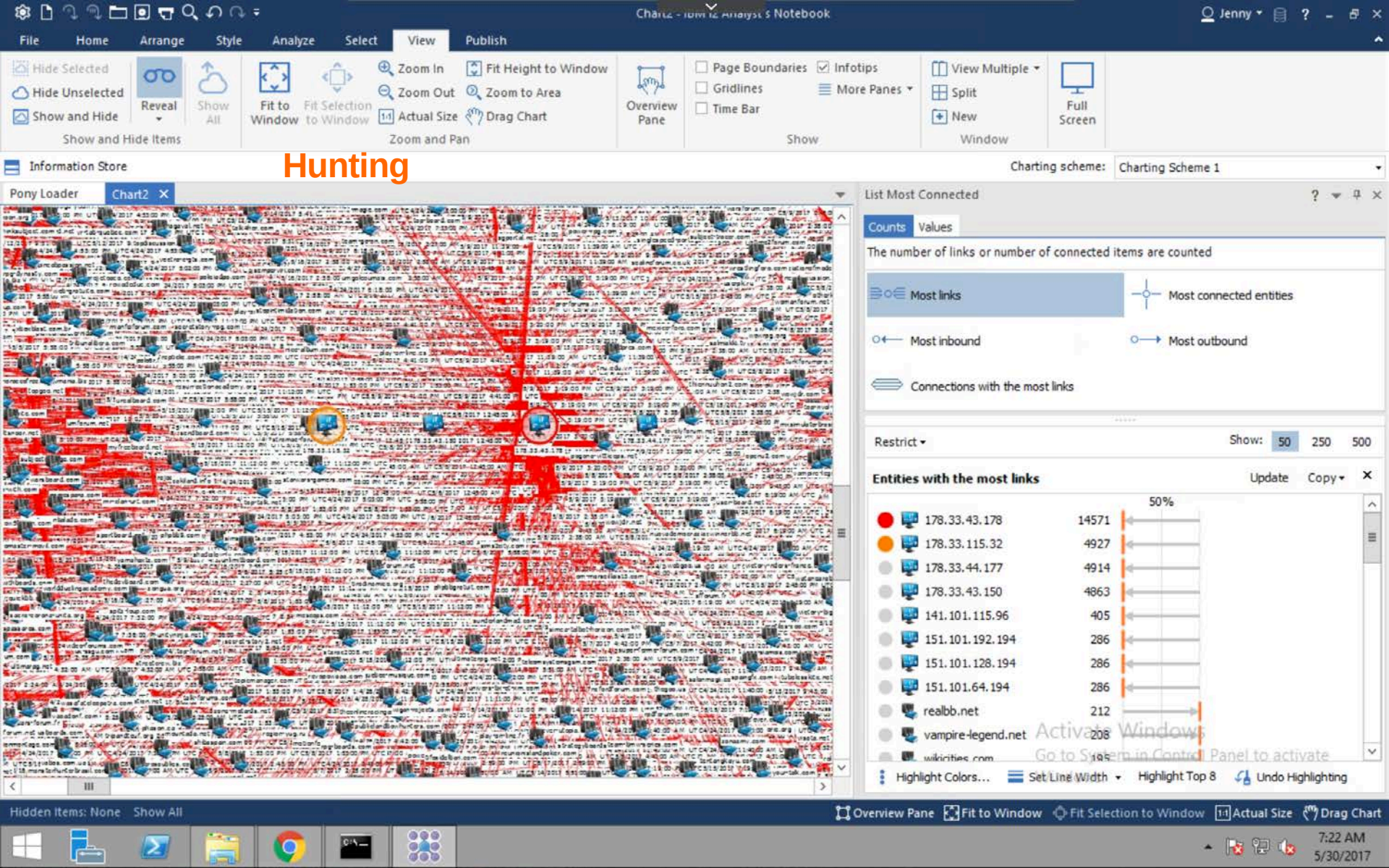
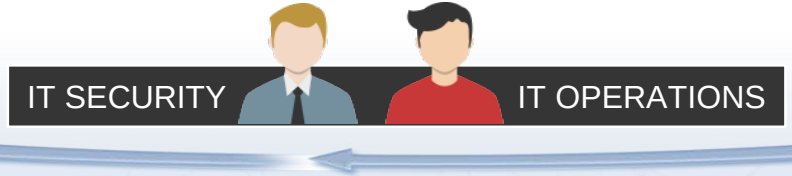


