SANS Cyber Threat Intelligence SUMMIT & TRAINING

There Can Be Only One!: Last CTI Vendor Standing Pitch

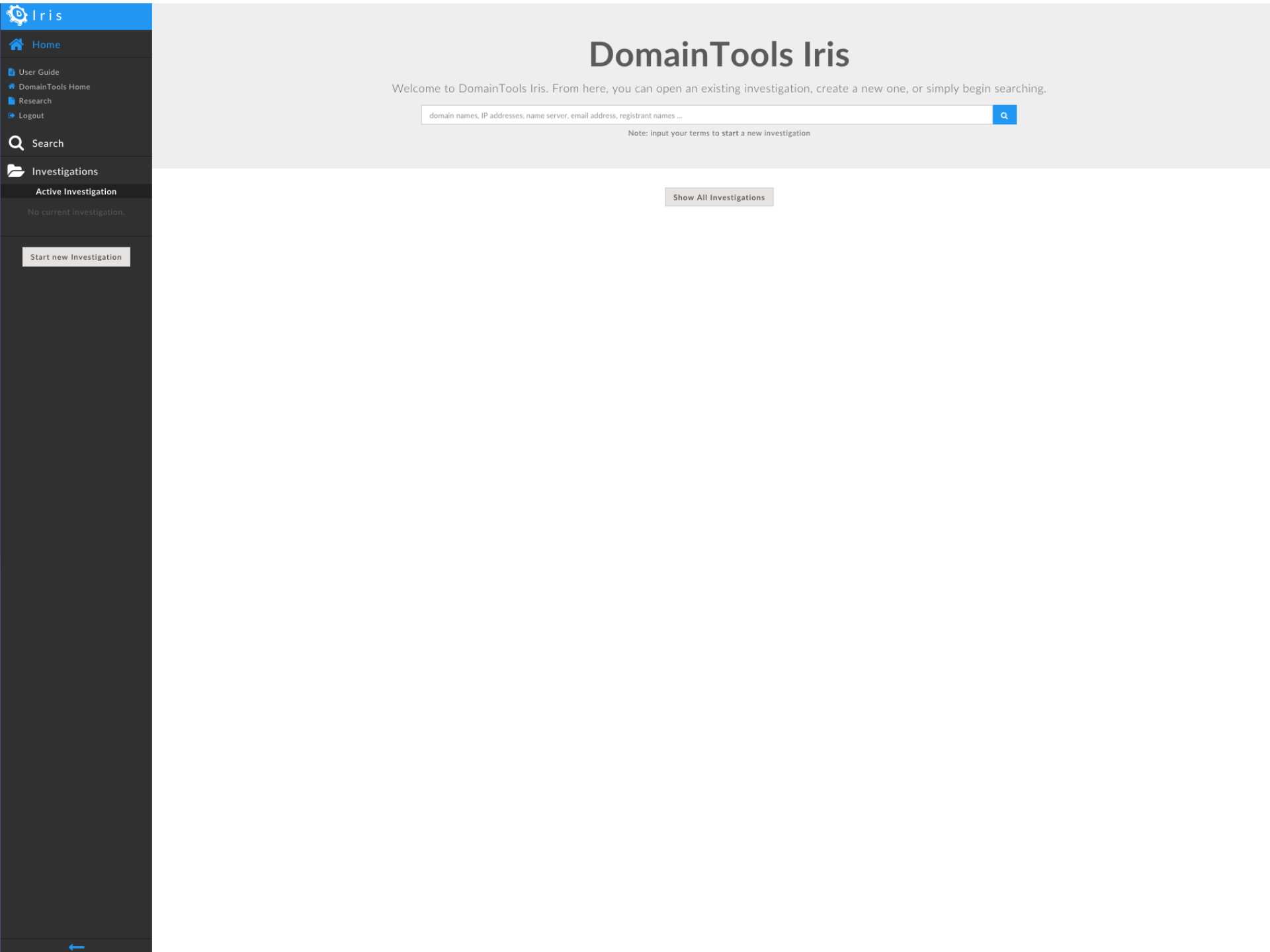
Moderator: John Pescatore, Director, SANS Institute
Mark Kendrick, DomainTools
Matt Kodama, RecordedFuture
Jess Parnell, Centripetal Networks
Roselle Safran, UpLevel Security

SANS Cyber Threat Intelligence SUMMIT & TRAINING

There Can Be Only One!: Last CTI Vendor Standing Pitch

Mark Kendrick, DomainTools


See Threats Coming
DETECT | INVESTIGATE | PREVENT
DOMAINTOOLS


Iris
Home
User Guide
DomainTools Home
Research
Logout
Search
Investigations
Active Investigation
No current investigation.
Start new Investigation
DomainTools Iris
Welcome to DomainTools Iris. From here, you can open an existing investigation, create a new one, or simply begin searching.
domain names, IP addresses, name server, email address, registrant names ...
Note: input your terms to start a new investigation
Show All Investigations

pdfpump.net | Advanced | Back | Filters: pdfpump.net

Pivot Engine | Stats

View: Default | .CSV

Page 1 of 1 *(1 record total)*

Domain	Risk Score	Email	Email Domain	Contact Information
pdfpump.net	20.42	Address: contact@privacyprotect.org (Admin, Registrant, Technical) Address: abuse-contact@publicdomainregistry.com (Whois)	privacyprotect.org publicdomainregistry.com	Name: Domain Admin Organization: Privacy Protection Service INC d/b/a PrivacyProtect.or

Search History

Last updated: a few seconds ago

Domain Profile | Whois History | Hosting History

pdfpump.net

Email

- abuse-contact@publicdomainregistry.com is associated with ~ 4,608,914 domains
- contact@privacyprotect.org is associated with ~ 1,591,727 domains

Registrant

- Domain Admin

Registrant Org

- Privacy Protection Service INC d/b/a PrivacyProtect.org

Registrar

- PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM

Registrar Status

- clientTransferProhibited

Dates

- **Created:** 2015-10-15
- **Expires:** 2016-10-15

Name Servers

- ns1.pdfpump.net (has 1 domain)
- ns2.pdfpump.net (has 1 domain)

IP Address

- 199.80.54.171 ~ 1 other site hosted on this server

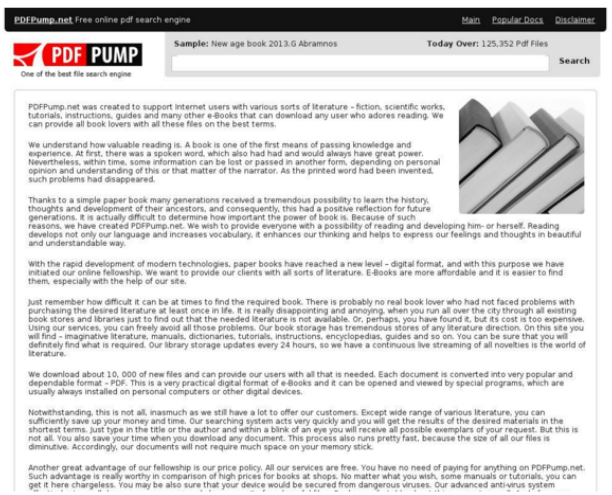
IP Profile | Screenshot History | IP Tools

pdfpump.net

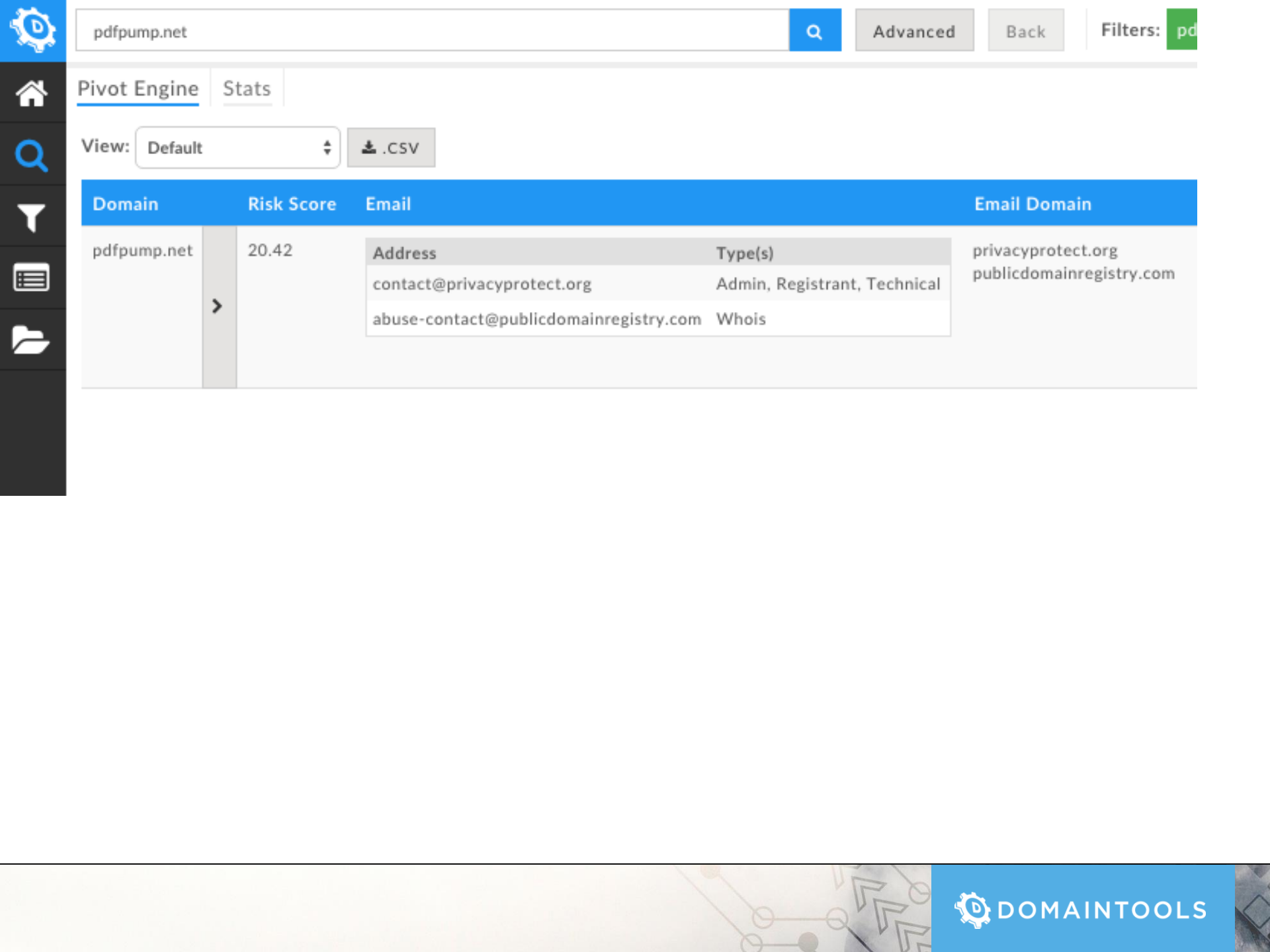
Queue screenshot for update

See all

‹ Previous | Nov 10, 2015 (2 months ago) | Next ›



Pivot Engine | Search History | Stats | Domain Profile | Screenshot History | Whois History | IP Profile | Hosting History | IP Tools | Visualization


pdfpump.net
Advanced
Back
Filters: pd
Pivot Engine
Stats
View: Default
.CSV
Domain
Risk Score
Email
Email Domain
pdfpump.net
20.42
Address
Type(s)
contact@privacyprotect.org
Admin, Registrant, Technical
abuse-contact@publicdomainregistry.com
Whois
privacyprotect.org
publicdomainregistry.com
DOMAINTOOLS

