IBM Security

The New Security Frontier:

Threat Hunting, Augmented Intelligence, and Automated Response

Michael Melore, CISSP
IBM Cyber Security Advisor

Follow us on Twitter **@MichaelMelore**

June 2018

IBM

IBM Security

“We need help analyzing huge amounts of information in real-time to identify trends and useful information for more actionable insights.”

Detect & Stop Advanced Threats

Orchestrate Incident Response

Master Threat Hunting

IBM Security

Josh
L1 Threat Analyst

- Monitor incoming incidents detected by the organization's SIEM
- Initial threat investigation
- Detect and close false positive or erroneous incidents
- Escalate potentially serious security incidents to tier 2 analysts for triage using incident response system

Saima
L2 Triage Analyst

- Triage threats, analyzing incidents passed from tier 1 analysts
- Promote security incidents for response and additional escalation
- Determine threat root cause using advanced analytics skills

James
L3 Analyst

- * Incident Response Automate/orchestrating workflows, notifications and reporting
- * Forensics Further analyze finding from L2 Analyst to better determine causation.
- * Threat Hunting Use threat intelligence, analysis of anomalous log data and results of brainstorming sessions to detect threat actors

IT / Ops

- Blocks inbound attack traffic and disables user IDs used in attack
- Threat hunting: No internal users involved
- Forensics: no data lost through exfiltration

Sue
Sec Ops Manager

- Run smooth security operations
- Reduce false positives, improve productivity
- Plan and supervise the execution of technical security controls to counter identified threats
- Handle high priority situations
- Provide dashboards and metrics that show the security risk posture

