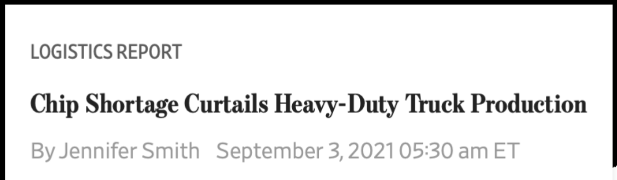
The Evolution of AI in Security

Michael Melore, CISSP
IBM Senior Cybersecurity Advisor
Chair SECRT (Security <Leaders> Round Table)
FBI InfraGard Committeemen
NASCIO Privacy and Cyber Security Committees
CISA / ATARC CDRT (Critical Defense Round Table) Steering Committee

FOLLOW US ON twitter

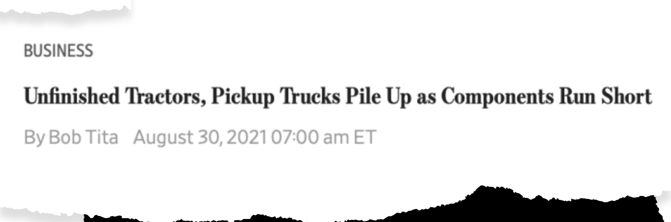
@MichaelMelore

Demand uncertainty and supply chain disruptions are making unprecedented headlines


LOGISTICS REPORT

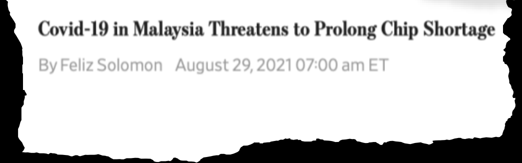
Chip Shortage Curtails Heavy-Duty Truck Production

By Jennifer Smith September 3, 2021 05:30 am ET

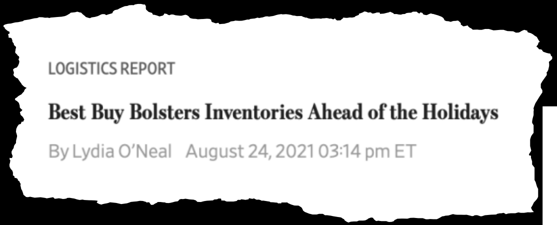

BUSINESS

Unfinished Tractors, Pickup Trucks Pile Up as Components Run Short

By Bob Tita August 30, 2021 07:00 am ET

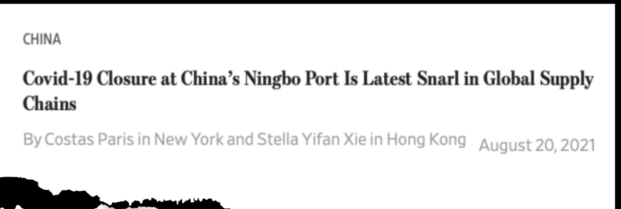

Covid-19 in Malaysia Threatens to Prolong Chip Shortage

By Feliz Solomon August 29, 2021 07:00 am ET


LOGISTICS REPORT

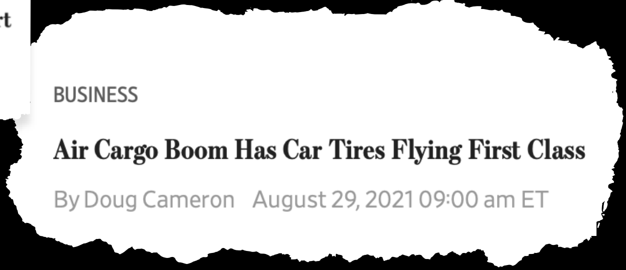
Best Buy Bolsters Inventories Ahead of the Holidays

By Lydia O'Neal August 24, 2021 03:14 pm ET


CHINA

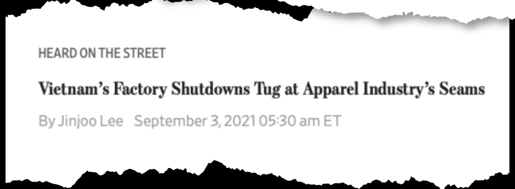
Covid-19 Closure at China's Ningbo Port Is Latest Snarl in Global Supply Chains

By Costas Paris in New York and Stella Yifan Xie in Hong Kong August 20, 2021


BUSINESS

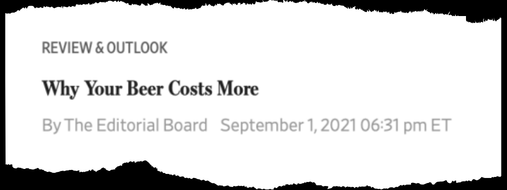
Air Cargo Boom Has Car Tires Flying First Class

By Doug Cameron August 29, 2021 09:00 am ET


HEARD ON THE STREET

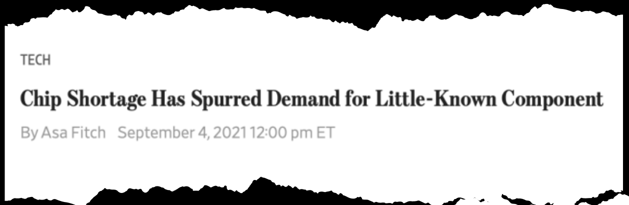
Vietnam's Factory Shutdowns Tug at Apparel Industry's Seams

By Jinjoo Lee September 3, 2021 05:30 am ET


REVIEW & OUTLOOK

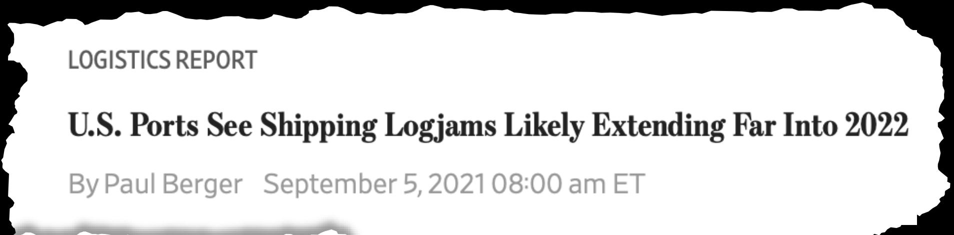
Why Your Beer Costs More

By The Editorial Board September 1, 2021 06:31 pm ET


TECH

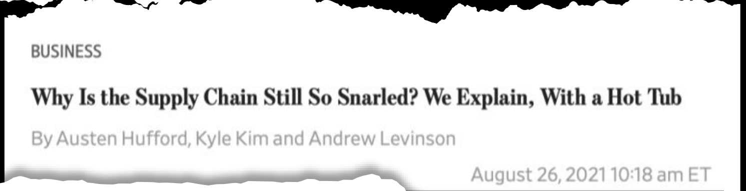
Chip Shortage Has Spurred Demand for Little-Known Component

By Asa Fitch September 4, 2021 12:00 pm ET


LOGISTICS REPORT

U.S. Ports See Shipping Logjams Likely Extending Far Into 2022

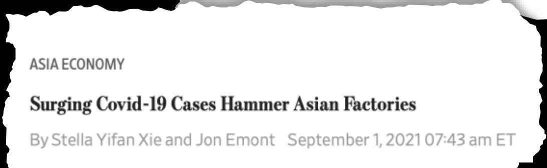
By Paul Berger September 5, 2021 08:00 am ET


BUSINESS

Why Is the Supply Chain Still So Snarled? We Explain, With a Hot Tub

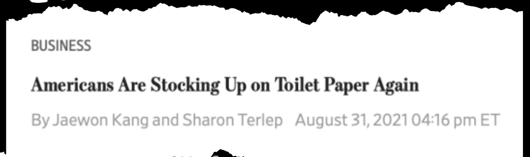
By Austen Hufford, Kyle Kim and Andrew Levinson

August 26, 2021 10:18 am ET


ASIA ECONOMY

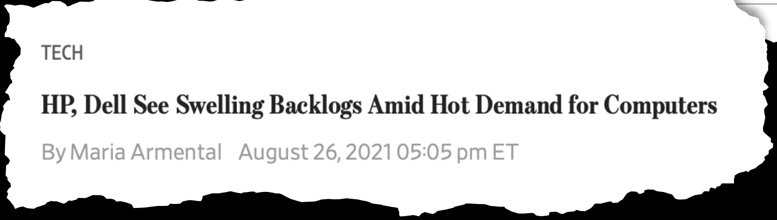
Surging Covid-19 Cases Hammer Asian Factories

By Stella Yifan Xie and Jon Emont September 1, 2021 07:43 am ET


BUSINESS

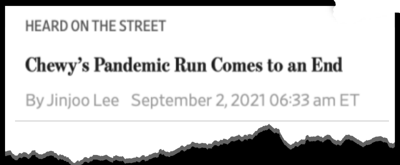
Americans Are Stocking Up on Toilet Paper Again

By Jaewon Kang and Sharon Terlep August 31, 2021 04:16 pm ET


TECH

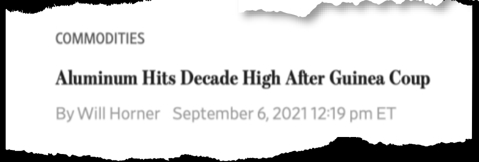
HP, Dell See Swelling Backlogs Amid Hot Demand for Computers