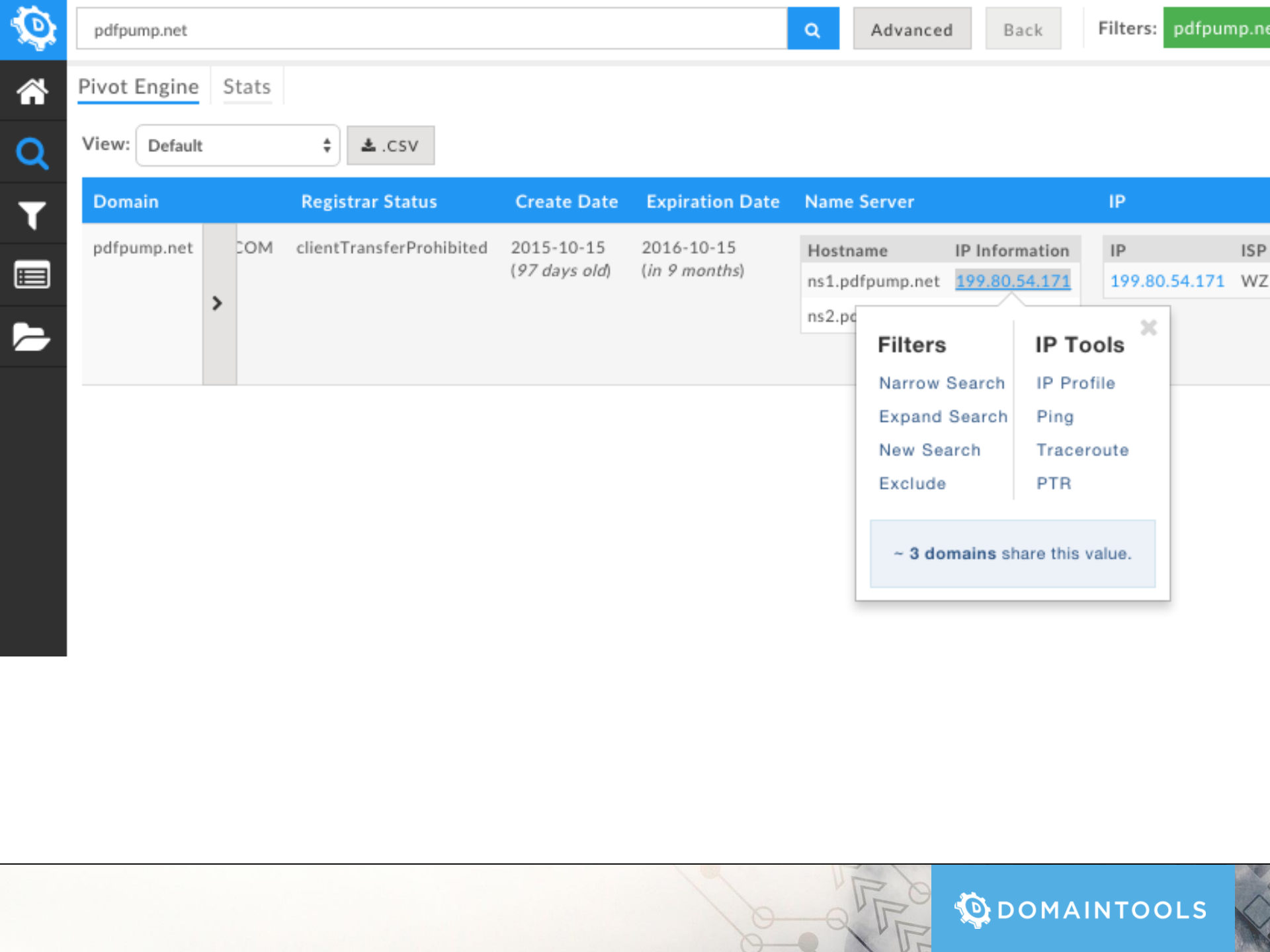
pdfpump.net

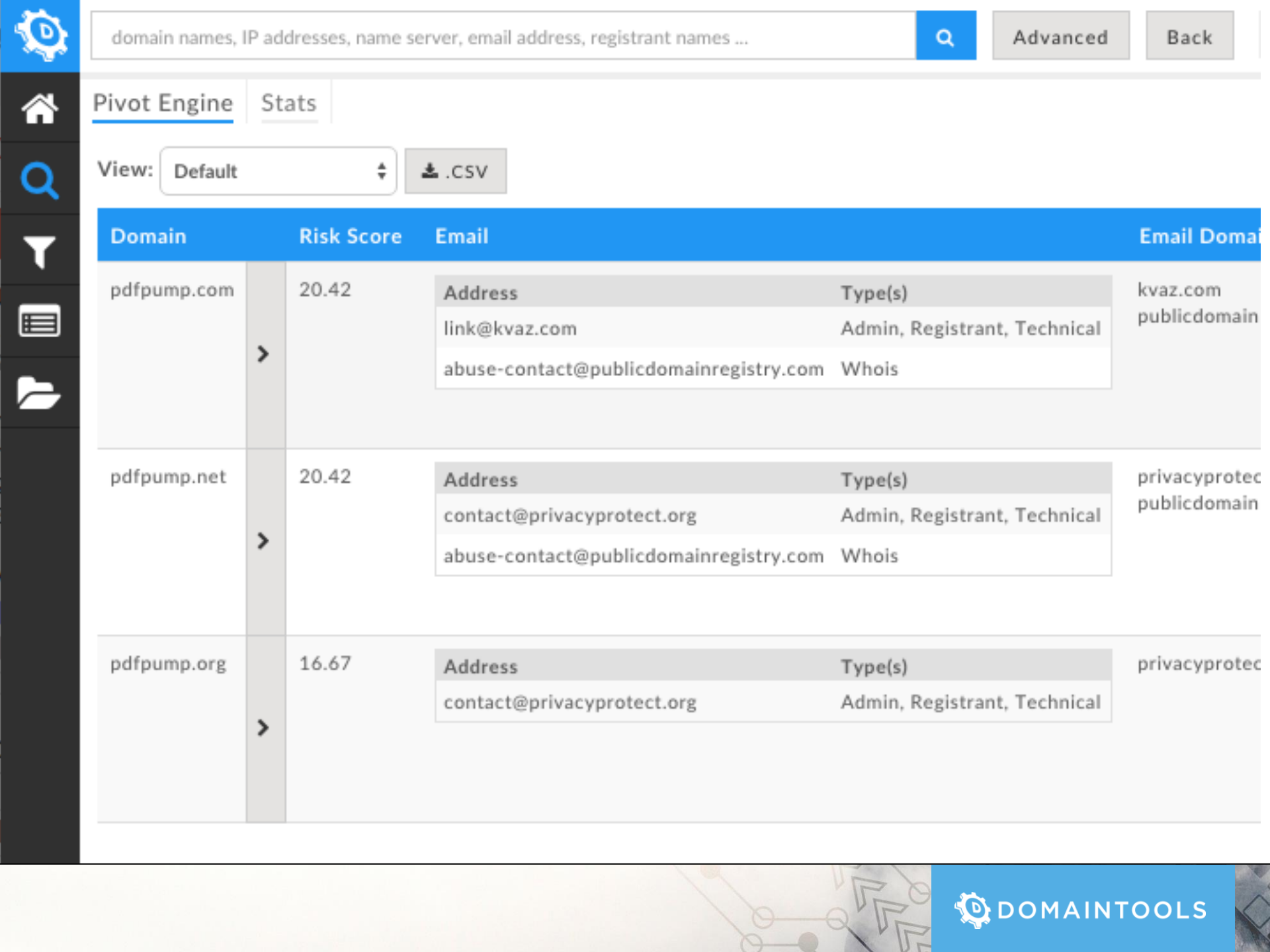
Advanced | Back | Filters: pdfpump.n

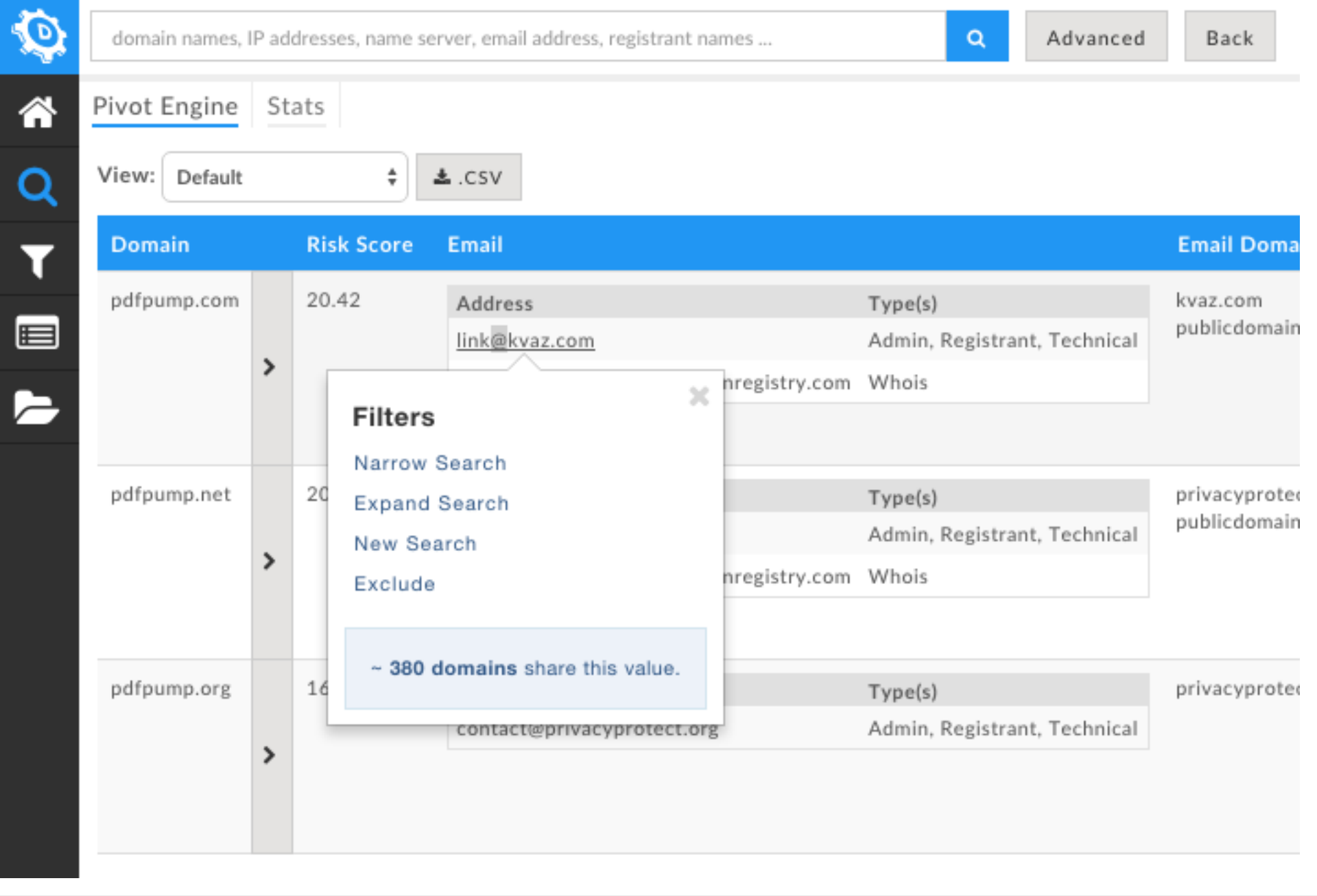
Pivot Engine | Stats

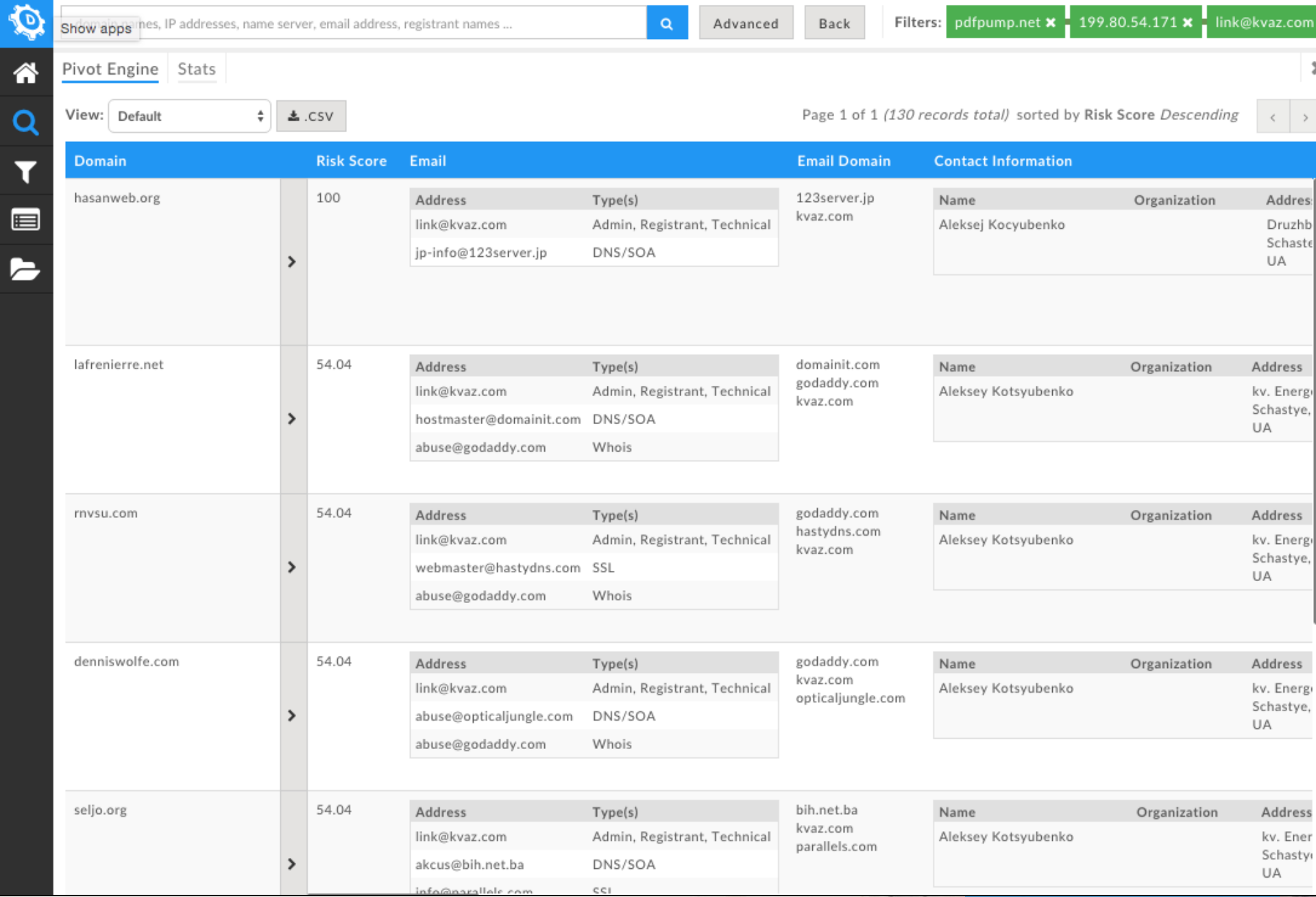
View: Default | .CSV

Domain		Registrar Status	Create Date	Expiration Date	Name Server		IP	
pdfpump.net	COM	clientTransferProhibited	2015-10-15 (*97 days old*)	2016-10-15 (*in 9 months*)	Hostname	IP Information	IP	ISP
					ns1.pdfpump.net	199.80.54.171	199.80.54.171	WZ
					ns2.pdfpump.net	199.80.54.183		


pdfpump.net
Advanced
Back
Filters:
pdfpump.ne
Pivot Engine
Stats
View:
Default
.CSV
Domain
Registrar Status
Create Date
Expiration Date
Name Server
IP
pdfpump.net
COM
clientTransferProhibited
2015-10-15
(97 days old)
2016-10-15
(in 9 months)
Hostname
IP Information
ns1.pdfpump.net
199.80.54.171
ns2.pd
IP
ISP
199.80.54.171
WZ
Filters
Narrow Search
Expand Search
New Search
Exclude
IP Tools
IP Profile
Ping
Traceroute
PTR
~ 3 domains share this value.
DOMAINTOOLS


domain names, IP addresses, name server, email address, registrant names ...
Advanced
Back
Pivot Engine
Stats
View:
Default
.CSV
Domain
Risk Score
Email
Email Domai
pdfpump.com
20.42
Address
Type(s)
link@kvaz.com
Admin, Registrant, Technical
abuse-contact@publicdomainregistry.com
Whois
kvaz.com
publicdomain
pdfpump.net
20.42
Address
Type(s)
contact@privacyprotect.org
Admin, Registrant, Technical
abuse-contact@publicdomainregistry.com
Whois
privacyprotec
publicdomain
pdfpump.org
16.67
Address
Type(s)
contact@privacyprotect.org
Admin, Registrant, Technical
privacyprotec
DOMAINTOOLS


domain names, IP addresses, name server, email address, registrant names ...
Advanced
Back
Pivot Engine
Stats
View:
Default
.CSV
Domain
Risk Score
Email
Email Doma
pdfpump.com
20.42
Address
Type(s)
kvaz.com
publicdomain
link@kvaz.com
Admin, Registrant, Technical
nregistry.com
Whois
Filters
Narrow Search