Workflow

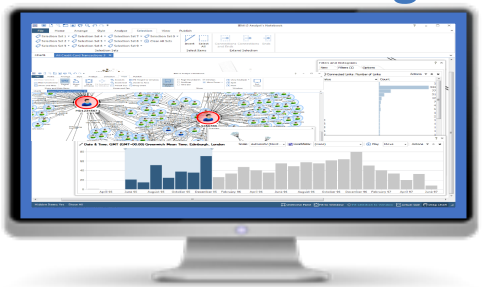
Advanced Analytics

DETECT

Cognitive

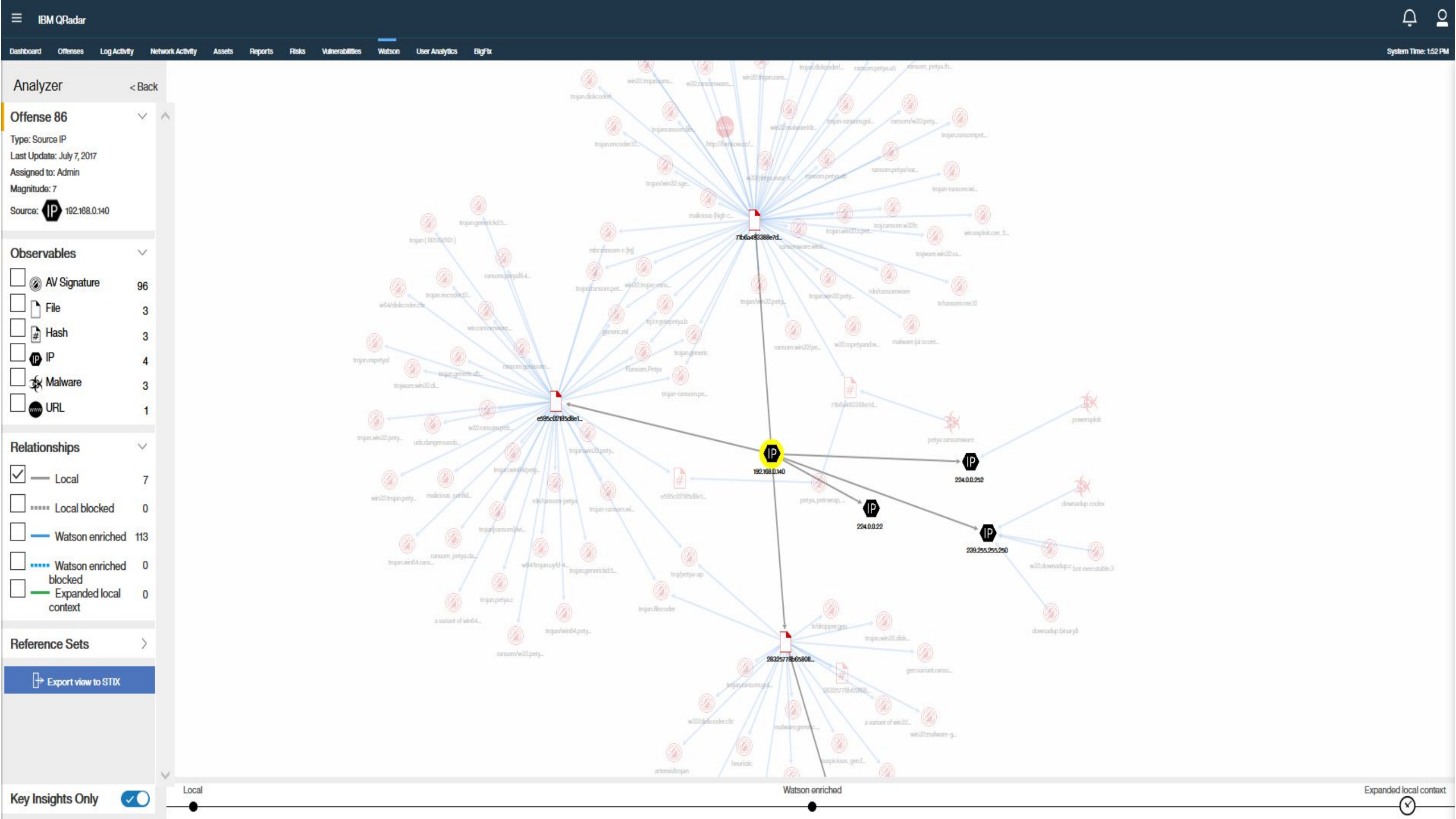
ENRICH

Threat Hunting



INVESTIGATE

ORCHESTRATE


IBM QRadar
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Risks
Vulnerabilities
Watson
User Analytics
BigFix
System Time: 1:52 PM
Analyzer
< Back
Offense 86
Type: Source IP
Last Update: July 7, 2017
Assigned to: Admin
Magnitude: 7
Source: 192.168.0.140
Observables
AV Signature 96
File 3
Hash 3
IP 4
Malware 3
URL 1
Relationships
Local 7
Local blocked 0
Watson enriched 113
Watson enriched blocked 0
Expanded local context 0
Reference Sets
Export view to STIX
Key Insights Only
192.168.0.140
224.0.0.252
224.0.0.22
239.255.255.250
Local
Watson enriched
Expanded local context

Analyzer

< Back

Offense 86

Type: Source IP
Last Update: July 7, 2017
Assigned to: Admin
Magnitude: 7
Source: IP 192.168.0.140