By Maria Armental August 26, 2021 05:05 pm ET


HEARD ON THE STREET

Chewy's Pandemic Run Comes to an End

By Jinjoo Lee September 2, 2021 06:33 am ET


COMMODITIES

Aluminum Hits Decade High After Guinea Coup

By Will Horner September 6, 2021 12:19 pm ET

**Supply Chain Headlines from WSJ in the last 3 months*

Supply chain leaders are looking for actionable visibility and control based on real-time analytics for digital transformation

85%

of companies felt that supply chain complexity is a significant and growing challenge for their operations

97%

of companies recognize the importance of and are prioritizing efforts to improve end-to end supply chain visibility

50%

of manufacturers will use supply chain orchestration tools for innovation delivery and disruption avoidance by 2024

70%

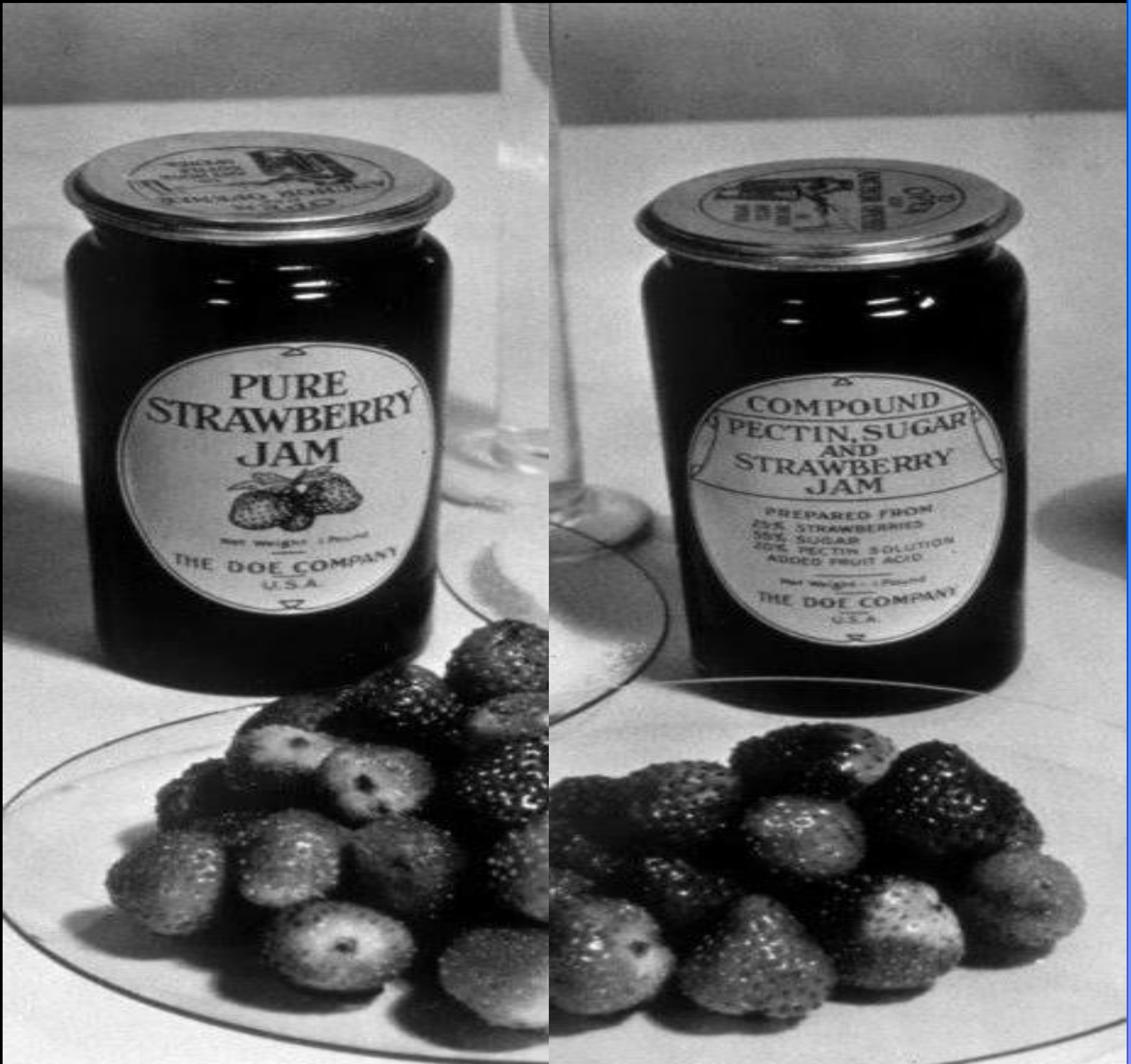
of Consumers look at very specific attributes and willing to pay 37% premium for full transparency