Chart2 - IBM i2 Analyst's Notebook
Jenny
File
Home
Arrange
Style
Analyze
Select
View
Publish
Hide Selected
Hide Unselected
Show and Hide
Reveal
Show All
Show and Hide Items
Fit to Window
Fit Selection to Window
Zoom In
Zoom Out
Actual Size
Fit Height to Window
Zoom to Area
Drag Chart
Zoom and Pan
Overview Pane
Page Boundaries
Gridlines
Time Bar
Infotips
More Panes
Show
View Multiple
Split
New
Window
Full Screen
Hunting
Information Store
Charting scheme:
Charting Scheme 1
Pony Loader
Chart2
List Most Connected
Counts
Values
The number of links or number of connected items are counted
Most links
Most connected entities
Most inbound
Most outbound
Connections with the most links
Restrict
Show:
50
250
500
Entities with the most links
Update
Copy
50%
178.33.43.178 14571
178.33.115.32 4927
178.33.44.177 4914
178.33.43.150 4863
141.101.115.96 405
151.101.192.194 286
151.101.128.194 286
151.101.64.194 286
realbb.net 212
vampire-legend.net 208
Highlight Colors...
Set Line Width
Highlight Top 8
Undo Highlighting
Hidden Items: None
Show All
Overview Pane
Fit to Window
Fit Selection to Window
Actual Size
Drag Chart
7:22 AM
5/30/2017