Expand Search
New Search
Exclude
~ 380 domains share this value.
pdfpump.net
Type(s)
privacyprotec
publicdomain
Admin, Registrant, Technical
nregistry.com
Whois
pdfpump.org
Type(s)
privacyprotec
contact@privacyprotect.org
Admin, Registrant, Technical


Show apps
nes, IP addresses, name server, email address, registrant names ...
Advanced
Back
Filters:
pdfpump.net
199.80.54.171
link@kvaz.com
Pivot Engine
Stats
View:
Default
.CSV
Page 1 of 1 (130 records total) sorted by Risk Score Descending
Domain
Risk Score
Email
Email Domain
Contact Information
hasanweb.org
100
Address
Type(s)
link@kvaz.com
Admin, Registrant, Technical
jp-info@123server.jp
DNS/SOA
123server.jp
kvaz.com
Name
Organization
Addres
Aleksej Kocyubenko
Druzhb
Schaste
UA
lafrenierre.net
54.04
Address
Type(s)
link@kvaz.com
Admin, Registrant, Technical
hostmaster@domainit.com
DNS/SOA
abuse@godaddy.com
Whois
domainit.com
godaddy.com
kvaz.com
Name
Organization
Address
Aleksey Kotsyubenko
kv. Energ
Schastye,
UA
rnvsu.com
54.04
Address
Type(s)
link@kvaz.com
Admin, Registrant, Technical
webmaster@hastydns.com
SSL
abuse@godaddy.com
Whois
godaddy.com
hastydns.com
kvaz.com
Name
Organization
Address
Aleksey Kotsyubenko
kv. Energ
Schastye,
UA
denniswolfe.com
54.04
Address
Type(s)
link@kvaz.com
Admin, Registrant, Technical
abuse@opticaljungle.com
DNS/SOA
abuse@godaddy.com
Whois
godaddy.com
kvaz.com
opticaljungle.com
Name
Organization
Address
Aleksey Kotsyubenko
kv. Energ
Schastye,
UA
seljo.org
54.04
Address
Type(s)
link@kvaz.com
Admin, Registrant, Technical
akcus@bih.net.ba
DNS/SOA
bih.net.ba
kvaz.com
parallels.com
Name
Organization
Address
Aleksey Kotsyubenko
kv. Ener
Schasty
UA
DOMAINTOOLS

Iris Overview

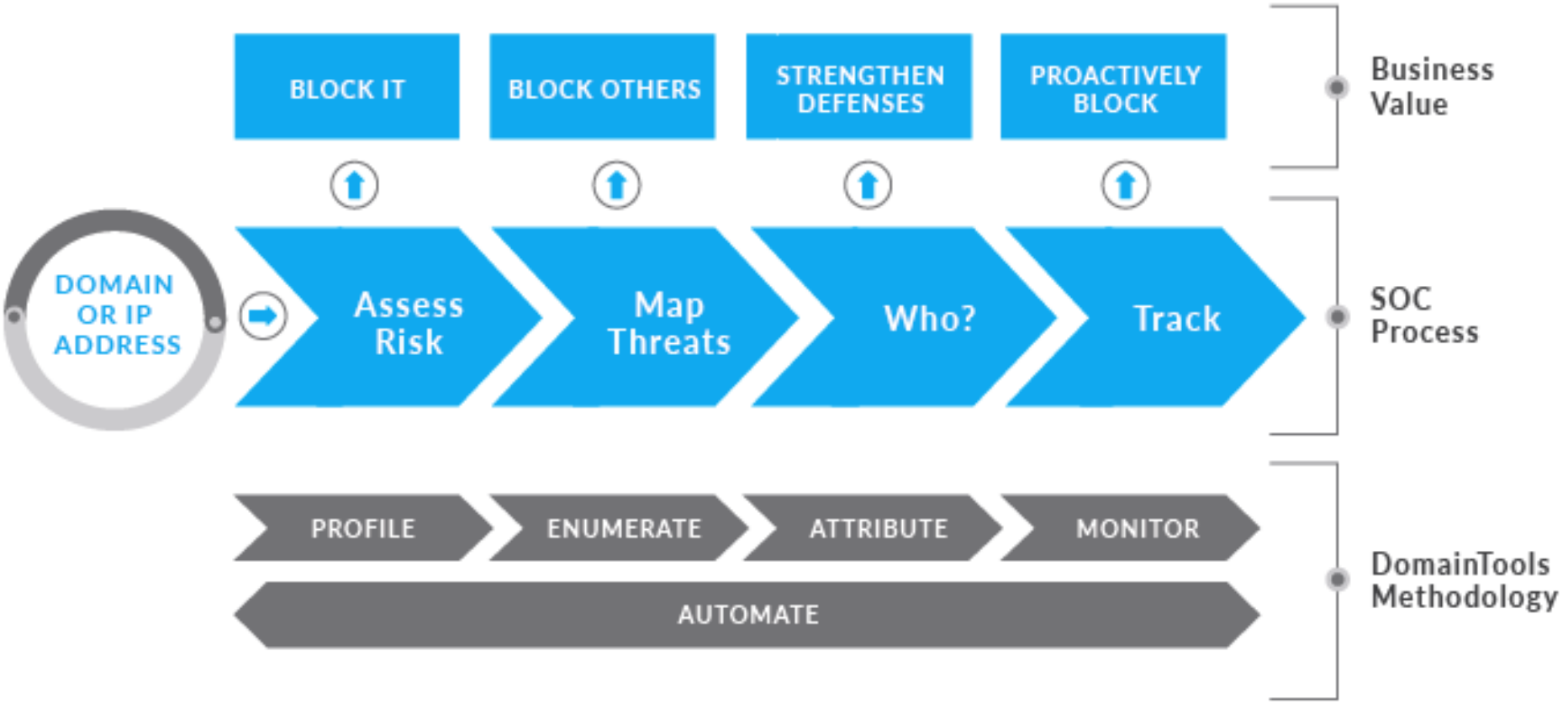
DOMAINTOOLS

USE CASES

- Got Behind Privacy by Leveraging Attached Infrastructure (NSIP)
- Uncovered Who Owned the Domain
- Uncovered the Domains Connected to the Same Actor