Observables

AV Signature	96
File	3
Hash	3
IP	4
Malware	3
URL	1

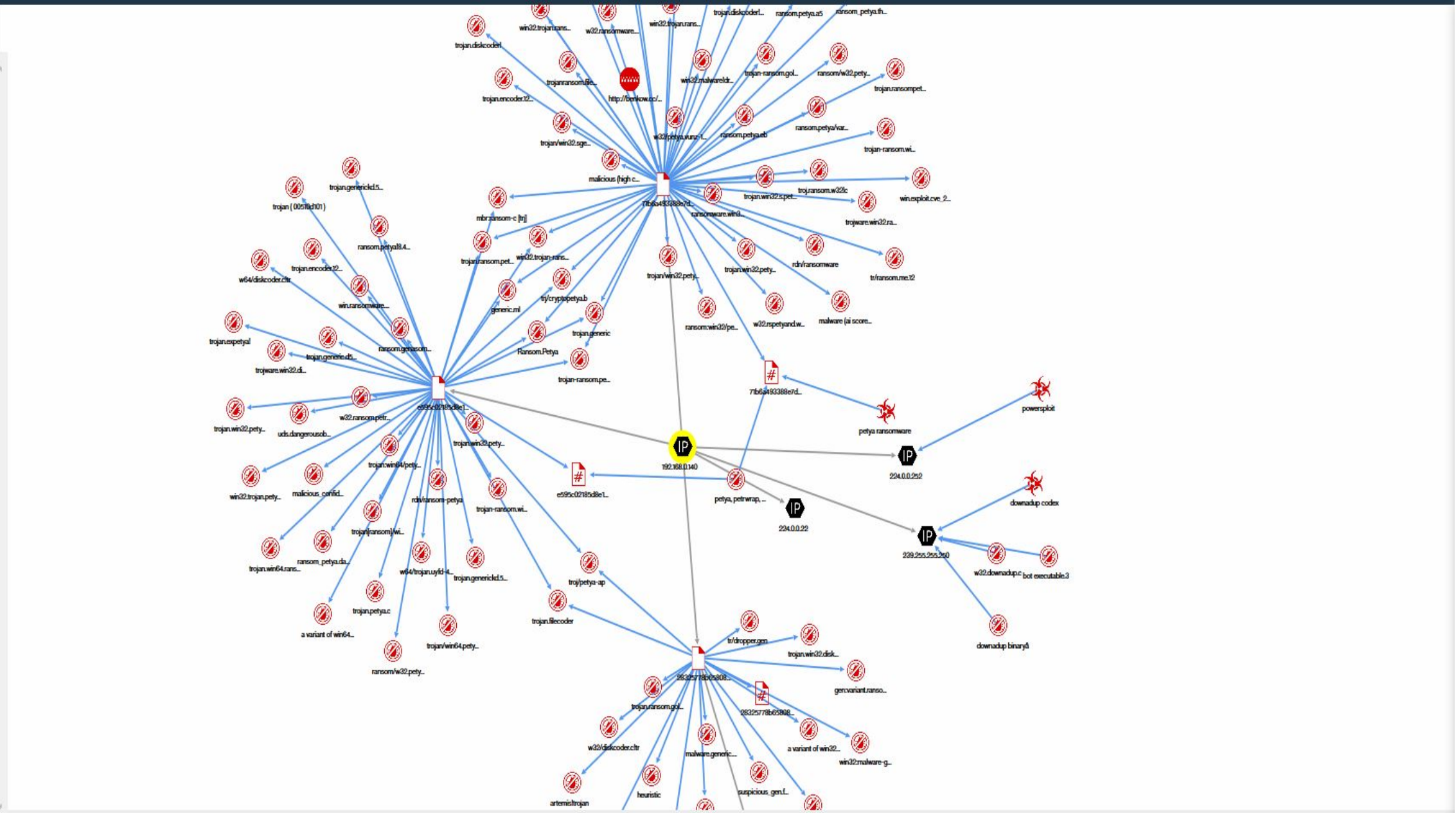
Relationships

Local	7
Local blocked	0
Watson enriched	113
Watson enriched blocked	0
Expanded local context	0