The Collaborative Endpoint Security and Management Platform

IBM BigFix



IBM BigFix

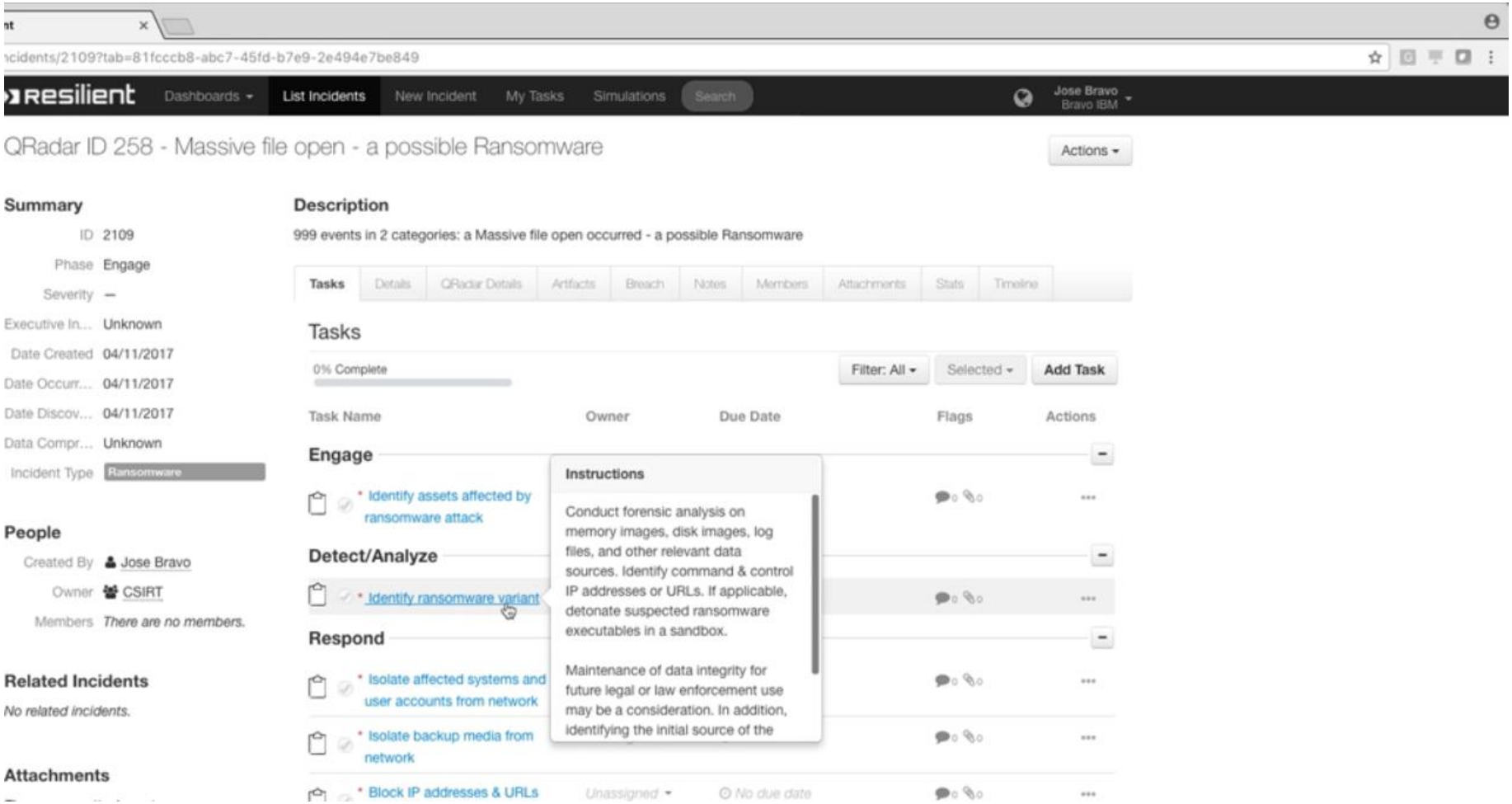
FIND IT. FIX IT. SECURE IT… ***FAST***

Detect	Compliance	Lifecycle	Inventory	Patch
Detect and respond to malicious activity	Continuous policy enforcement and reporting	Software patching, distribution and provisioning	Audit authorized and unauthorized software	Automated patching with high first pass success
• Asset discovery • Detect • Investigate • Response • Query • Patch management • Software distribution	• Query • Patch management • Security configuration management • Vulnerability assessment • Compliance analytics • Third-party anti-virus management • Self quarantine • Add-on: PCI DSS	• Asset discovery • Patch management • Software distribution • Query • Advance patching • Remote control • OS deployment • Power management • Sequenced Task Automation	• Software / hardware inventory • Software usage reporting • Software catalogue correlation • ISO 19770 software tagging	• OS patching • Third-party application patching • Offline patching

Resilient's unique value

- **Resilient integrates with all existing security systems create a single hub for IR transforming organizations' security posture.**
  - Aligns people, process, and technology across the organization
  - Enables security teams to automate and orchestrate their IR processes
  - Ensures IR processes are consistent, intelligent, and configured to teams' specific needs