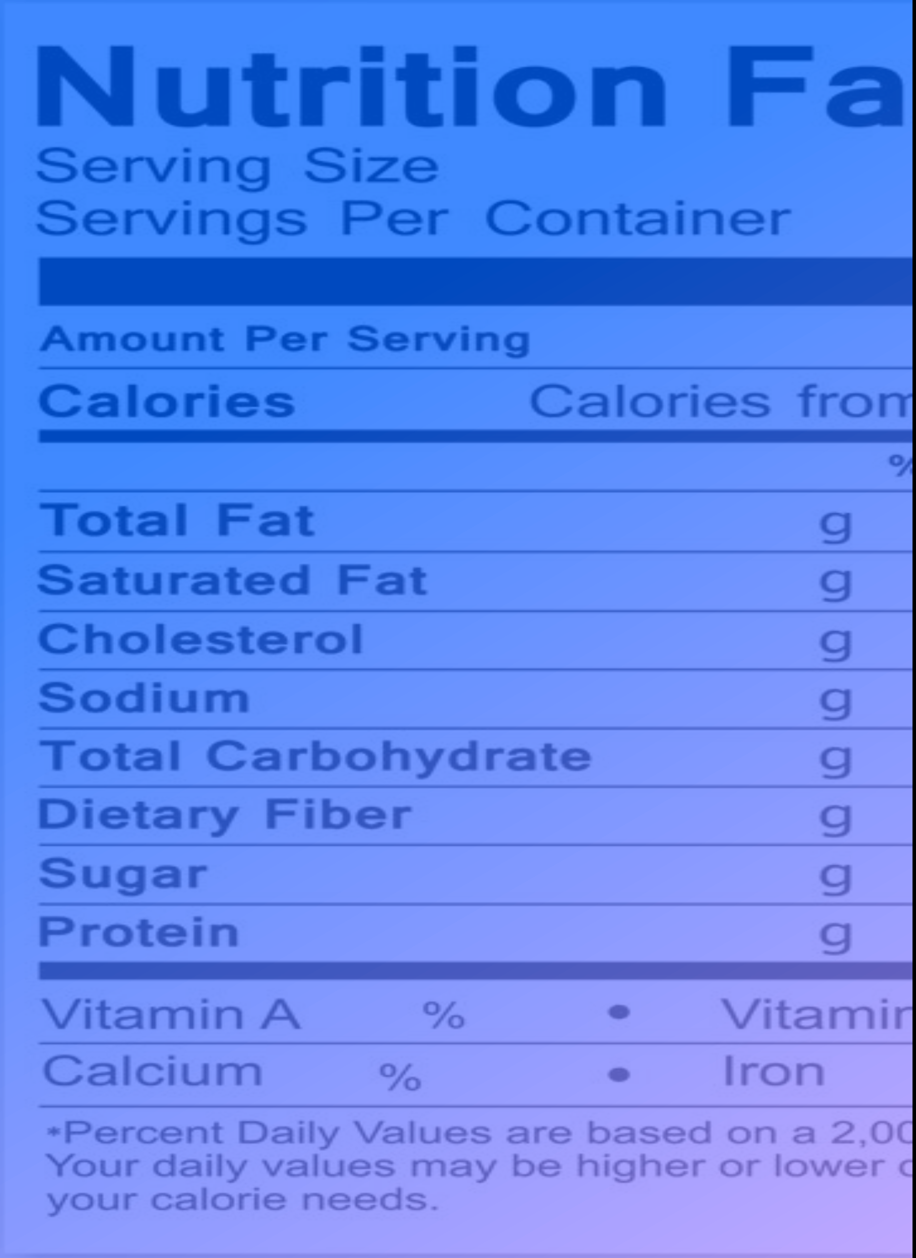
33%

of products from farmers goes uneaten, accounting for $161B USD in food waste

60%

of consumers willing to change shopping habits to reduce environmental impact





Nutrition Fa

Serving Size
Servings Per Container

Amount Per Serving

Calories Calories from

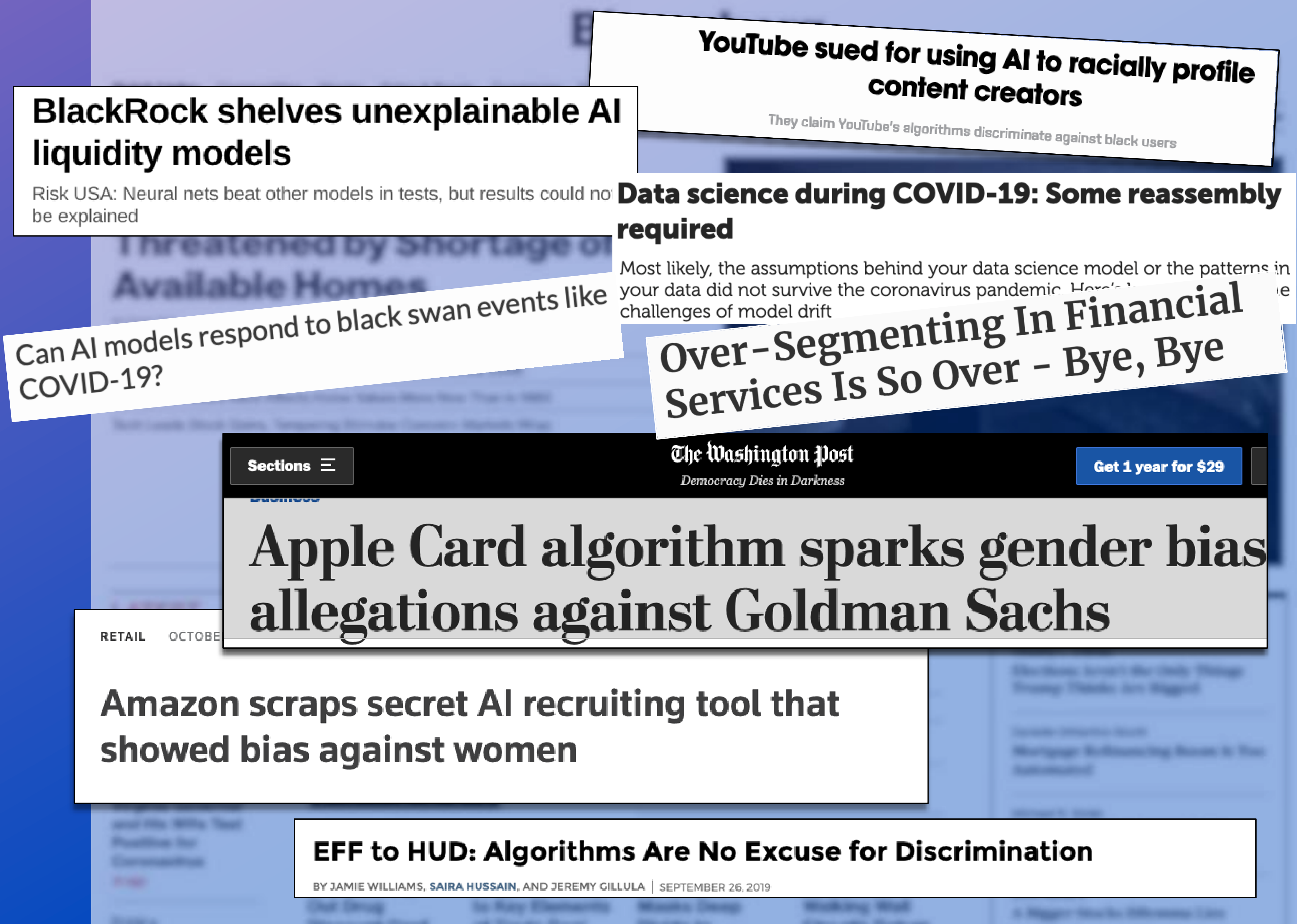
%

Total Fat g
Saturated Fat g
Cholesterol g
Sodium g
Total Carbohydrate g
Dietary Fiber g
Sugar g
Protein g

Vitamin A % • Vitamin
Calcium % • Iron

*Percent Daily Values are based on a 2,00
Your daily values may be higher or lower
your calorie needs.

Rising concerns over trust in AI



YouTube sued for using AI to racially profile content creators

They claim YouTube's algorithms discriminate against black users

BlackRock shelves unexplainable AI liquidity models

Risk USA: Neural nets beat other models in tests, but results could not be explained

Data science during COVID-19: Some reassembly required

Most likely, the assumptions behind your data science model or the patterns in your data did not survive the coronavirus pandemic. Here's ... challenges of model drift

Can AI models respond to black swan events like COVID-19?

Over-Segmenting In Financial Services Is So Over - Bye, Bye

Sections

The Washington Post

Democracy Dies in Darkness

Get 1 year for $29

Apple Card algorithm sparks gender bias allegations against Goldman Sachs

RETAIL OCTOBE

Amazon scraps secret AI recruiting tool that showed bias against women

EFF to HUD: Algorithms Are No Excuse for Discrimination

BY JAMIE WILLIAMS, SAIRA HUSSAIN, AND JEREMY GILLULA | SEPTEMBER 26, 2019

The AI opportunity

AI is the largest economic opportunity of our lifetime, estimated to contribute **$16 trillion** to global DP by 2030.

- **AI and automation will fuel the future of work.**
  - ➢ Enterprises spend over **120** billion hours a year on low-value work.

IDC
ANALYZE THE FUTURE

- **3 in 4 business are exploring or deploying AI.**
  - ➢ CIOs cite AI as the #1 game-changing technology.

Gartner

MORNING CONSULT

- **Winners will scale the value of data with AI.**
  - ➢ **90%** of data is either inaccessible, untrusted, or unanalyzed.

IDC
ANALYZE THE FUTURE

Trustworthy AI:

Governed Data and AI

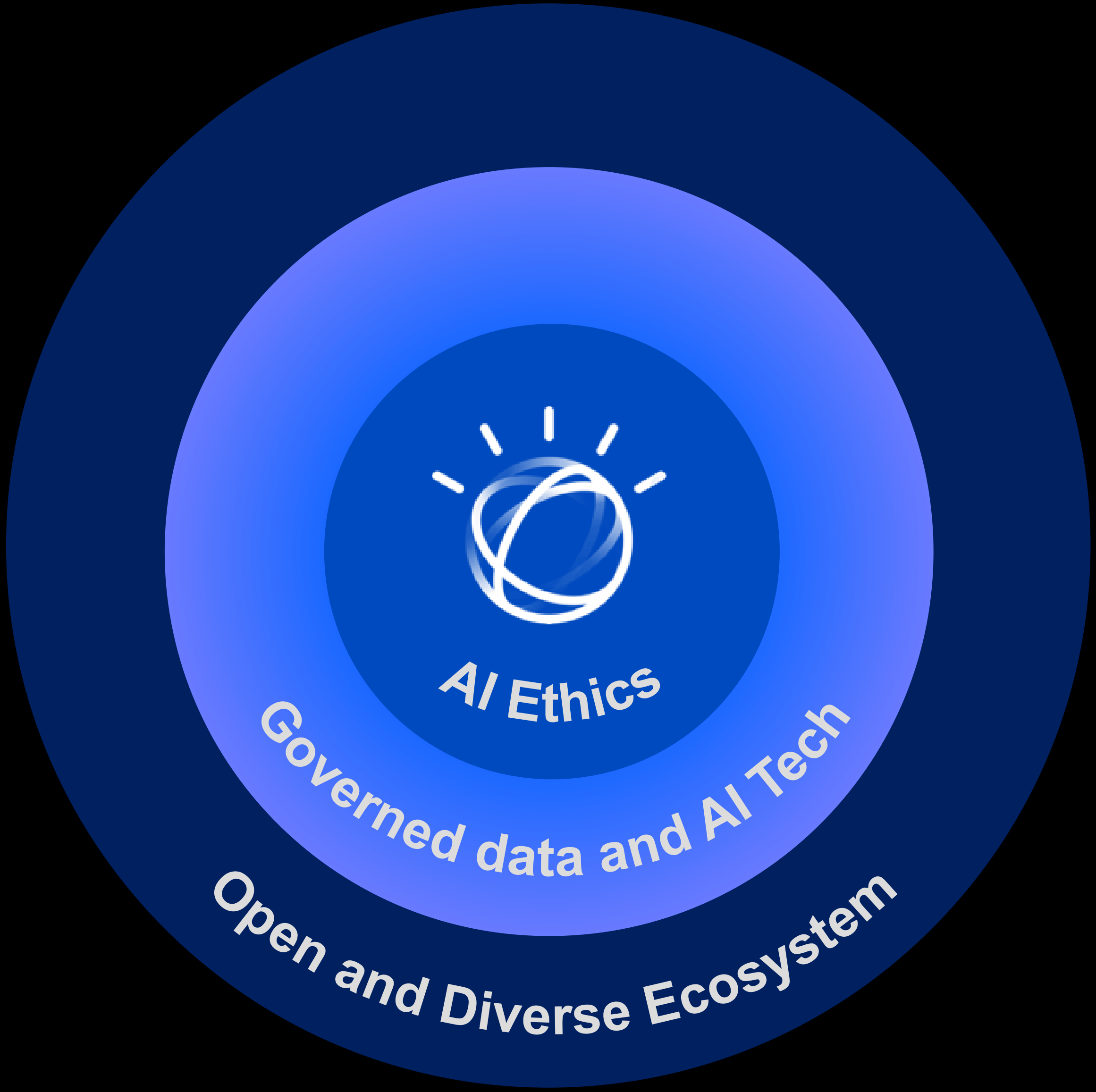
1. Transparent: open to inspection

2. **Explainable**: easy to understand outcomes/decisions

3. **Fair**: impartial and bias mitigated

4. **Robust**: handles exceptional conditions effectively and minimizes security risk