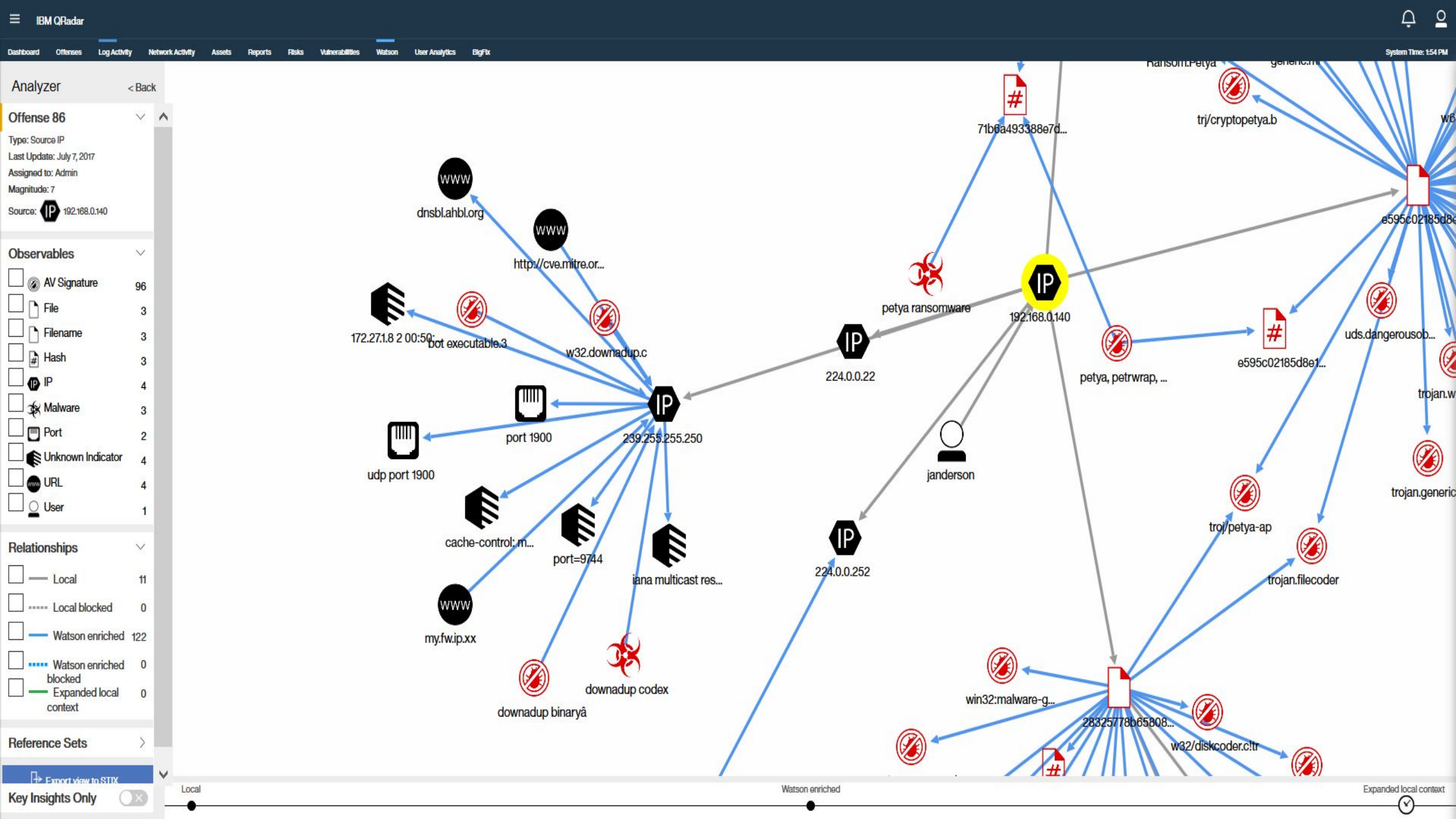
Reference Sets

Export view to STIX

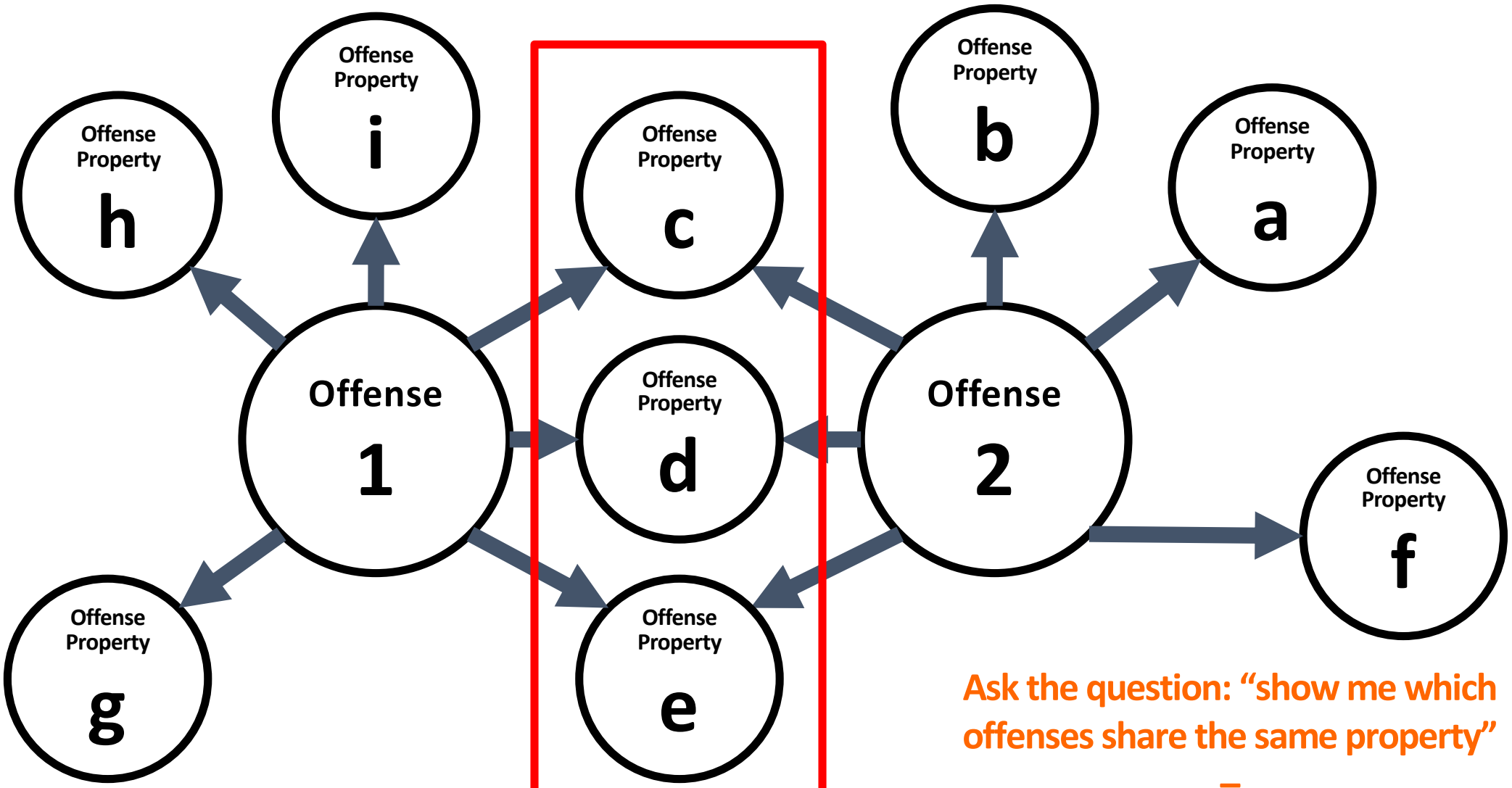
Key Insights Only



Local — Watson enriched — Expanded local context


IBM QRadar
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Risks
Vulnerabilities
Watson
User Analytics
BigFix
System Time: 1:54 PM
Analyzer
< Back
Offense 86
Type: Source IP
Last Update: July 7, 2017
Assigned to: Admin
Magnitude: 7
Source: 192.168.0.140
Observables
AV Signature 96
File 3
Filename 3
Hash 3
IP 4
Malware 3
Port 2
Unknown Indicator 4
URL 4
User 1
Relationships
Local 11
Local blocked 0
Watson enriched 122
Watson enriched blocked 0
Expanded local context 0
Reference Sets
Export view to STIX
Key Insights Only
dnsbl.ahbl.org
http://cve.mitre.or...
172.27.1.8 2 00:50:
bot executable.3
w32.downadup.c
port 1900
udp port 1900
239.255.255.250
cache-control: m...
port=9744
iana multicast res...
my.fw.ip.xx
downadup binaryâ
downadup codex
71b6a493388e7d...
petya ransomware
192.168.0.140
224.0.0.22
janderson
224.0.0.252
petya, petrwrap, ...
e595c02185d8e1...
trj/cryptopetya.b
uds.dangerousob...
trojan.generic
troj/petya-ap
trojan.filecoder
win32:malware-g...
28325778b65808...
w32/diskcoder.c!tr
Local
Watson enriched
Expanded local context