- Proactively block access
- Search For Domains in Network Logs (DNS, Proxy, etc)
- Study Infrastructure
- Monitor Future Registrations

Methodology & Process




See Threats Coming
DETECT | INVESTIGATE | PREVENT
sales@domaintools.com
DOMAINTOOLS

SANS Cyber Threat Intelligence SUMMIT & TRAINING

There Can Be Only One!: Last CTI Vendor Standing Pitch

Matt Kodama, RecordedFuture

Recorded Future
CREATING AN INSIGHTFUL WORLD

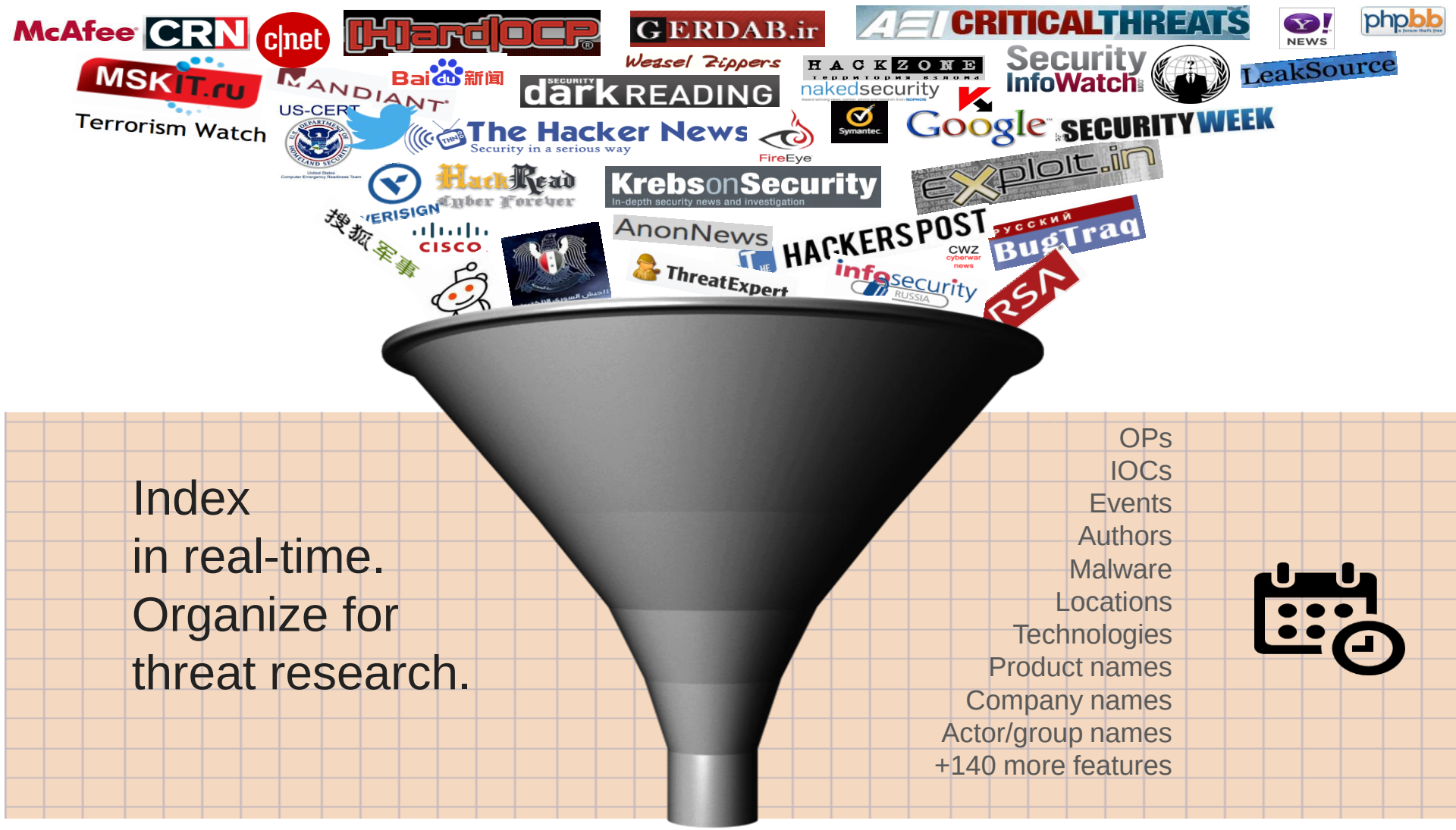
Threat Intelligence Kumite!

SANS CTI Summit 2016

Matt Kodama, VP Products

Threat Intelligence Capability Wish List

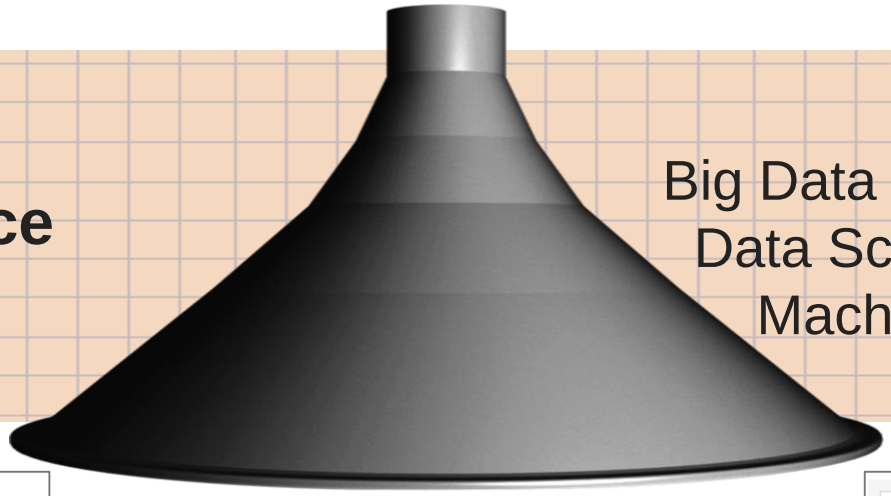
- ❑ Works for TI teams like us
- ❑ Versatile for many TI problems
- ❑ Enhances current TI methods
- ❑ Improves our defensive controls
- ❑ Empowers other security teams
- ❑ Informs strategic decisions



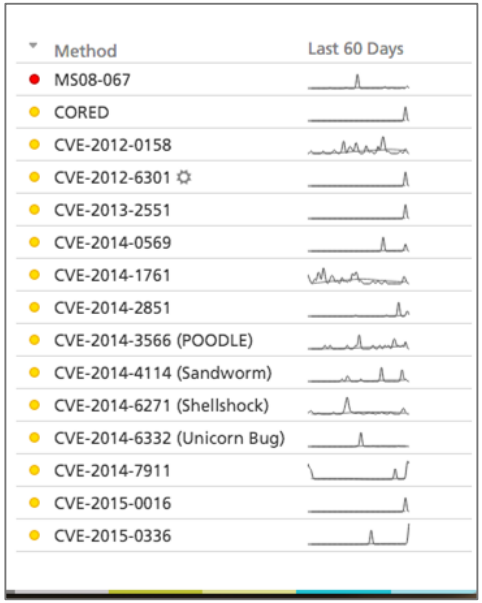
Index
in real-time.
Organize for
threat research.

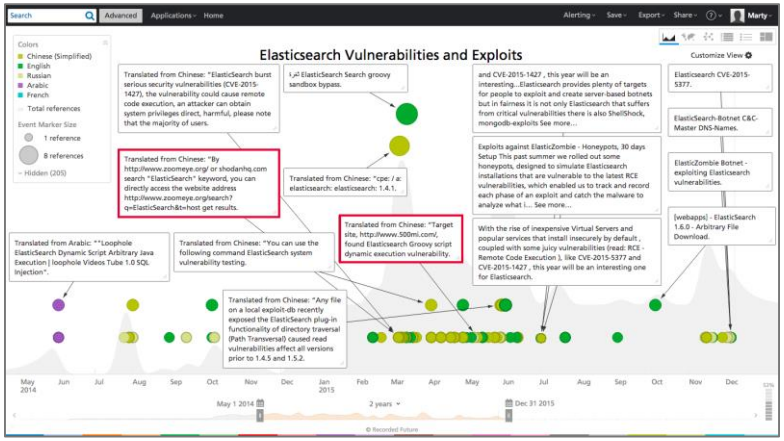
OPs
IOCs
Events
Authors
Malware
Locations
Technologies
Product names
Company names
Actor/group names
+140 more features