5. **Private**: fueled by high integrity data and is business compliant



Cost of a Data Breach Report

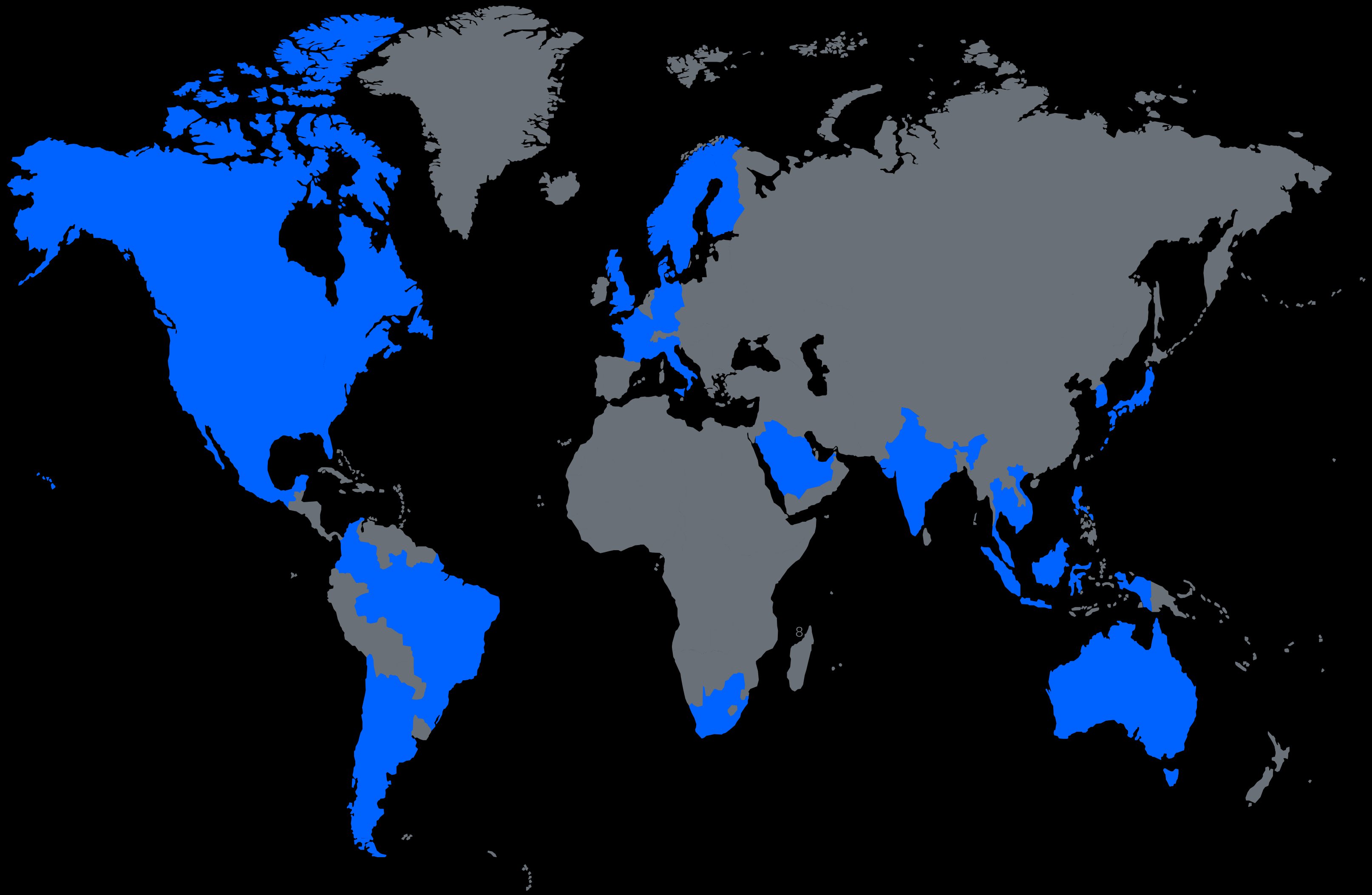
537 breaches studied

3,500 interviews

17 countries/regions

17 industries

17th year



Key findings

- Data breach costs reached a record high, increasing to $4.24M USD.

- The United States ($9.05M) was the costliest country. Healthcare ($9.23M) was the costliest industry.

- The biggest cost savings was due to security AI and automation. Breach costs at orgs with fully deployed security AI/automation had an average cost $3.81M less than orgs with no security AI/automation deployed.

- A zero-trust approach was effective at mitigating costs. Breaches at orgs with mature zero trust deployment were $1.76M less than orgs without zero trust.

- Cloud breaches were least costly in hybrid cloud environments. Breaches in hybrid clouds cost an average $1.19M less than breaches in public clouds.

- Remote working due to COVID-19 increased cost. Breaches where remote work was a factor averaged $1.07 million more than breaches where remote work was not a factor.

Global highlights

$4.24M

Global average cost of a data breach

10%
increase from 2020

$1.07M
Cost increase where remote work was a factor in the breach

$402 million

Average total cost of a breach of >50M records

$3.81 million

Cost savings due to security AI and automation

$180

Cost per record for compromised customer PII

20%

Share of breaches caused by compromised credentials

Top 3 cost amplifying factors

1. Compliance failures
2. System complexity
3. Cloud migration

Top 3 cost mitigating factors

1. AI platforms
2. Encryption
3. Analytics

Time to identify and contain

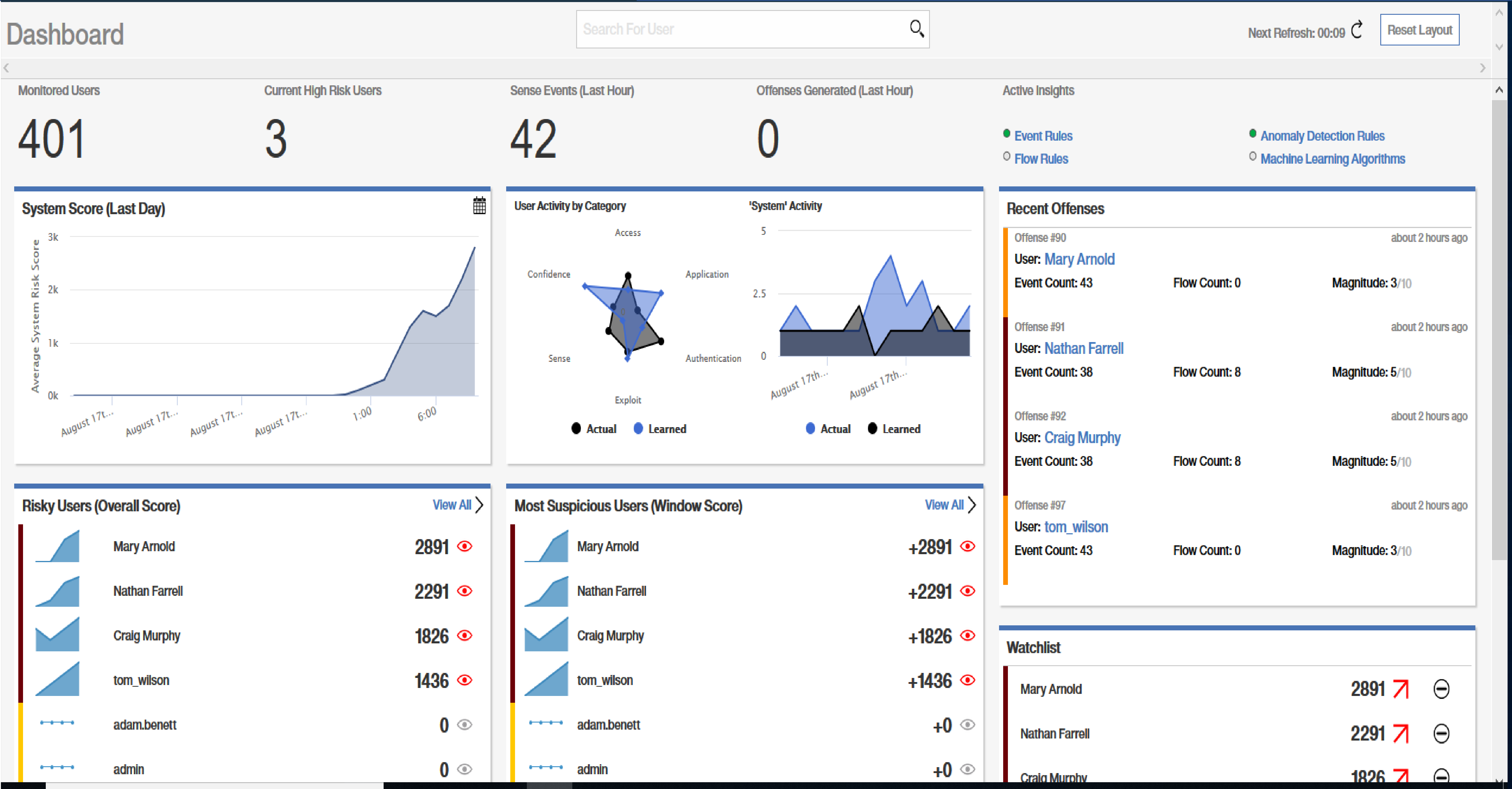
Global average: 287 days

212 days to identify | **75** days to contain

$2.46 million ↓
Average cost savings with incident response teams and IR testing vs. no IR teams or testing