Resilient Playbooks



Gain integrated, real-time threat intelligence

IBM X-Force Exchange

Find, fix, and secure endpoints

Prevent advanced network attacks

Use analytics to discover and eliminate threats

Coordinate response activity

Understand the latest threat actors

Get help from security experts

Crowd-sourced information sharing
based on 700+TB of threat intelligence

https://exchange.xforce.ibmcloud.com

Gain integrated, real-time threat intelligence

IBM X-Force Exchange – Tailored Dashboards

Find, fix, and secure endpoints

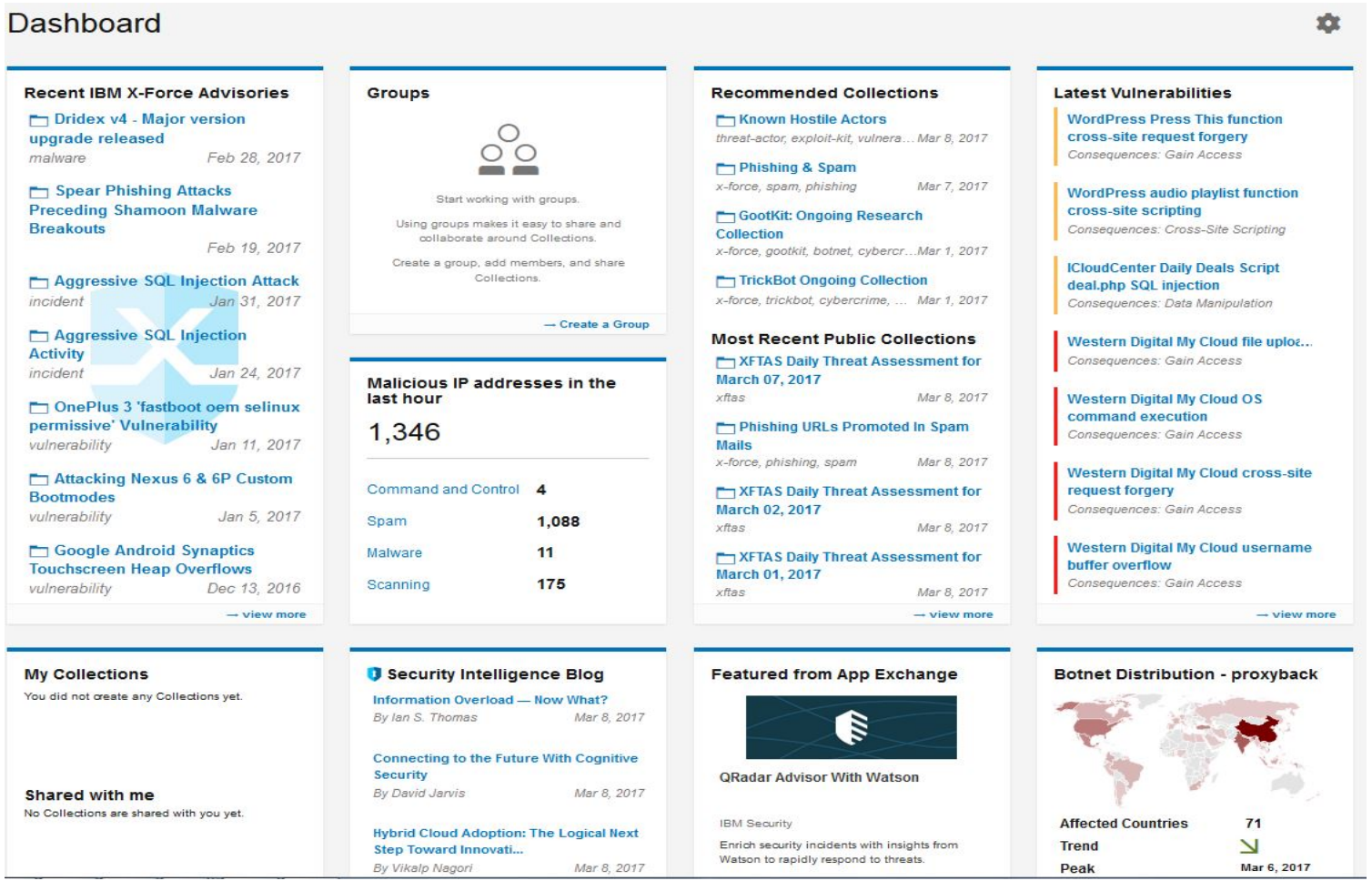
Prevent advanced network attacks

Use analytics to discover and eliminate threats

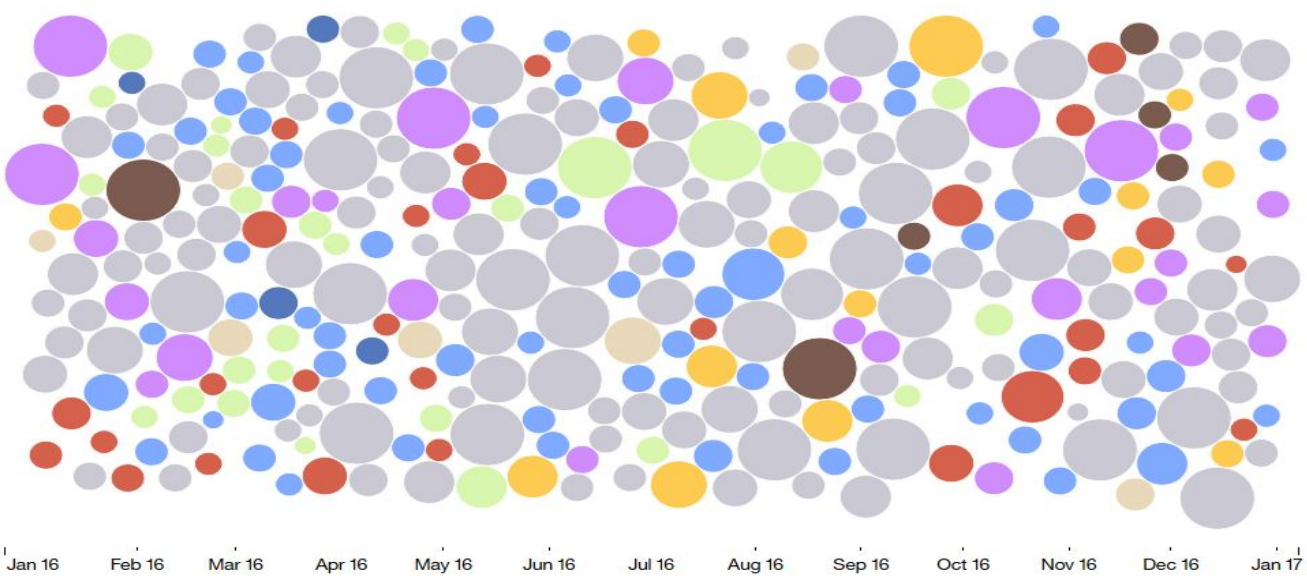
Coordinate response activity

Understand the latest threat actors

Get help from security experts