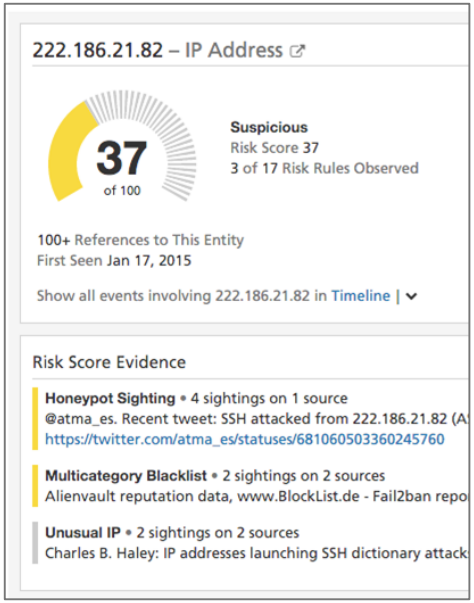
Patented
Web Intelligence
Engine



Big Data +
Data Science +
Machine Learning

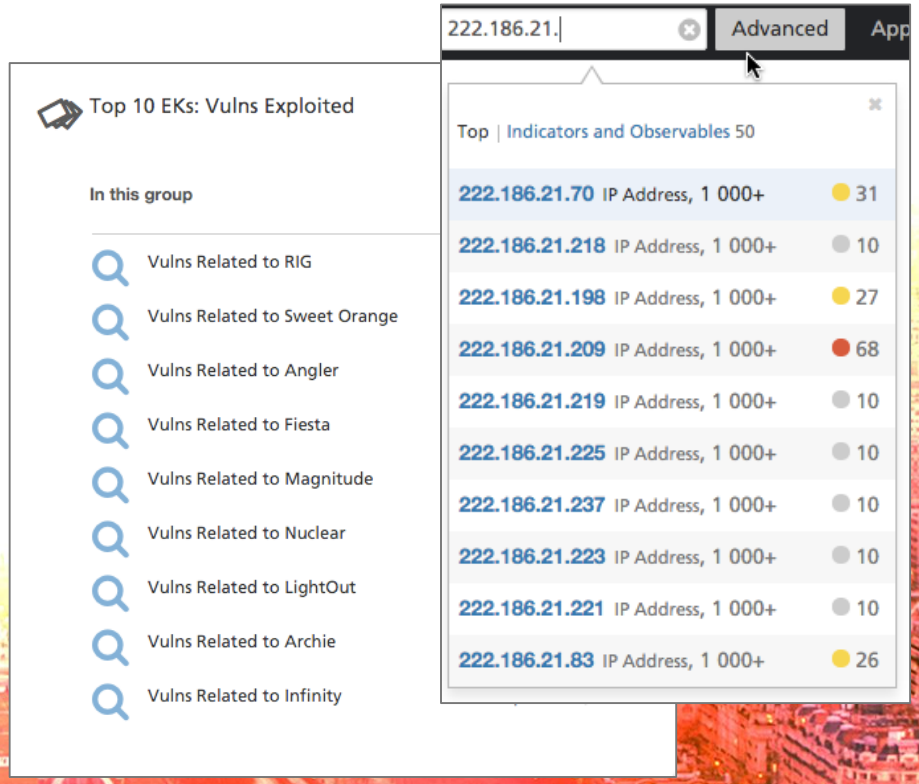






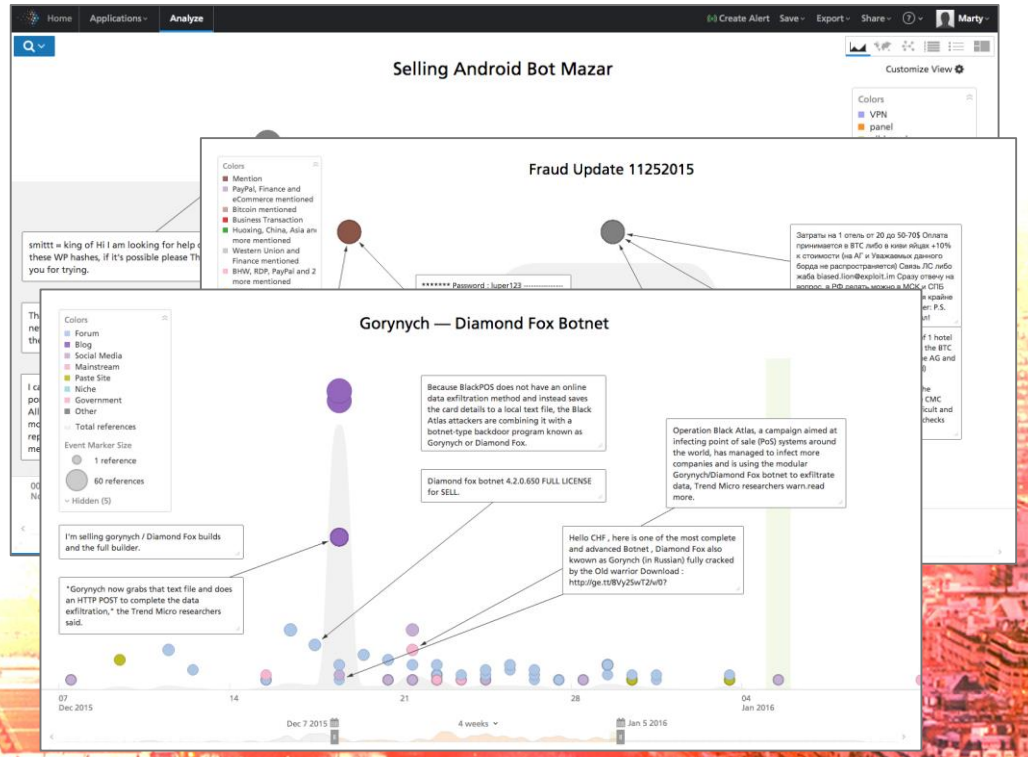
Works for Threat Intel teams like us

- Delivers value immediately
- Usable by novice analysts
- Precision targeting for ninjas
- Durable through turnover



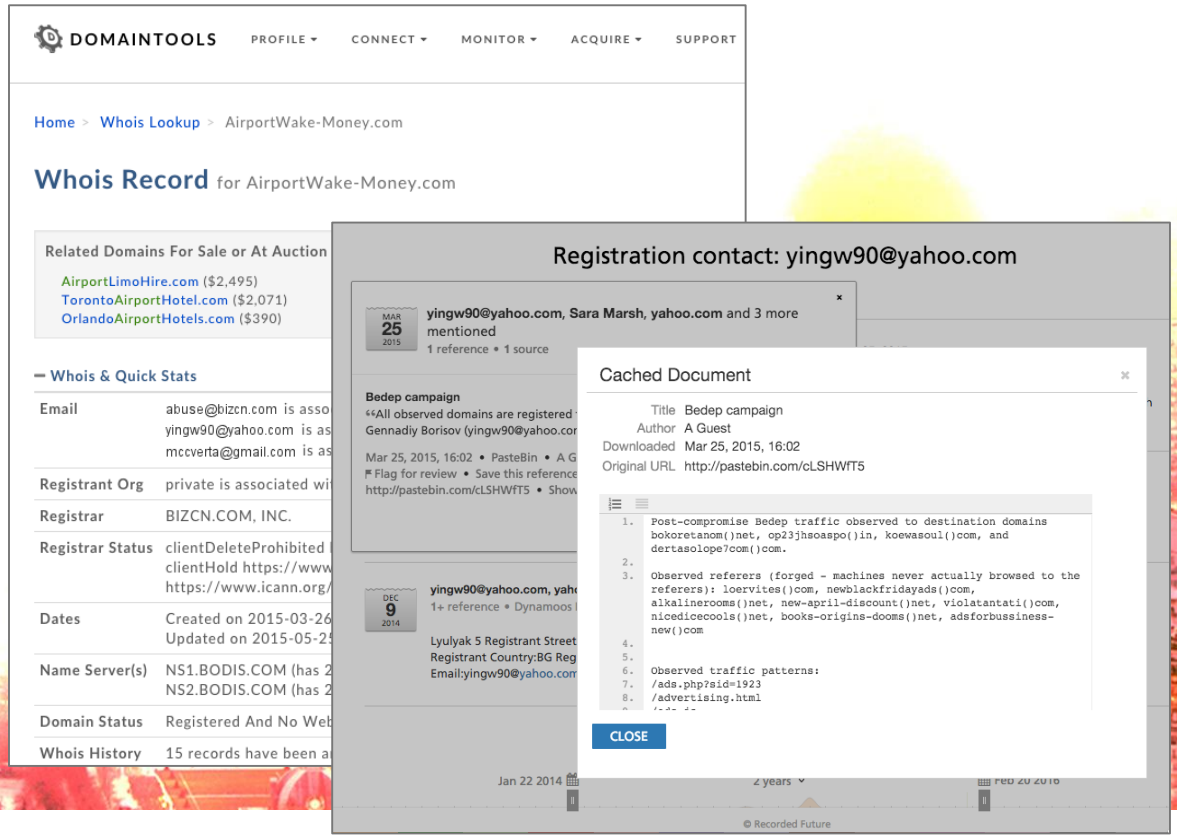
Versatile for many Threat Intel problems

- Many internal customers
- Evolving IT environment
- New vulnerabilities
- New actors and TTPs



Enhances my current Threat Intel methods

- Internal telemetry
- DHS, CERT, ISAC
- Trusted peers
- Community services

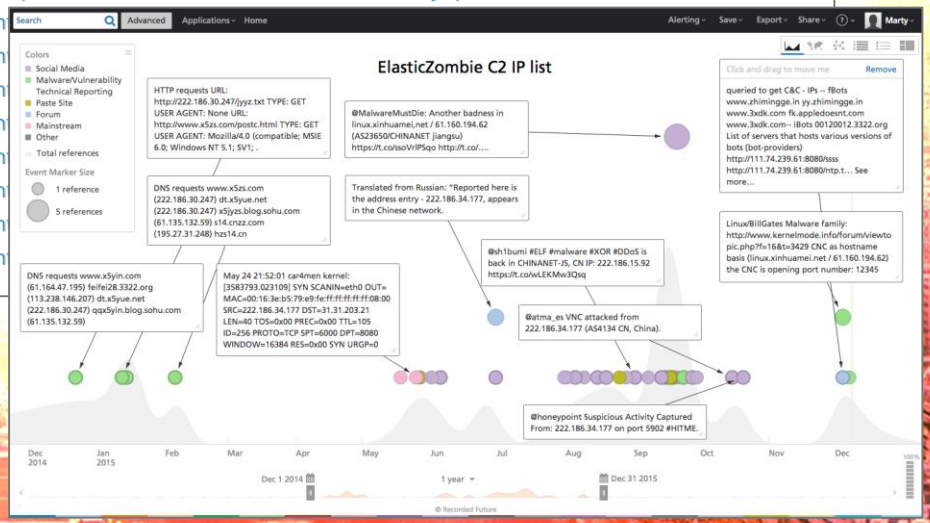


Improves our defensive controls

- Indicators to block/detect
- Higher-leverage TTPs
- Prioritize events and alarms
- Context for incident review

ElasticZombie C2 IP address results from the Recorded Future API enrichment script:

https://www.recordedfuture.com/live/sc/entity/ip:103.105.144.172
https://www.recordedfuture.com/live/sc/entity/ip:61.160.194.62
https://www.recordedfuture.com/live/sc/entity/ip:222.186.190.233
https://www.recordedfuture.com/live/sc/entity/ip:23.234.50.12
https://www.recordedfuture.com/live/sc/entity/ip:222.186.15.92