User Behavior

Network Behavior



Monitored Users	Current High Risk Users	Sense Events (Last Hour)	Offenses Generated (Last Hour)
401	3	42	0

Active Insights

- ● Event Rules
- ○ Flow Rules
- ● Anomaly Detection Rules
- ○ Machine Learning Algorithms

System Score (Last Day)

User Activity by Category

'System' Activity

Recent Offenses

Offense #90			about 2 hours ago
User: Mary Arnold			
Event Count: 43	Flow Count: 0	Magnitude: 3/10	
Offense #91			about 2 hours ago
User: Nathan Farrell			
Event Count: 38	Flow Count: 8	Magnitude: 5/10	
Offense #92			about 2 hours ago
User: Craig Murphy			
Event Count: 38	Flow Count: 8	Magnitude: 5/10	
Offense #97			about 2 hours ago
User: tom_wilson			
Event Count: 43	Flow Count: 0	Magnitude: 3/10	

Risky Users (Overall Score)

View All

Mary Arnold	2891
Nathan Farrell	2291
Craig Murphy	1826
tom_wilson	1436
adam.benett	0
admin	0

Most Suspicious Users (Window Score)

View All

Mary Arnold	+2891
Nathan Farrell	+2291
Craig Murphy	+1826
tom_wilson	+1436
adam.benett	+0
admin	+0

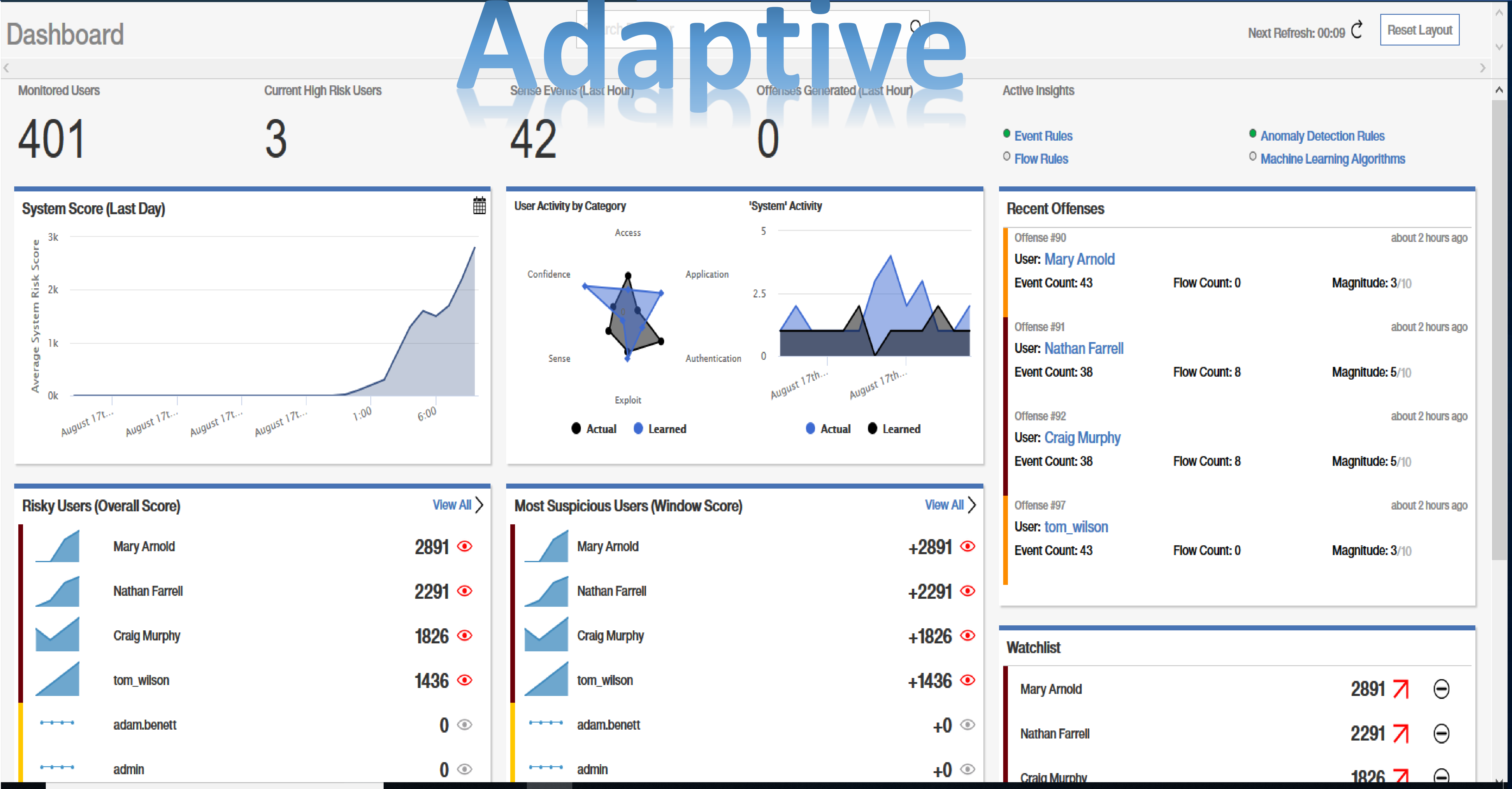
Watchlist

Mary Arnold	2891
Nathan Farrell	2291
Craig Murphy	1826

User Behavior

Network Behavior

Adaptive



Monitored Users: 401

Current High Risk Users: 3

Sense Events (Last Hour): 42

Offenses Generated (Last Hour): 0

Active Insights

- ● Event Rules
- ○ Flow Rules
- ● Anomaly Detection Rules
- ○ Machine Learning Algorithms

System Score (Last Day)

User Activity by Category

'System' Activity

Recent Offenses

Offense #90 — about 2 hours ago
User: Mary Arnold
Event Count: 43 Flow Count: 0 Magnitude: 3/10

Offense #91 — about 2 hours ago
User: Nathan Farrell
Event Count: 38 Flow Count: 8 Magnitude: 5/10

Offense #92 — about 2 hours ago
User: Craig Murphy
Event Count: 38 Flow Count: 8 Magnitude: 5/10

Offense #97 — about 2 hours ago
User: tom_wilson
Event Count: 43 Flow Count: 0 Magnitude: 3/10

Risky Users (Overall Score)

Mary Arnold	2891
Nathan Farrell	2291
Craig Murphy	1826
tom_wilson	1436
adam.benett	0
admin	0

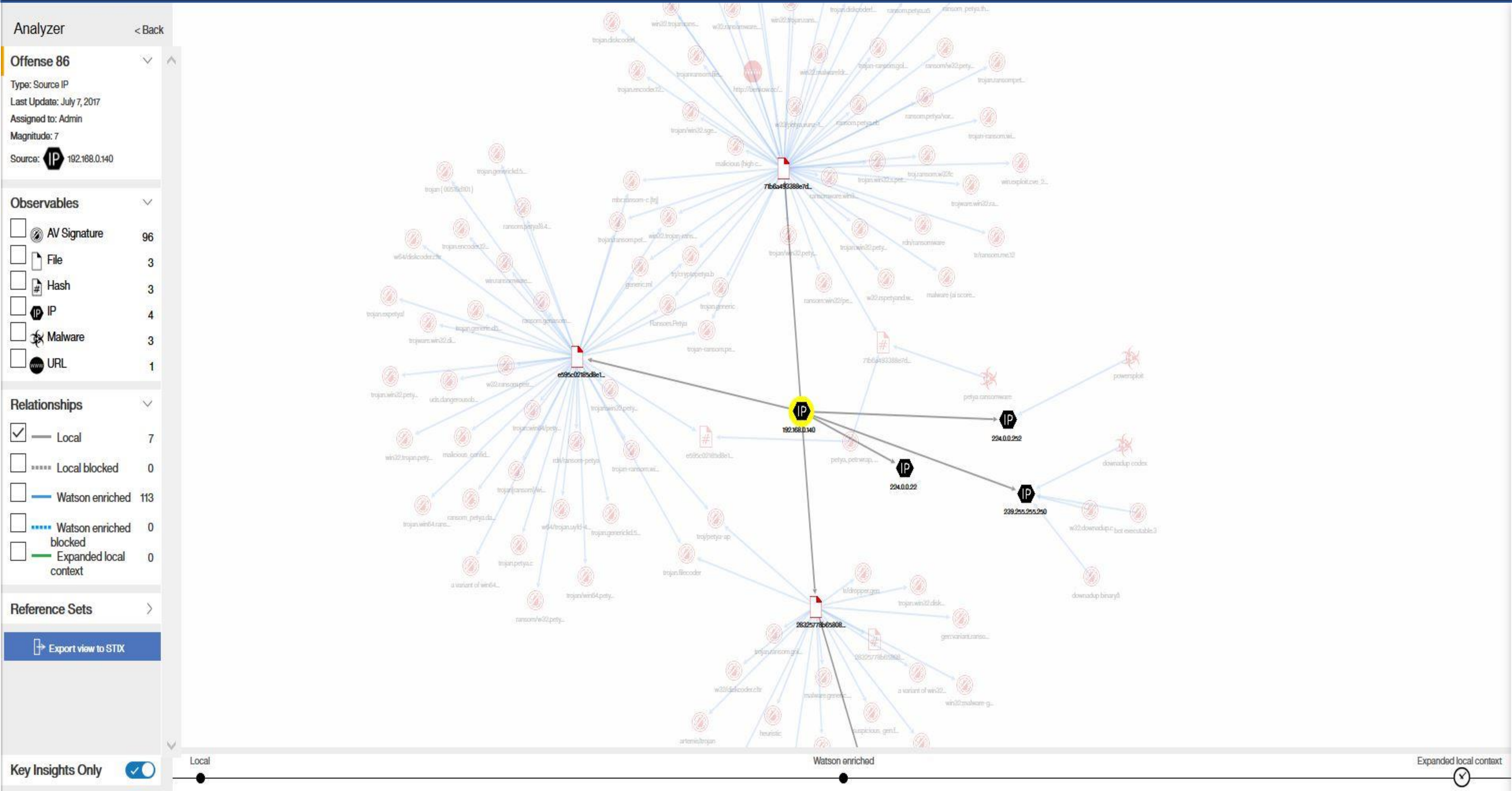
Most Suspicious Users (Window Score)