https:exchange.xforce.ibmcloud.com



Security Incidents ‹ 2016

Displaying **322** incidents
Jan 4, 2016 to **Dec 31, 2016**.

Each circle represents a target of a security incident such as a data leak or denial of service attack.

Click or hover over circles to see more information. Change the year view by clicking the arrows next to the year above.

Data is a sampling of notable incidents for each year and not a full representation of all incidents.

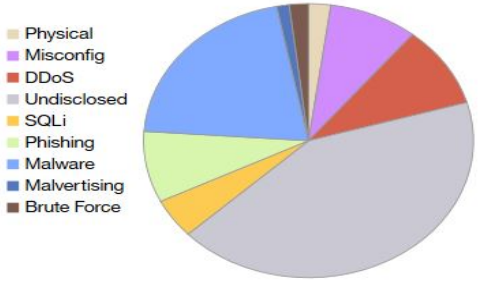
Learn More:

Read the 2016 Cost of a Data Breach Study from Ponemon Institute

Size of circle estimates relative impact of incident in terms of cost to business.

Attack Types (reset)

Click to view incidents for a specific attack type.



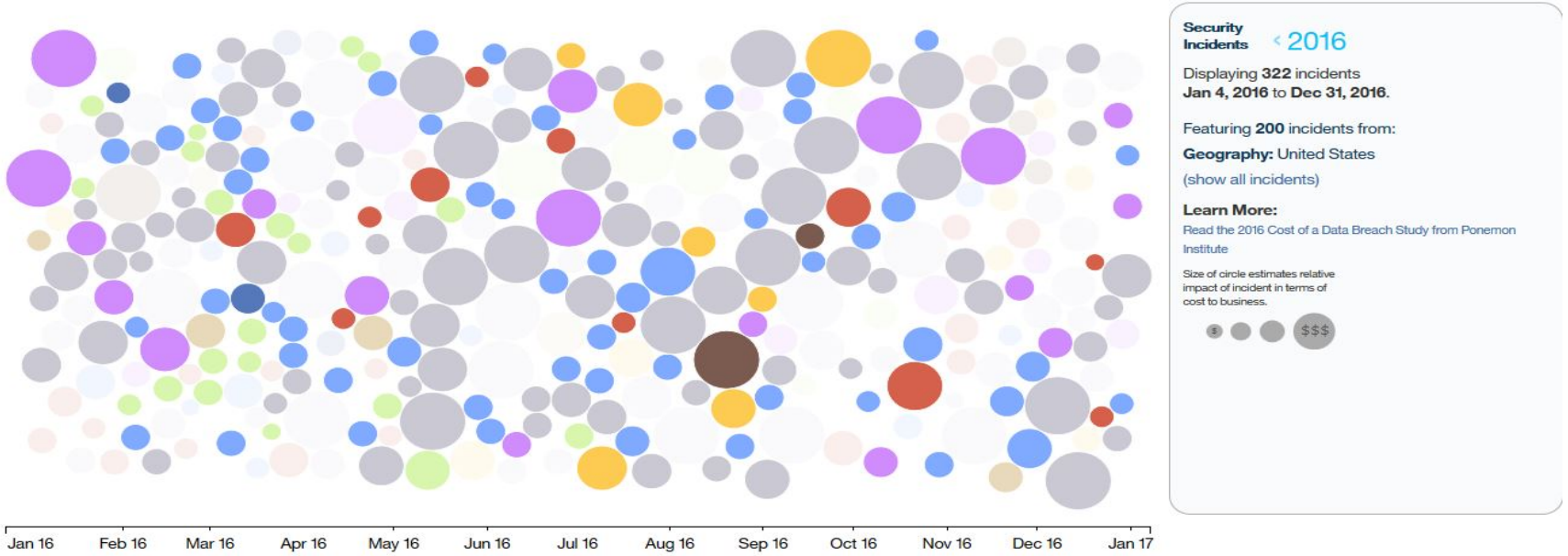
Industries (reset)