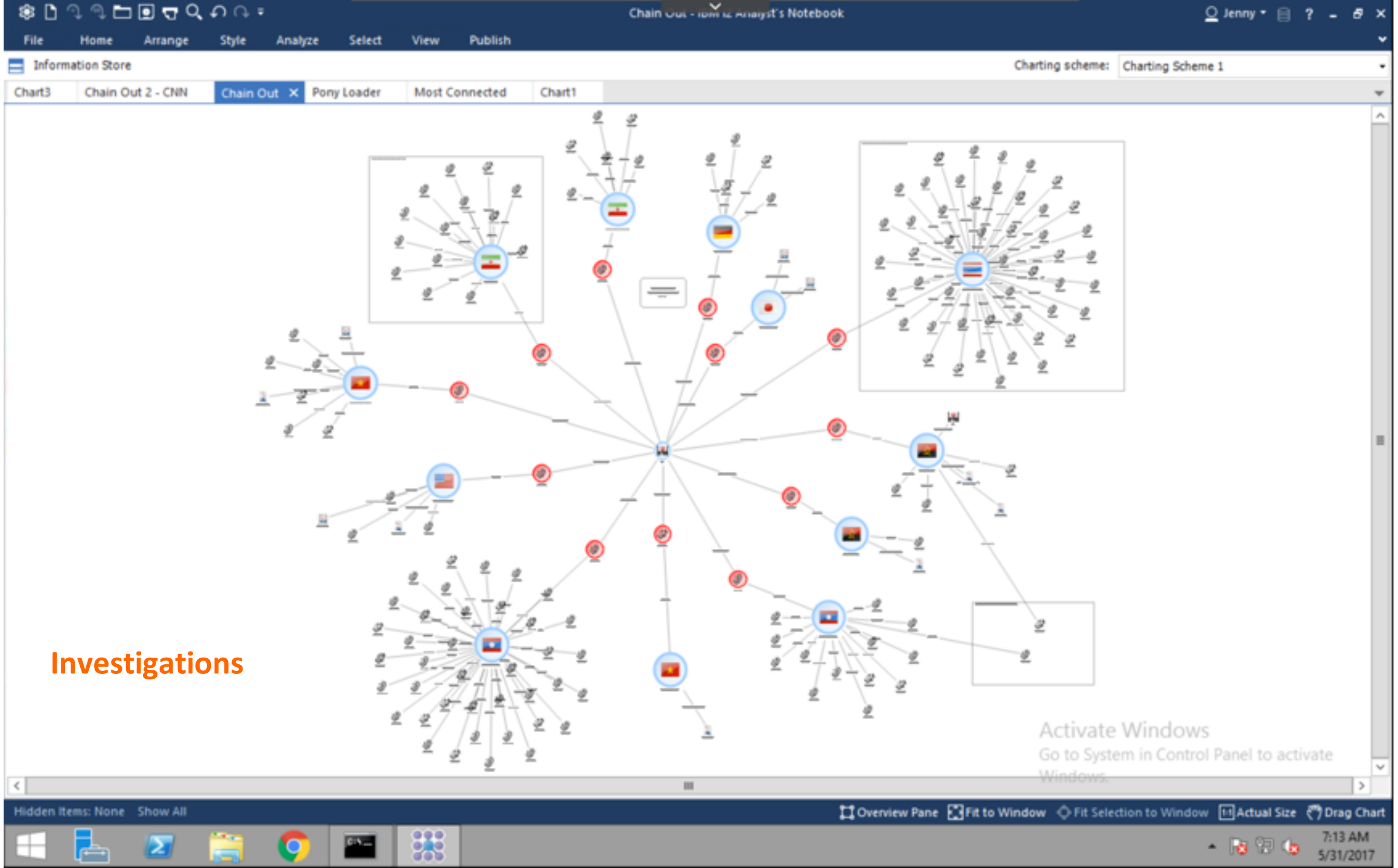
What is an Unknown Unknown Search

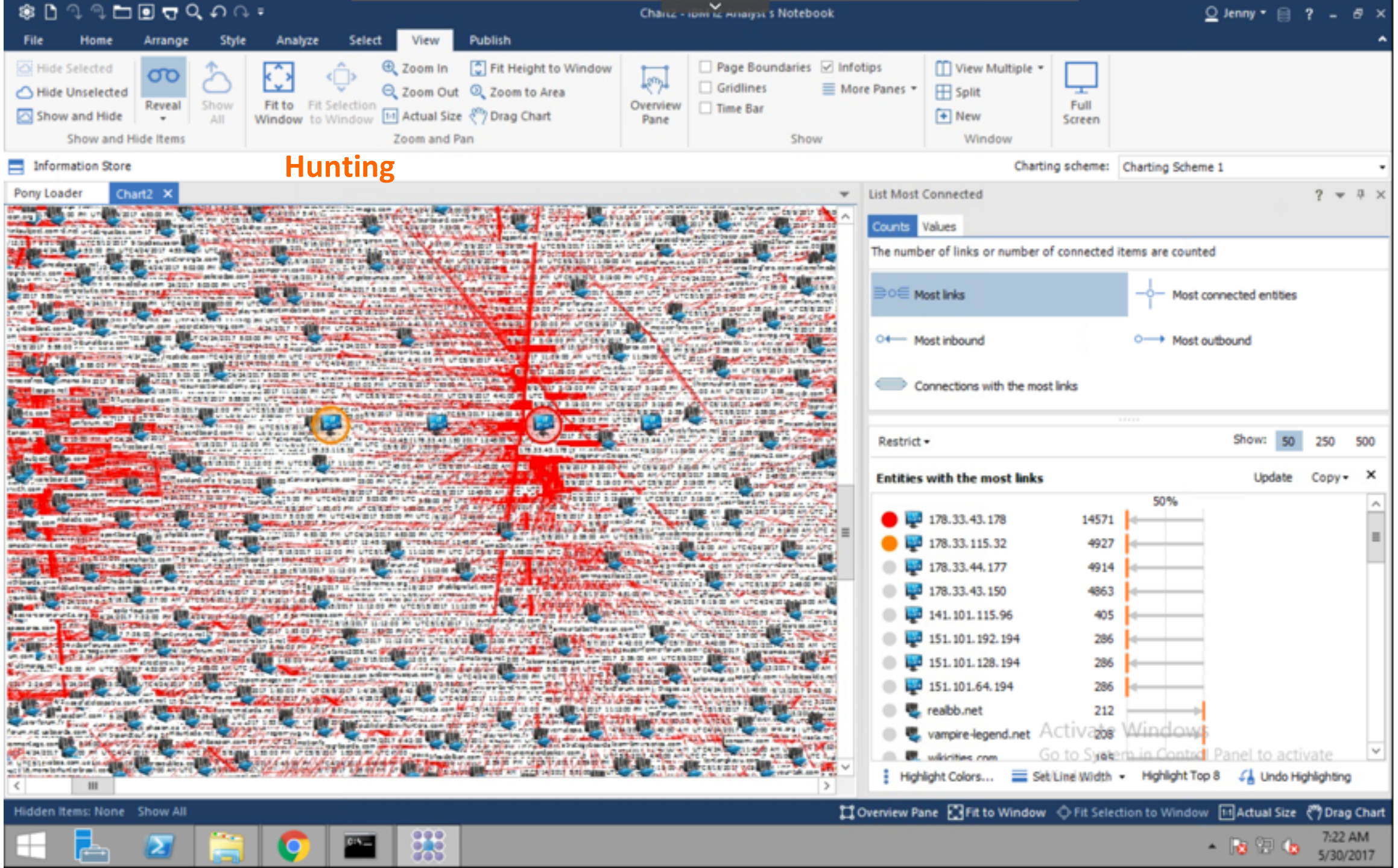


Ask the question: "show me which offenses share the same property"

–

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


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
Information Store
Hunting
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

Incident Response

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 lates 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