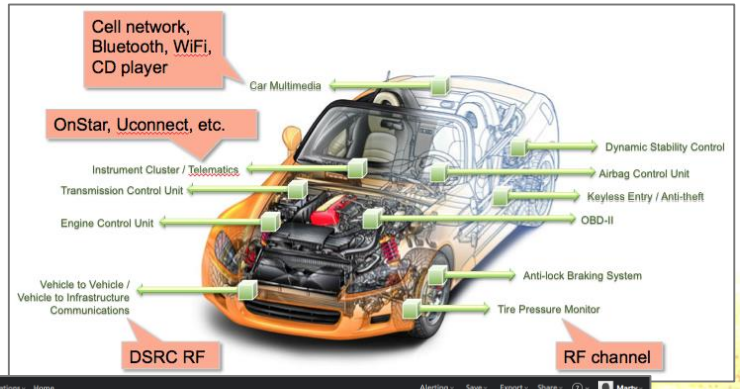


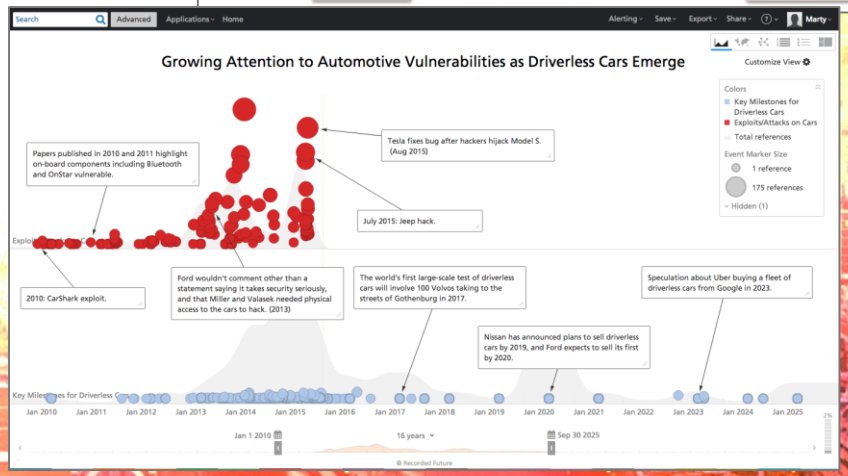
Empowers other security teams

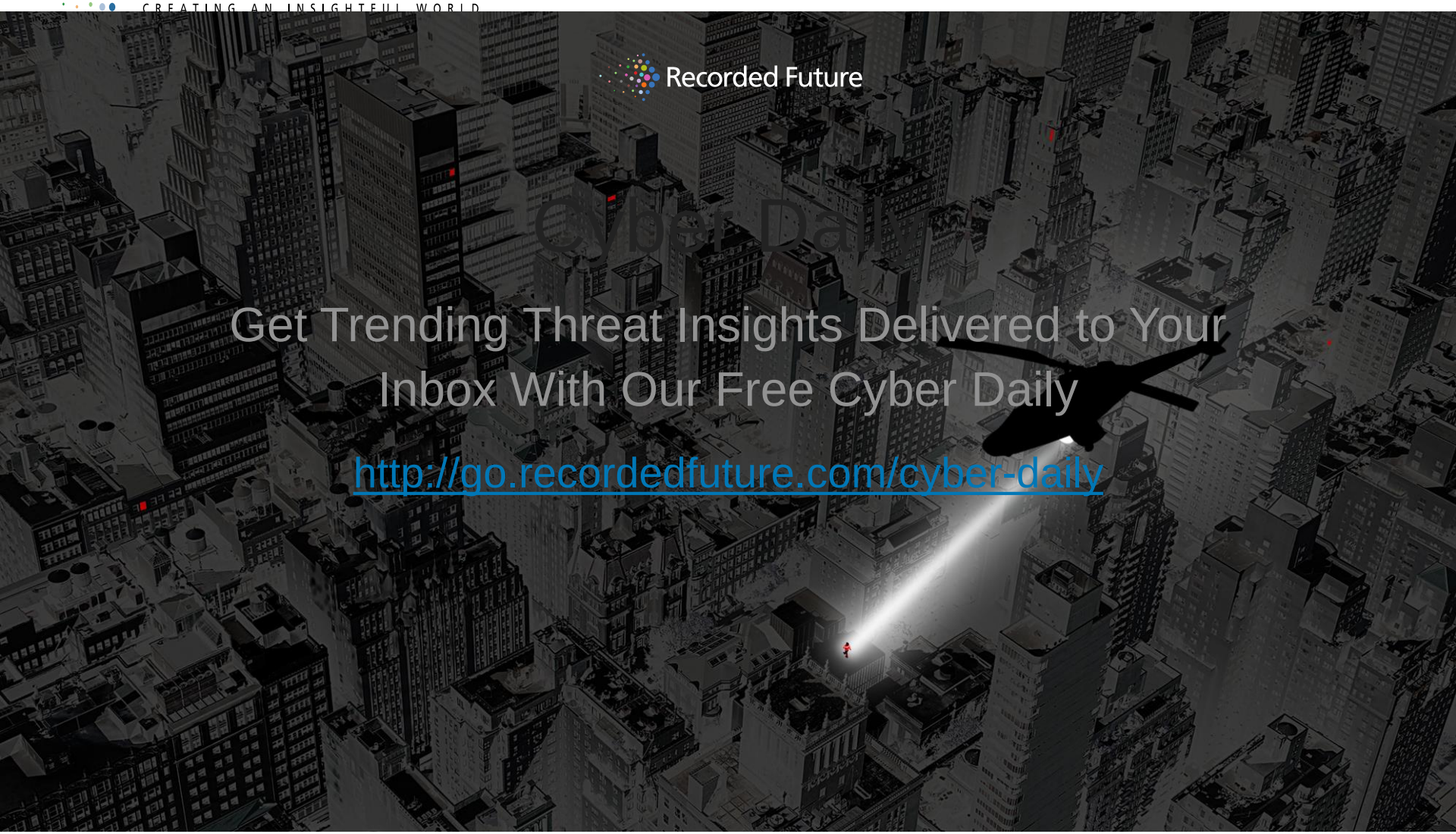
- Security policy changes
- Malcode samples to acquire
- Vulnerabilities to pen test
- Indicators for forensic scans

Informs strategic decisions

- Security architecture changes
- IT investment decisions
- Supplier due diligence
- Trends in business risk






Recorded Future
Get Trending Threat Insights Delivered to Your Inbox With Our Free Cyber Daily
http://go.recordedfuture.com/cyber-daily

SANS Cyber Threat Intelligence SUMMIT & TRAINING

There Can Be Only One!: Last CTI Vendor Standing Pitch

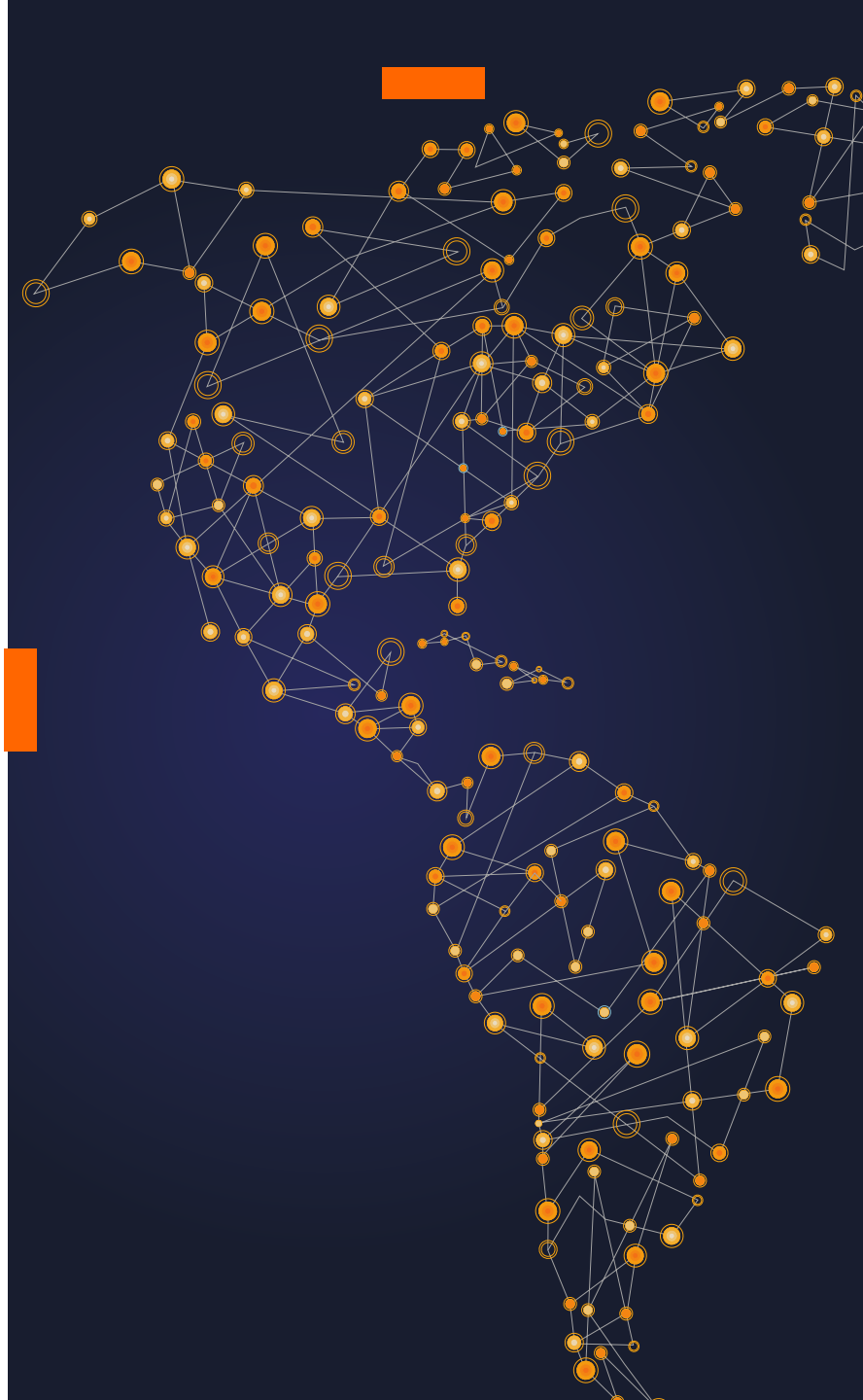
Jess Parnell, Centripetal Networks

CENTRIPETAL
NETWORKS

We Turn Intelligence Into Action™

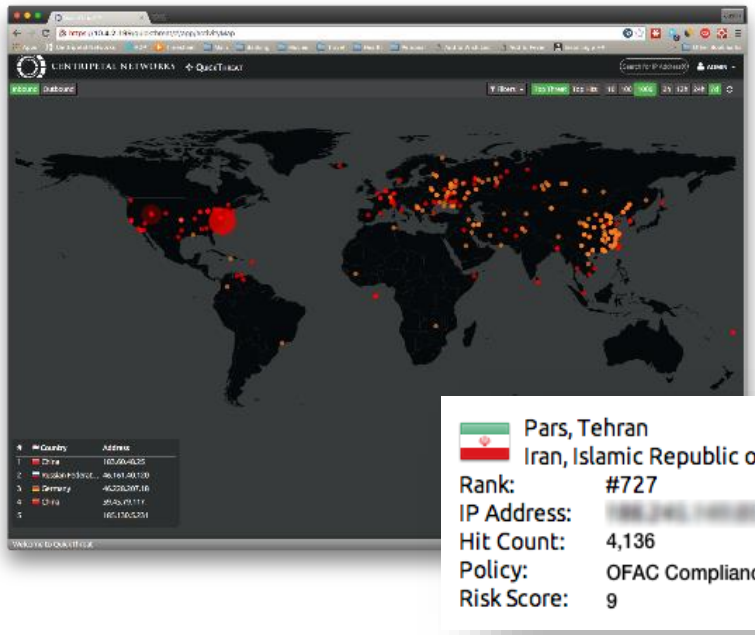
Jess Parnell

Director of Information Security



Layered Active Blocking & Logging

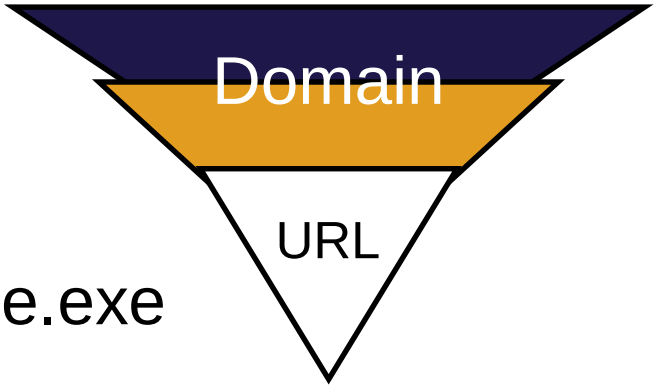
- Start with country blocking
  - Inbound drop/no log
  - Outbound resets/log
- OFAC is the easiest place to start
- ITAR & others unfriendly to US Law Enforcement



CENTRIPETAL NETWORKS

Pyramid of IOCs

- IP: 50.117.38[.]170
  - IP hosts many sites
- Domain: opm-learning[.]org
- URL: opm-learning[.]org/badfile.exe



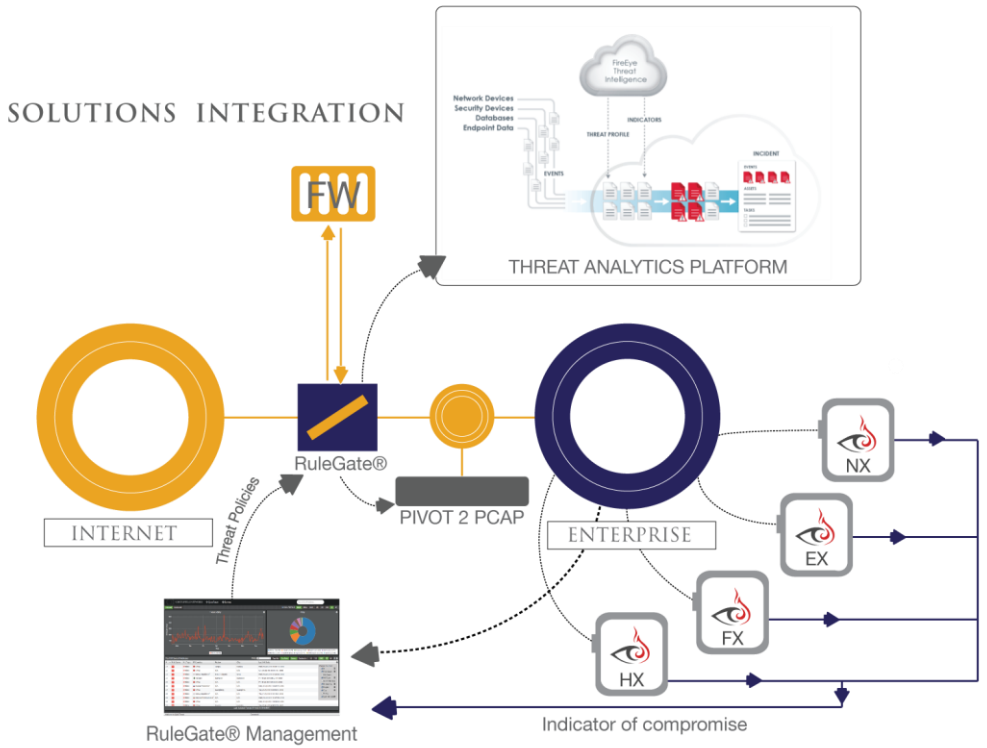
Ref: https://www.passivetotal.org/passive/opm-learning.org