Click below to view incidents from a specific industry.

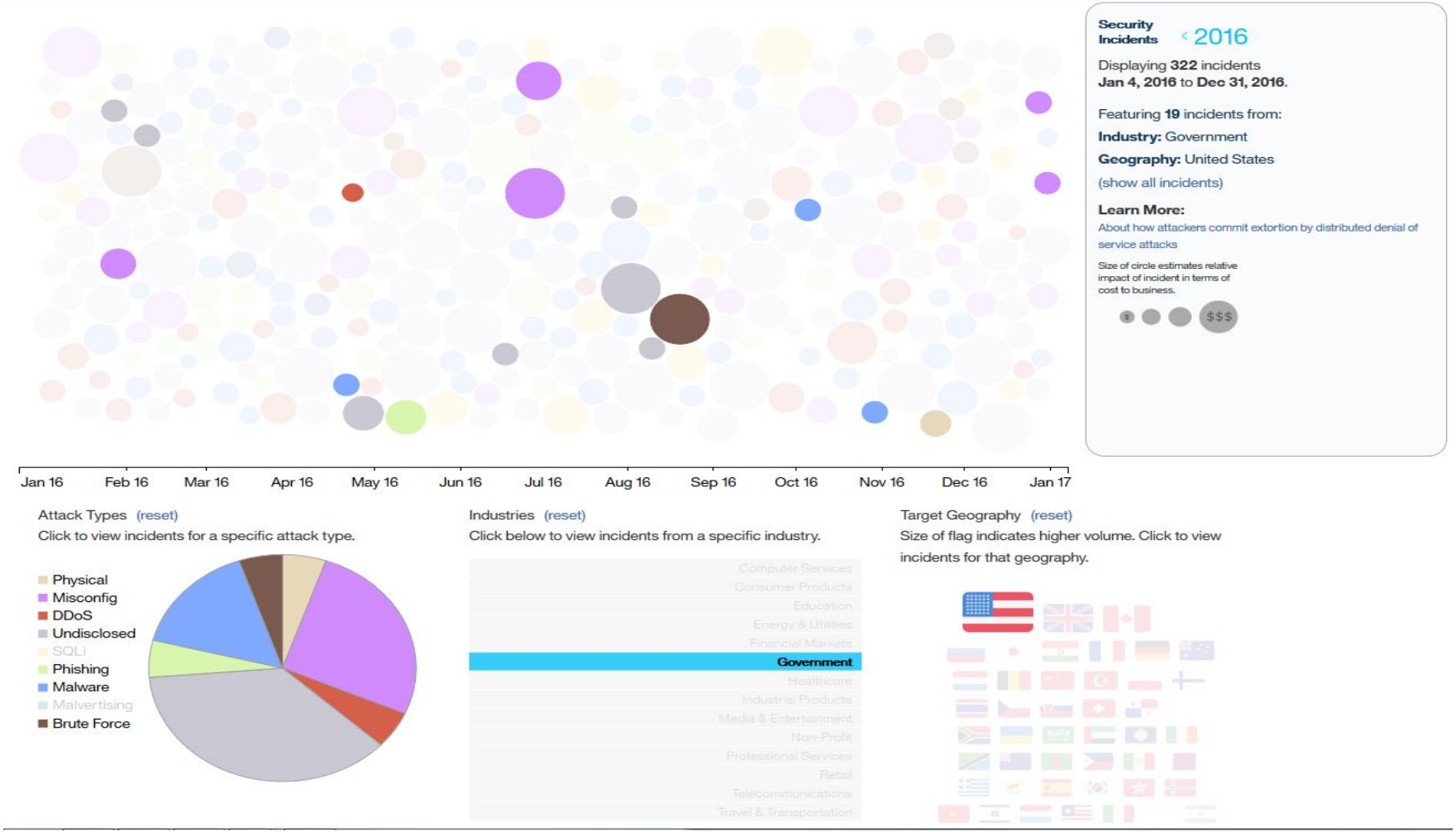
Target Geography (reset)