Mary Arnold	+2891
Nathan Farrell	+2291
Craig Murphy	+1826
tom_wilson	+1436
adam.benett	+0
admin	+0

Watchlist

Mary Arnold	2891
Nathan Farrell	2291
Craig Murphy	1826

Local Analysis



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

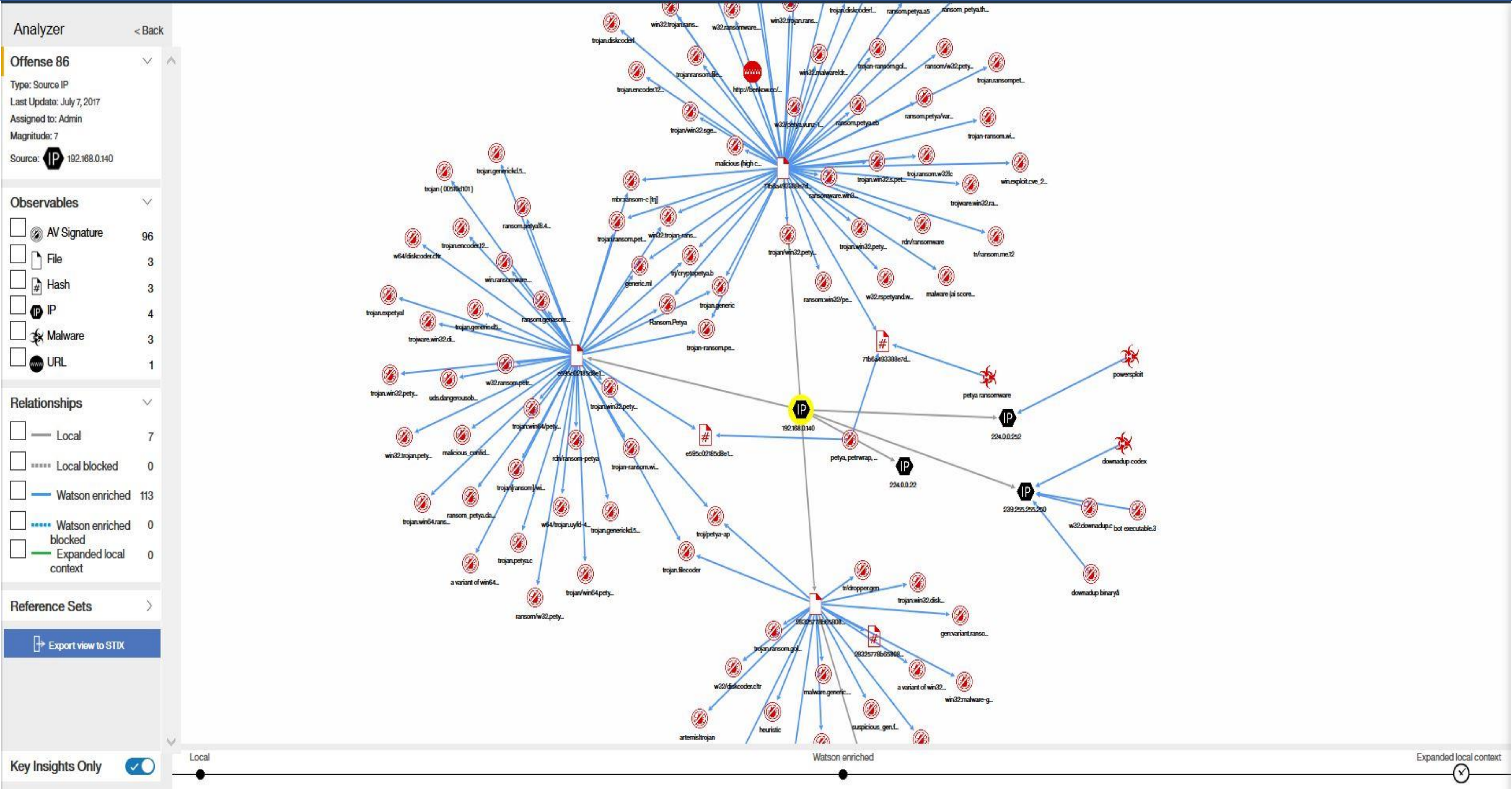
☑	Local	7
□	Local blocked	0
□	Watson enriched	113
□	Watson enriched blocked	0
□	Expanded local context	0

Reference Sets >

Export view to STIX

Key Insights Only ✓

AI Enriched Analysis



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

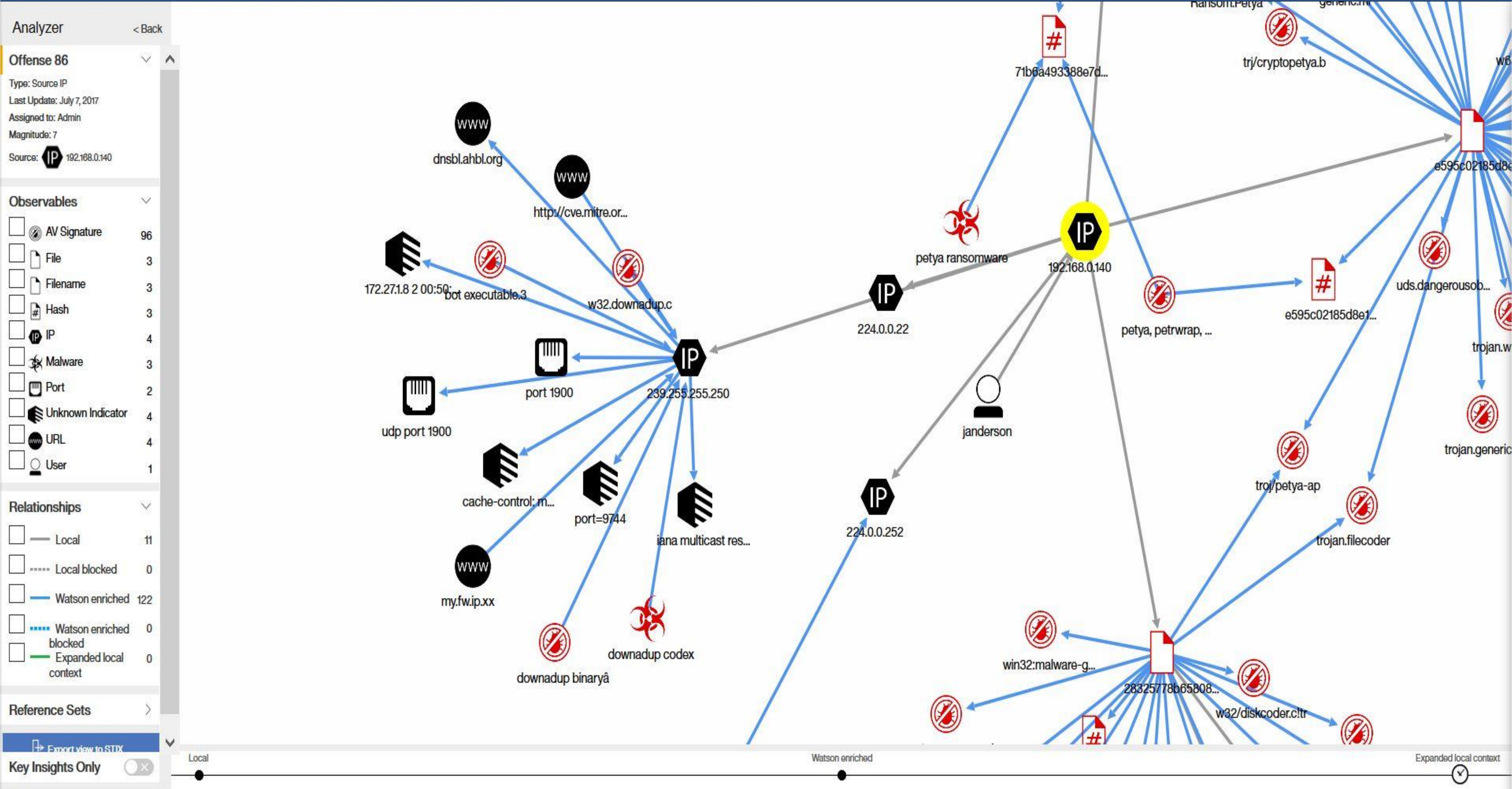
□	Local	7
□	Local blocked	0
□	Watson enriched	113
□	Watson enriched blocked	0
□	Expanded local context	0