Ref: https://www.threatconnect.com/opm-breach-analysis/

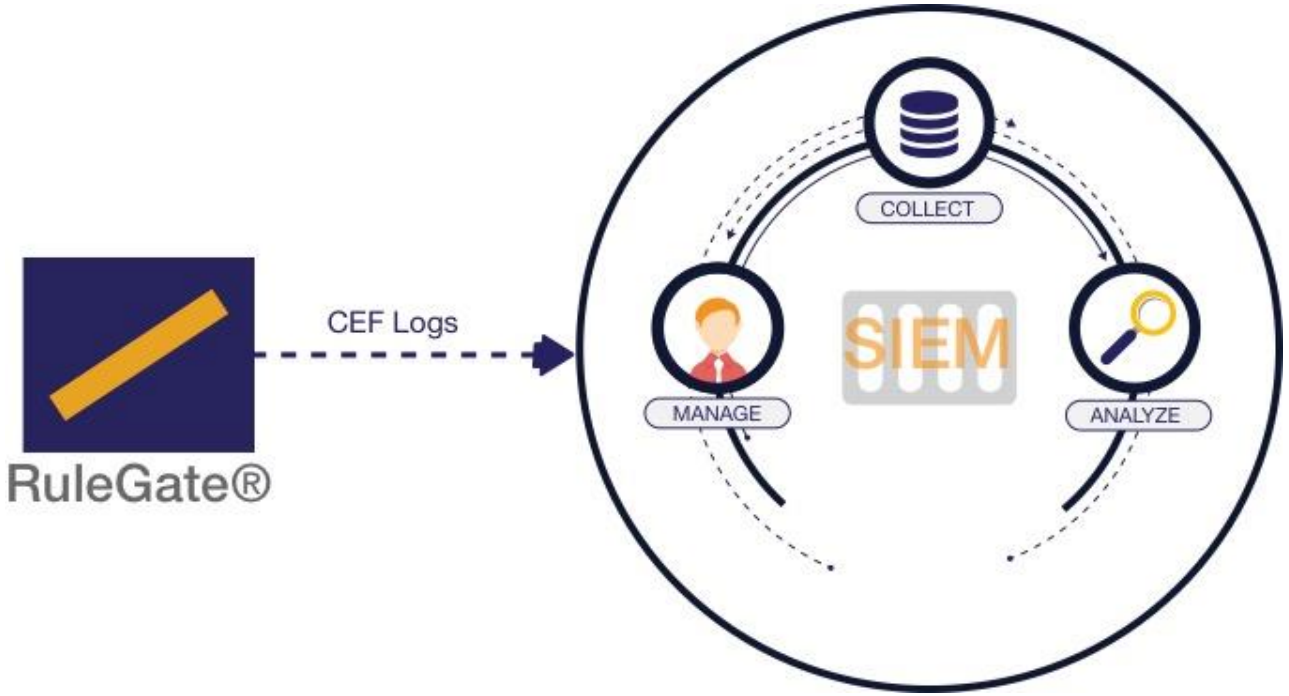
Actively Block on New Threats Discovered

- RuleGate® plugin updates IOCs from FireEye NX series malware sandbox
- Policies configured to actively block newly discovered IOCs

CENTRIPETAL NETWORKS & FireEye



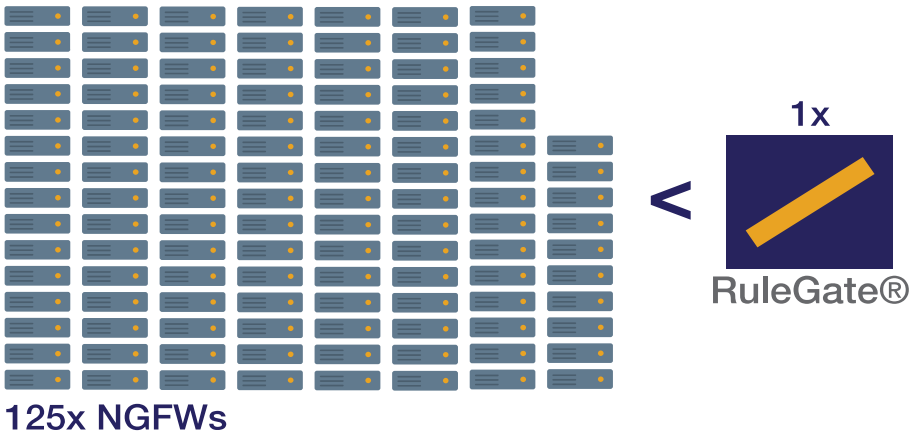
Send to SIEM: Correlate End-User



- RuleGate® sends events to the SIEM with applied threat intelligence context in real-time

Why not use my Firewall?

- GEO blocking China
  - ~ 300 Million IPs
  - ~ 8K RuleGate Rules
- GEO blocking in NGFW
  - Increased Latency
- RuleGate Performance
  - 5M+ Indicators/Rules
  - Up to 20Gbps aggregate throughput
  - < 10µS Latency



RuleGate handles 125x more indicators than the most powerful Next-Generation Firewall (NGFW) available

CENTRIPETAL NETWORKS

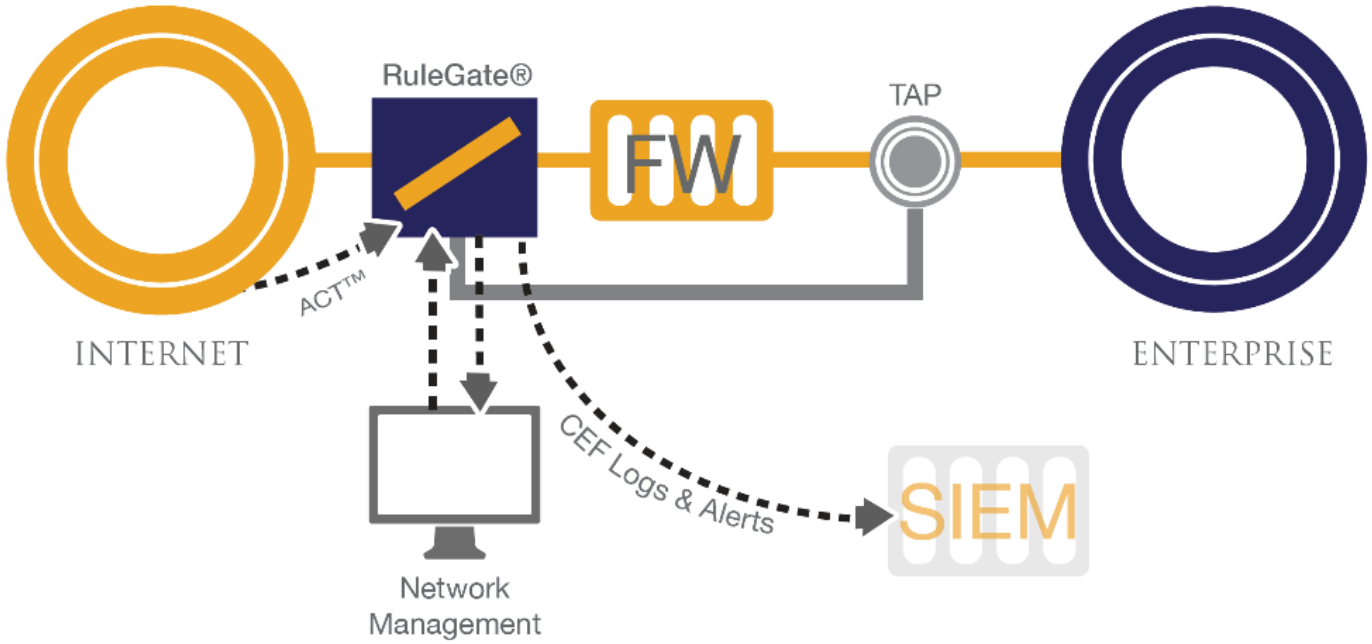
Why not use my SIEM?

- NO Active Blocking Capability
- Avg Security Team has 1-3M Indicators
  - Not feasible within current SIEM
- List-based matching difficult to manage
- ~28K Breaks SIEM

SIEM is purely for analysis, and has no Active Blocking capability

Is the RuleGate a Threat Intelligence Platform (TIP)?

- NO it's Threat Enforcement
- In-line deployment for Active Blocking



CENTRIPETAL NETWORKS

Indicators from Partners you Trust

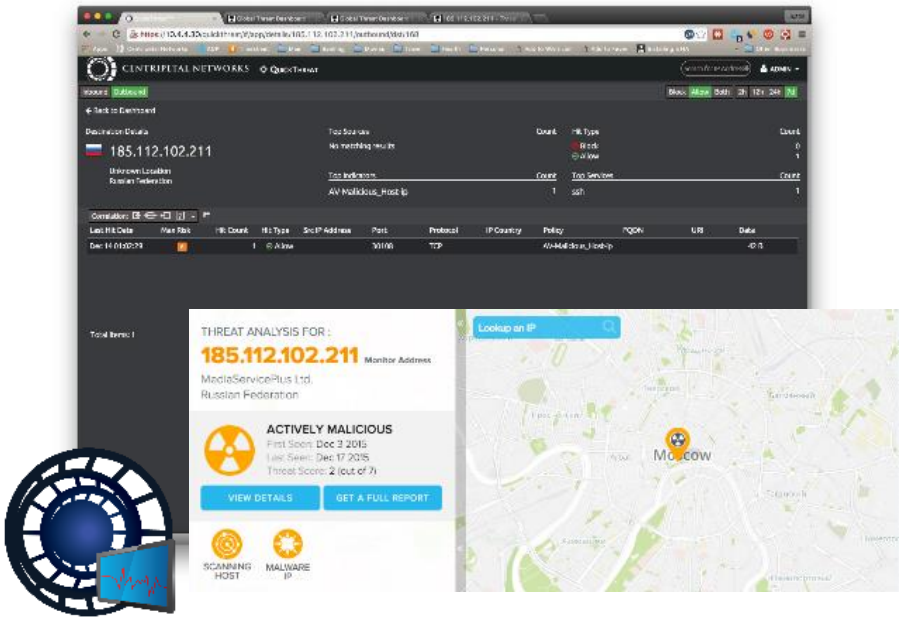
- Open Intelligence Platform
- Open Source & Commercial
- Fully Integrated: Automatic Updates & Application
- Source Multi-Attribution
- Technology Integrations
  - Malware Detection
  - Threat Intelligence Platforms
  - SIEM Tools

(not an exhaustive list of Centripetal intelligence sources)

CENTRIPETAL NETWORKS

You will NOT be overwhelmed with Actionable Intelligence

- Pivot to Source
- Targeted Packet Capture
- Instant Data Correlation
- Enterprise Specific Risk Models
- Geographic Visualizations