Size of flag indicates higher volume. Click to view incidents for that geography.

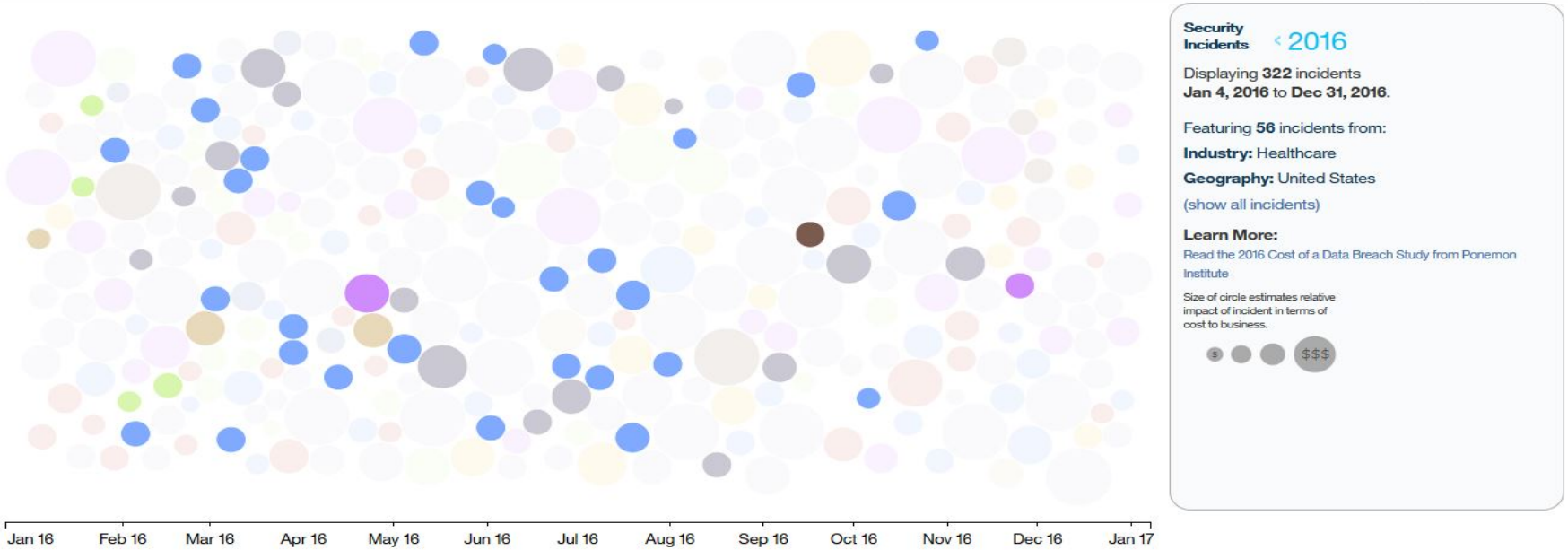
https:exchange.xforce.ibmcloud.com - US



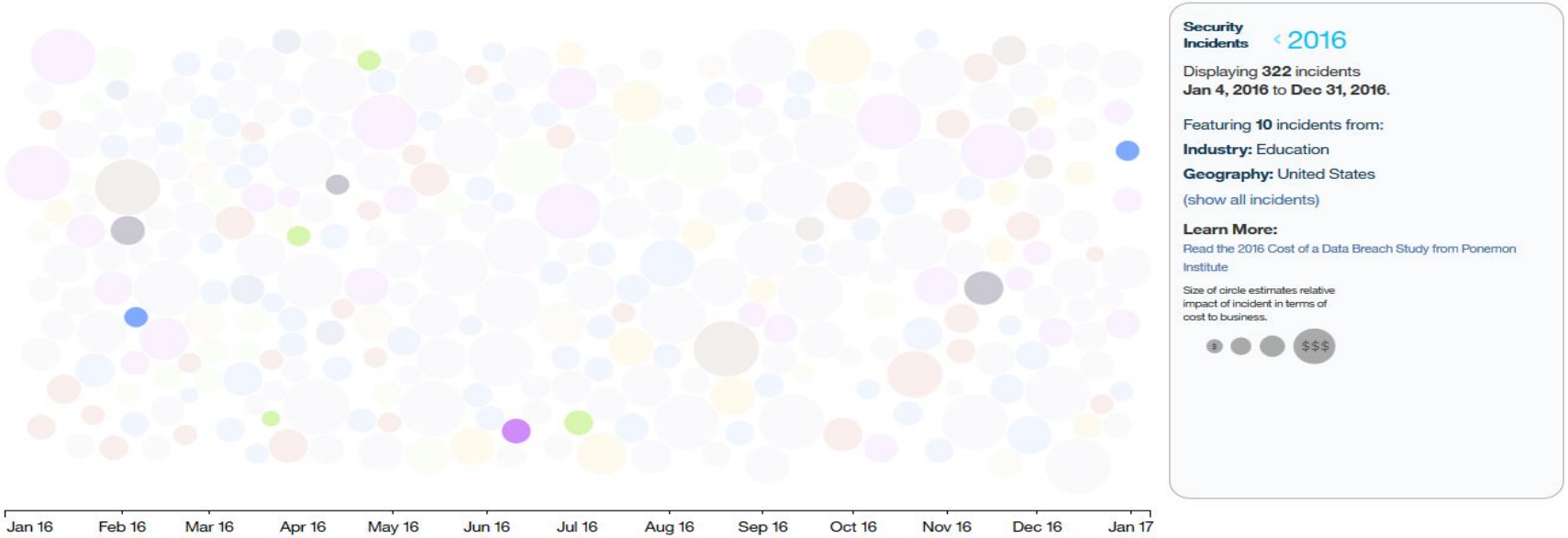
https:exchange.xforce.ibmcloud.com – US Government

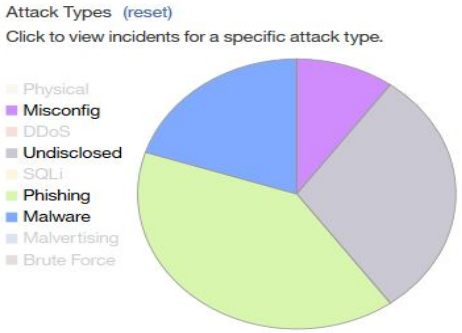


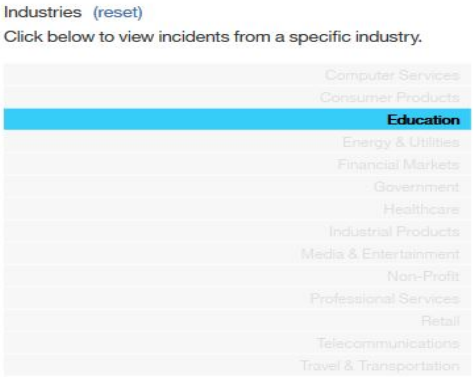
https:exchange.xforce.ibmcloud.com – US Healthcare



https:exchange.xforce.ibmcloud.com – US Education







IBM Security

State of NC QRadar Workshop

Threat Hunting, Advanced Analytics, Augmented Intelligence, and Automated Response

Michael Melore, CISSP
IBM Cyber Security Advisor

Follow us on Twitter **@MichaelMelore**

October 2017

IBM