Reference Sets

Export view to STIX

Key Insights Only

AI Deep Insight



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
□ Filename	3
□ Hash	3
□ IP	4
□ Malware	3
□ Port	2
□ Unknown Indicator	4
□ URL	4
□ User	1

Relationships

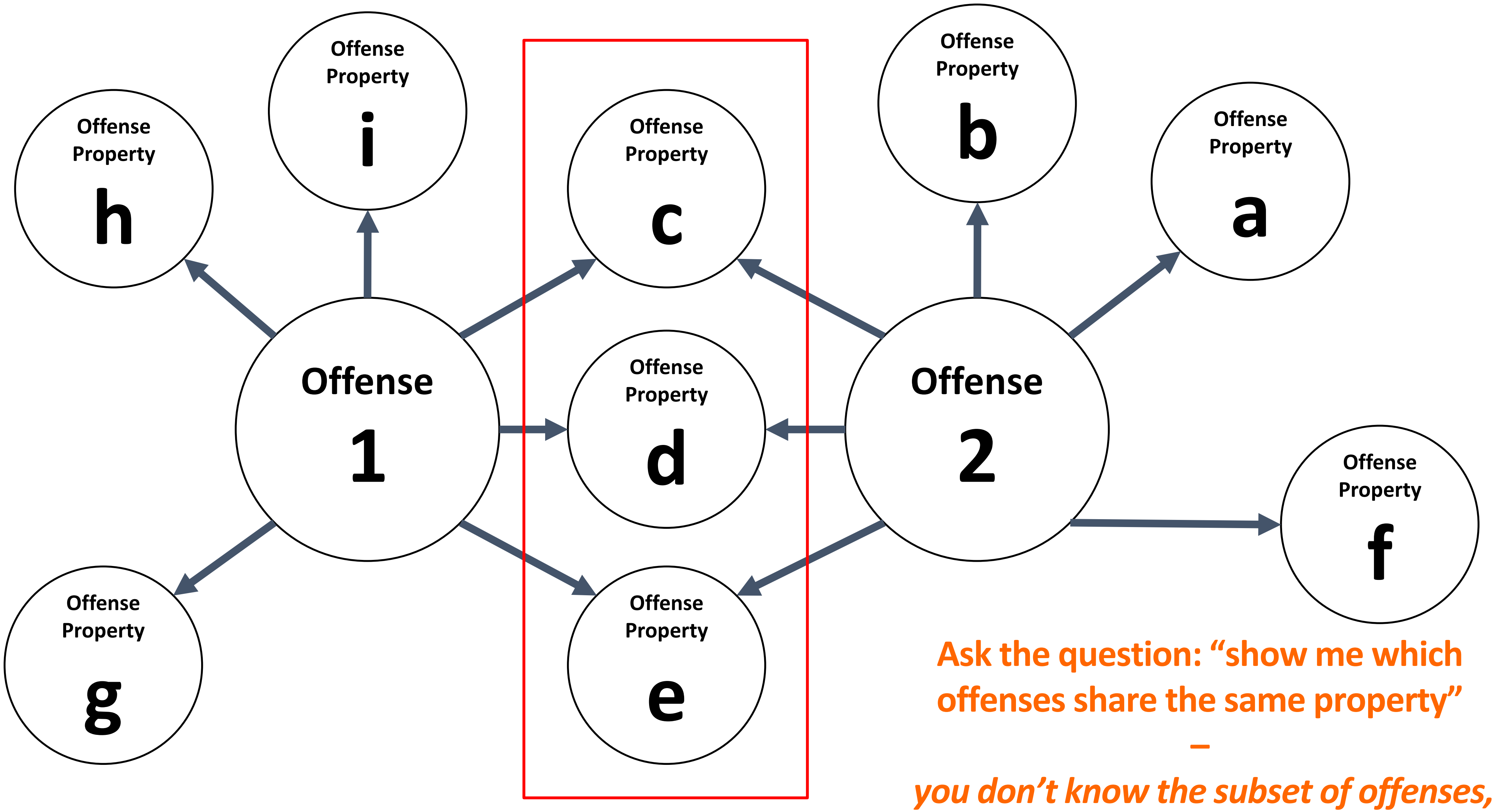
□ Local	11
□ Local blocked	0
□ Watson enriched	122
□ Watson enriched blocked	0
□ Expanded local context	0

Reference Sets

Export view to STIX

Key Insights Only

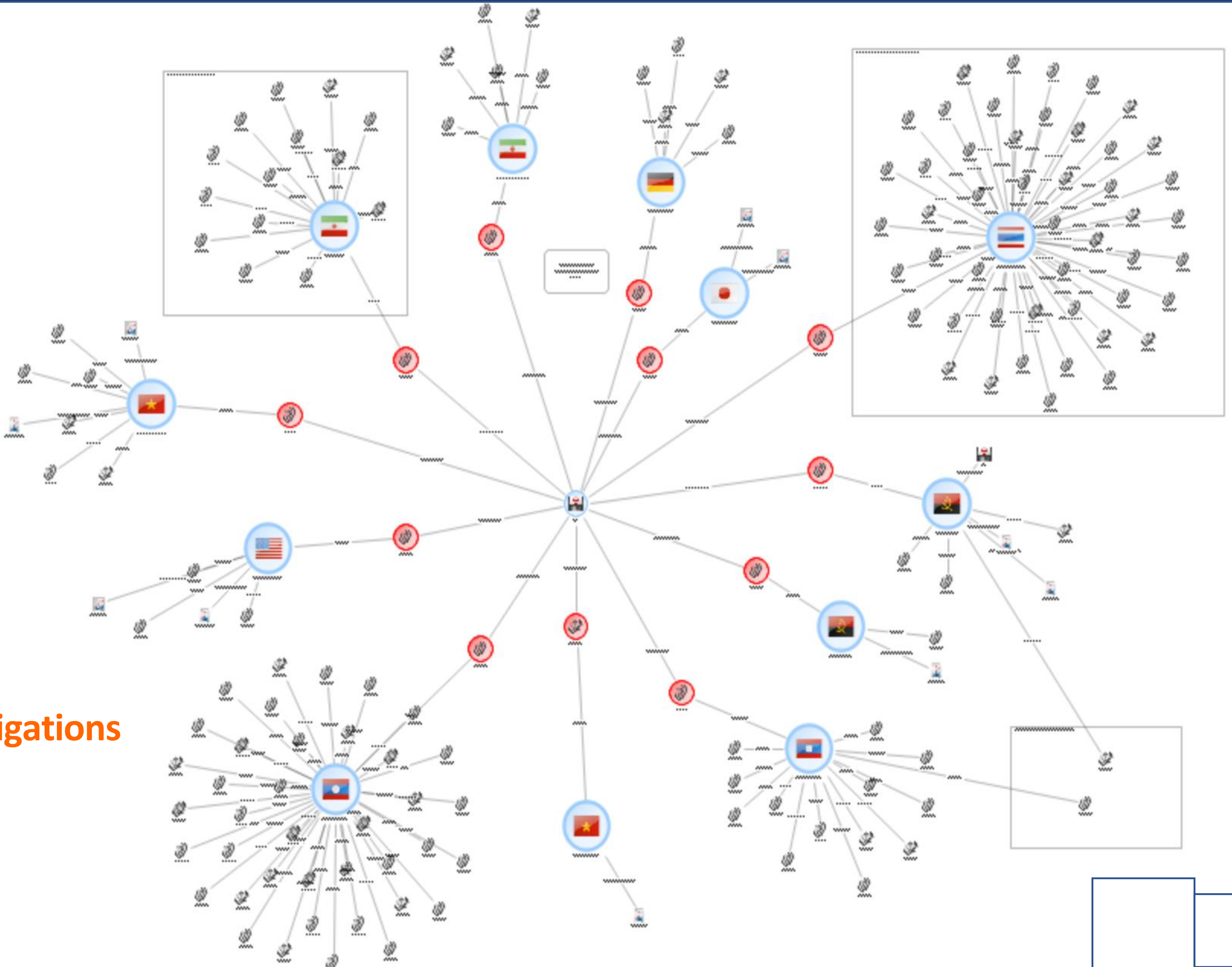
What is an Unknown Unknown Search



Ask the question: “show me which offenses share the same property”