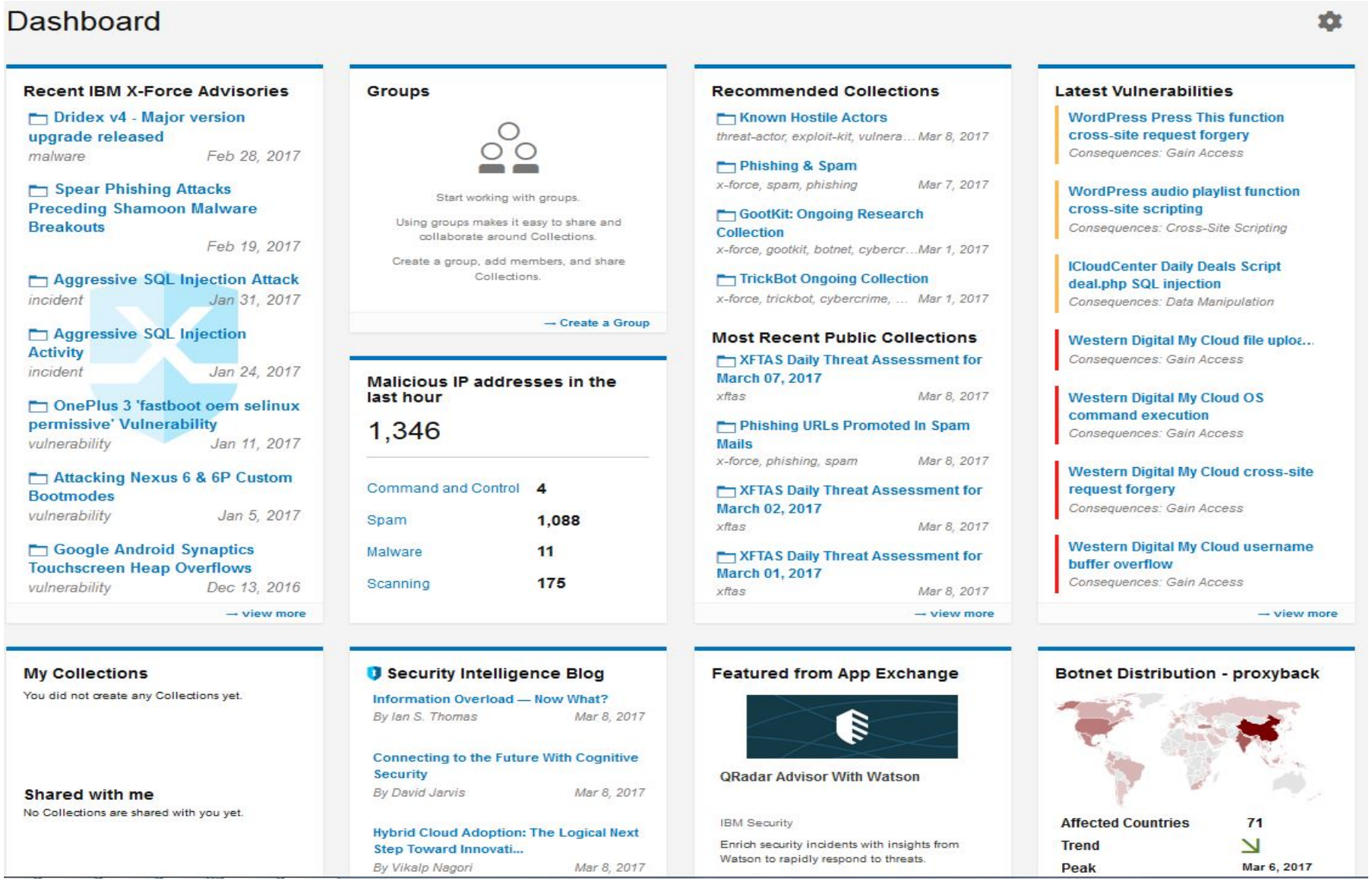
Prevent advanced network attacks

Use analytics to discover and eliminate threats

Coordinate response activity

Understand the latest threat actors

Get help from security experts



IBM Security

An integrated and intelligent security immune system

IBM

IBM Security

The New Security Frontier:

Threat Hunting, Augmented Intelligence, and Automated Response

Michael Melore, CISSP
IBM Cyber Security Advisor

Follow us on Twitter **@MichaelMelore**

June 2018

IBM