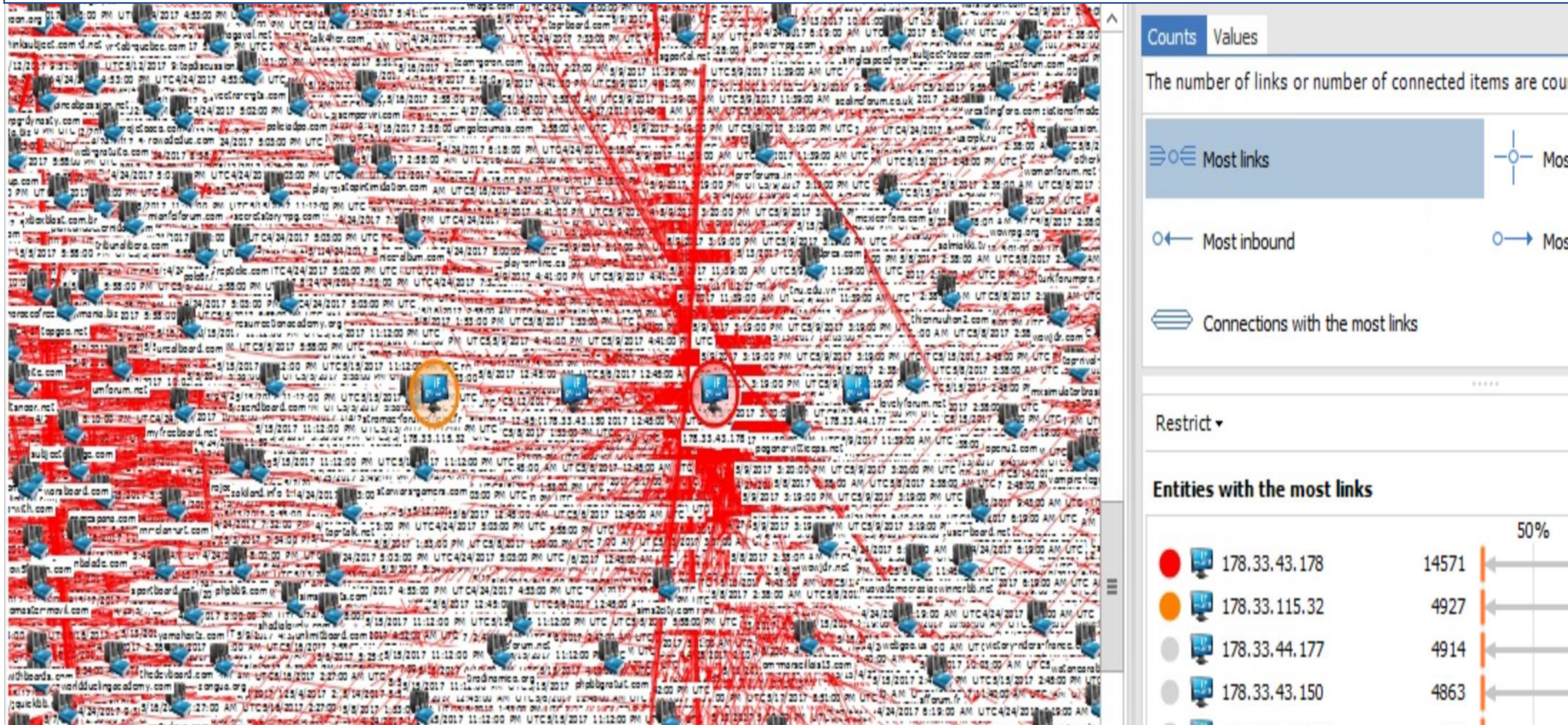
–

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



Investigations

Threat Hunting

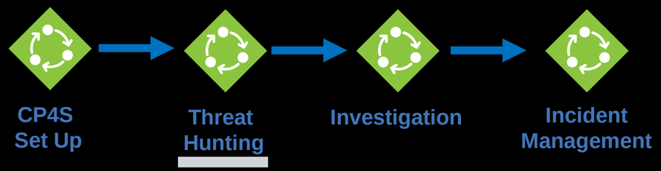


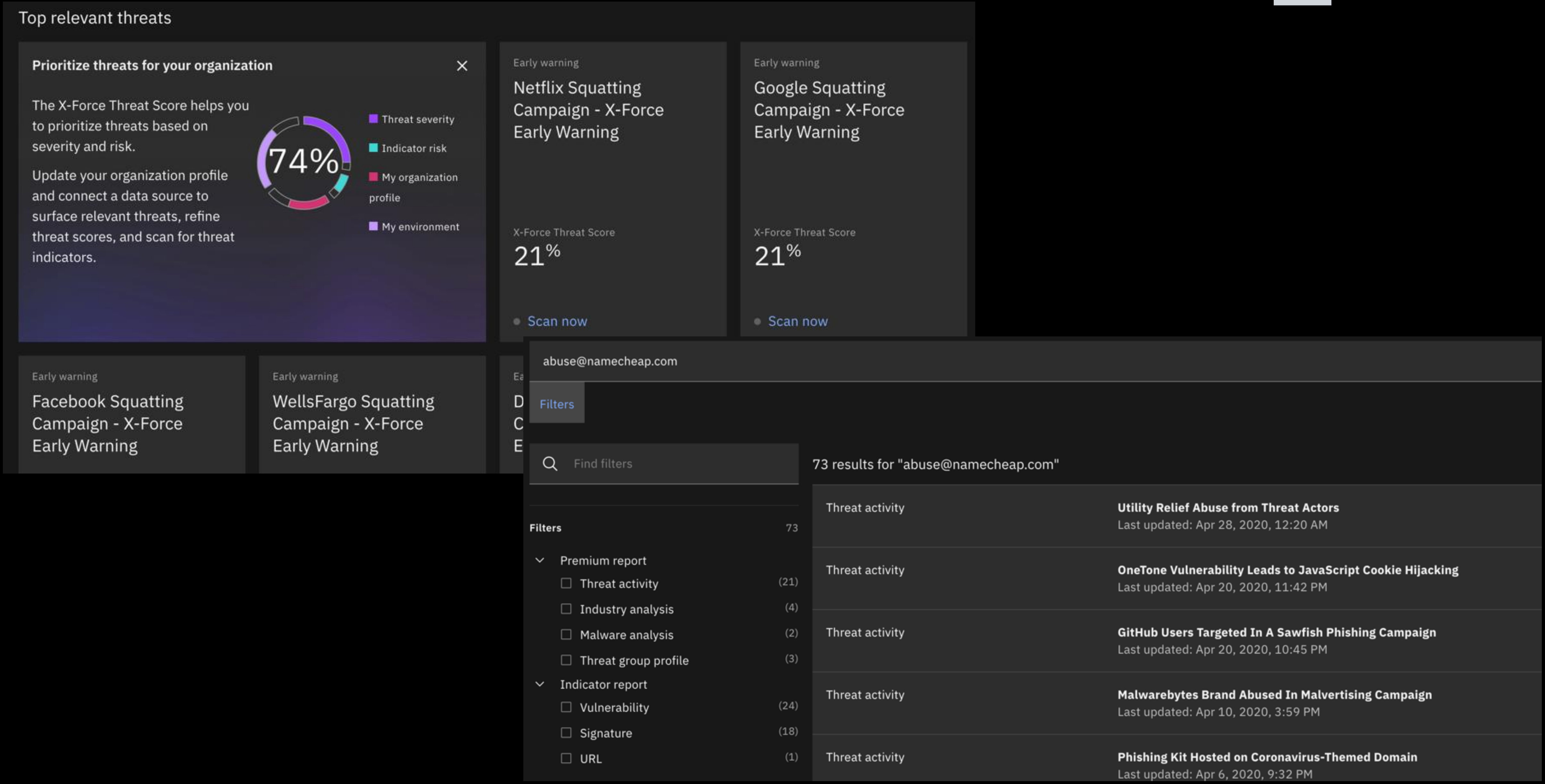
The number of links or number of connected items are cou

Entities with the most links

		50%
● 178.33.43.178	14571	
● 178.33.115.32	4927	
○ 178.33.44.177	4914	
○ 178.33.43.150	4863	

XDR - Extended Detection and Response





Top relevant threats

Prioritize threats for your organization ✕

The X-Force Threat Score helps you to prioritize threats based on severity and risk.

Update your organization profile and connect a data source to surface relevant threats, refine threat scores, and scan for threat indicators.

Early warning

Netflix Squatting Campaign - X-Force Early Warning

X-Force Threat Score

21%

Scan now

Early warning

Google Squatting Campaign - X-Force Early Warning

X-Force Threat Score

21%

Scan now

Early warning

Facebook Squatting Campaign - X-Force Early Warning

Early warning

WellsFargo Squatting Campaign - X-Force Early Warning

Ea

D

C

E

abuse@namecheap.com

Filters

Find filters

73 results for "abuse@namecheap.com"

Filters 73

- Premium report
  - □ Threat activity (21)
  - □ Industry analysis (4)
  - □ Malware analysis (2)
  - □ Threat group profile (3)
- Indicator report
  - □ Vulnerability (24)
  - □ Signature (18)
  - □ URL (1)

Threat activity	**Utility Relief Abuse from Threat Actors** Last updated: Apr 28, 2020, 12:20 AM
Threat activity	**OneTone Vulnerability Leads to JavaScript Cookie Hijacking** Last updated: Apr 20, 2020, 11:42 PM
Threat activity	**GitHub Users Targeted In A Sawfish Phishing Campaign** Last updated: Apr 20, 2020, 10:45 PM
Threat activity	**Malwarebytes Brand Abused In Malvertising Campaign** Last updated: Apr 10, 2020, 3:59 PM
Threat activity	**Phishing Kit Hosted on Coronavirus-Themed Domain** Last updated: Apr 6, 2020, 9:32 PM

The Evolution of AI in Security

Michael Melore, CISSP
IBM Senior Cybersecurity Advisor
Chair SECRT (Security <Leaders> Round Table)
FBI InfraGard Committeemen
NASCIO Privacy and Cyber Security Committees
CISA / ATARC CDRT (Critical Defense Round Table) Steering Committee

FOLLOW US ON twitter

@MichaelMelore