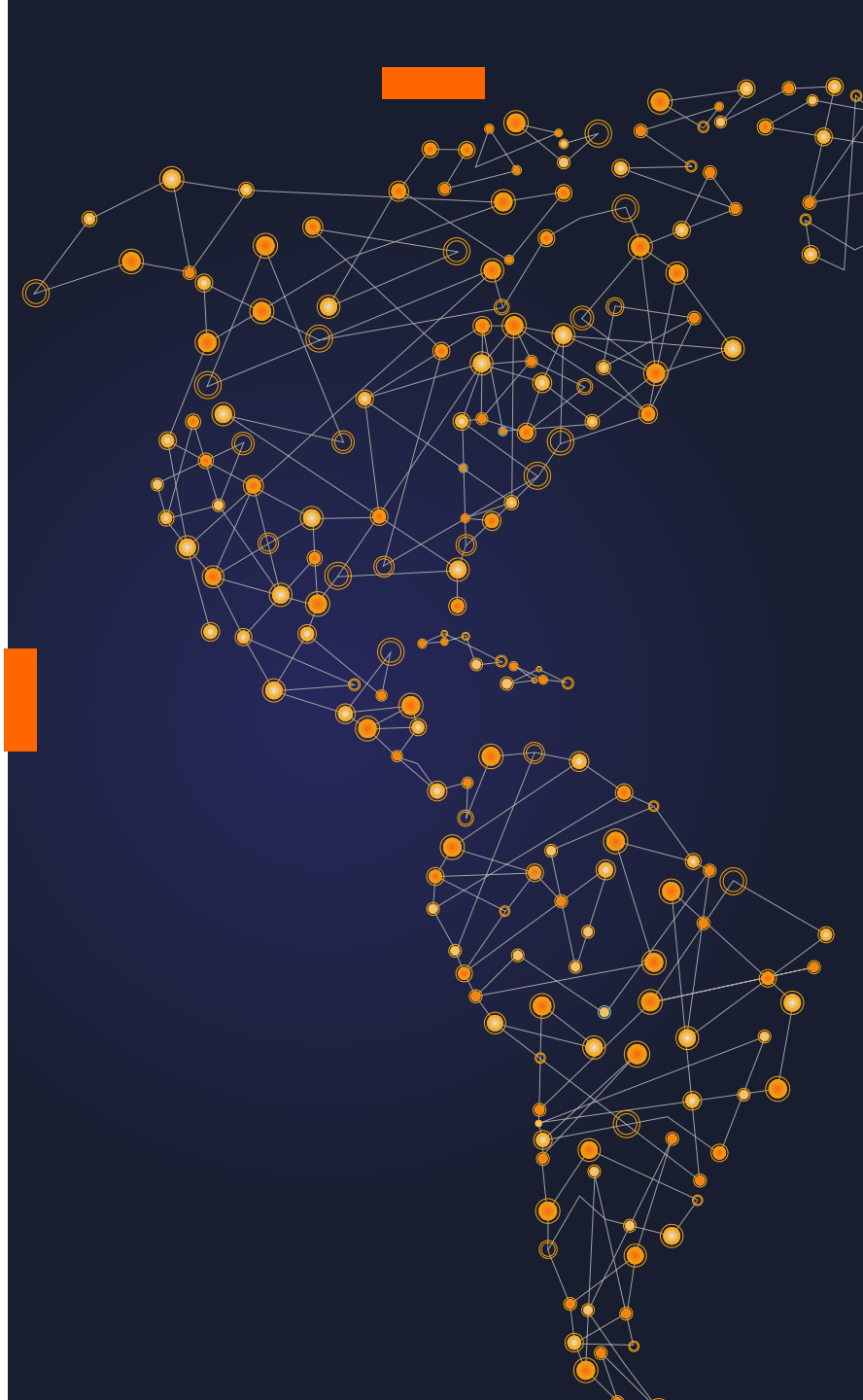


QuickThreat® - Pivot to Source

CENTRIPETAL NETWORKS

CENTRIPETAL
NETWORKS

Thank You



SANS Cyber Threat Intelligence SUMMIT & TRAINING

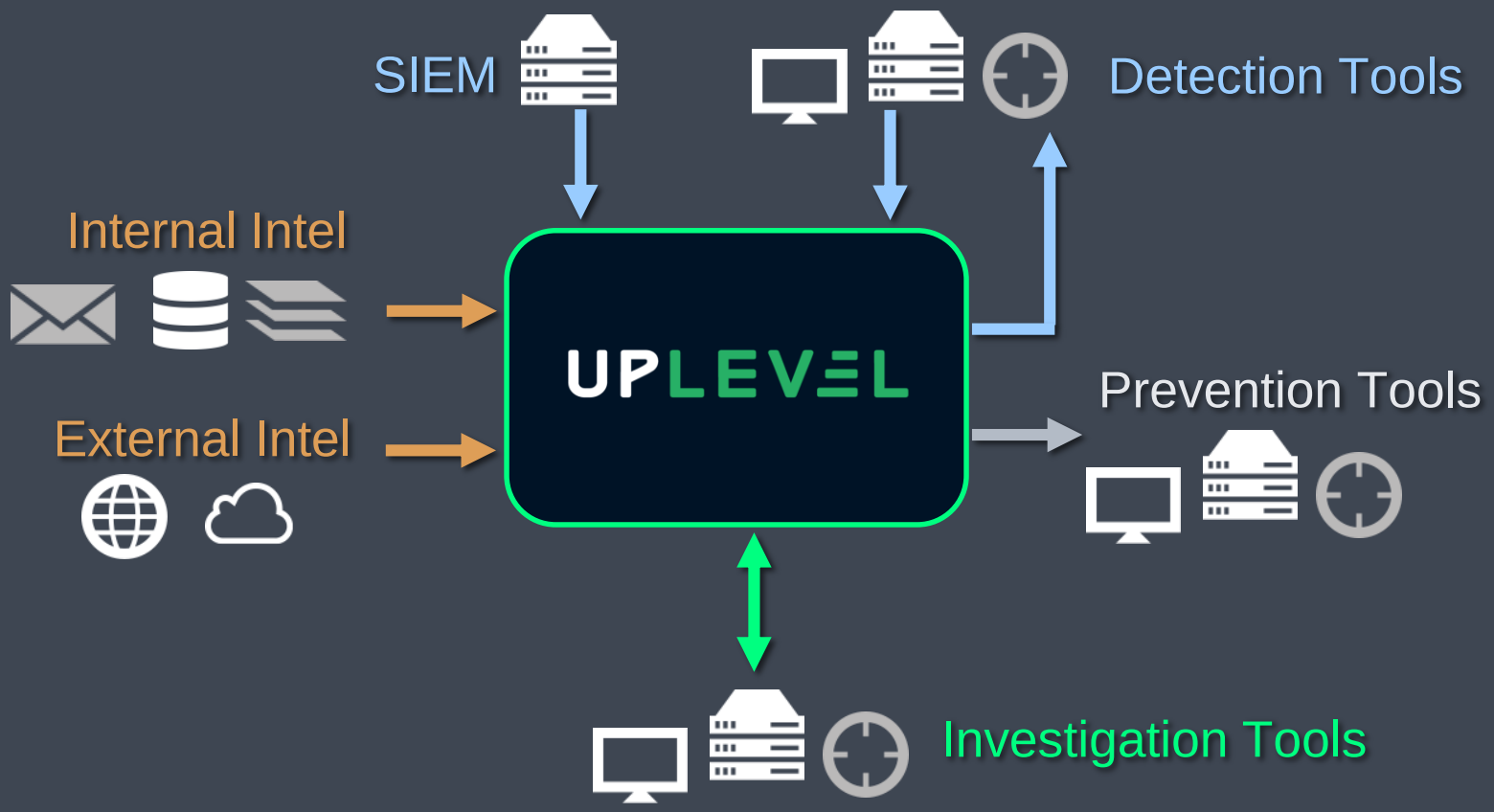
There Can Be Only One!: Last CTI Vendor Standing Pitch

Roselle Safran, UpLevel Security

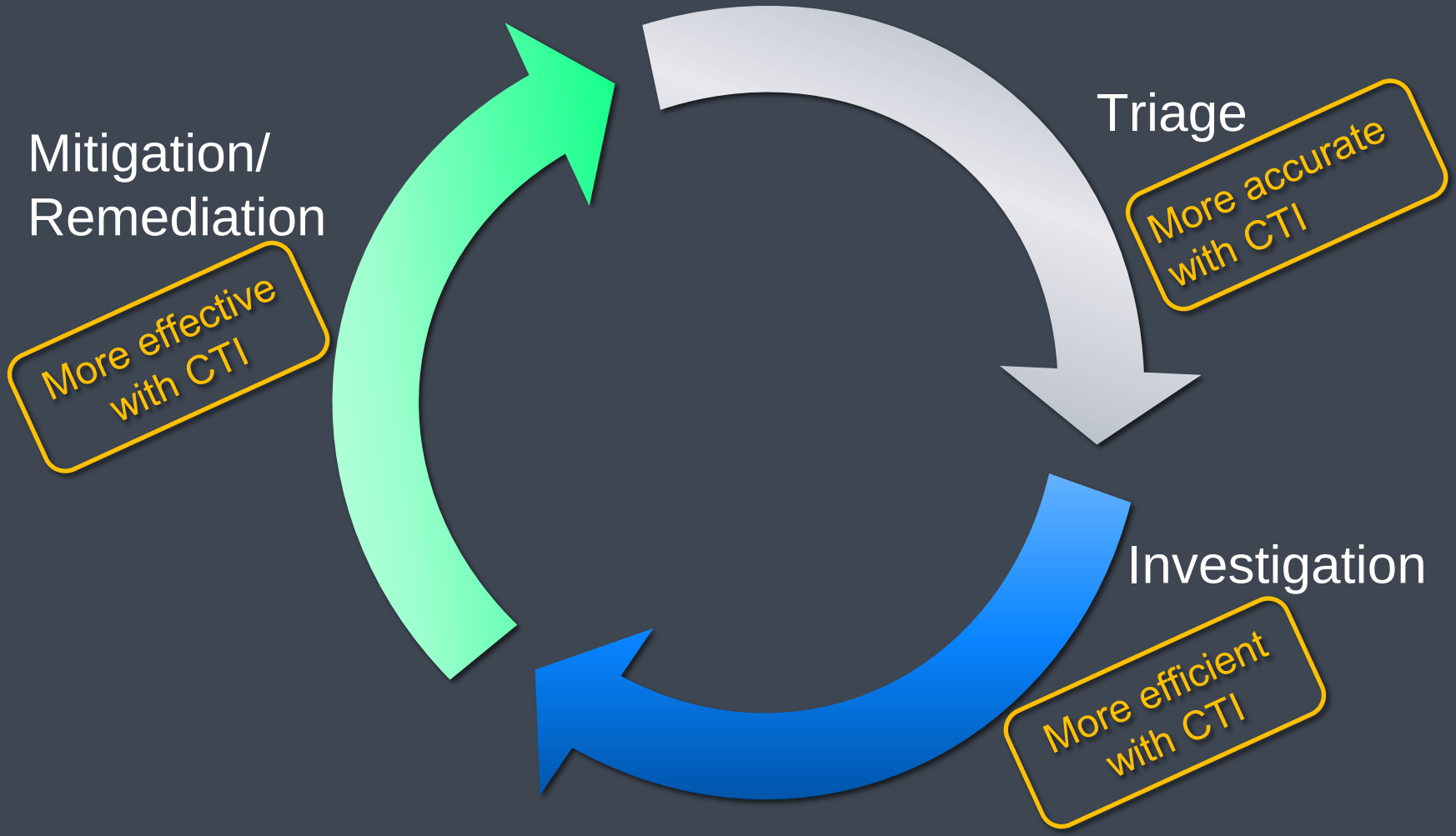
www.uplevelsecurity.com

@uplevelsecurity

What is Uplevel?
Intelligence-based
Incident Response Platform



Incident Response Lifecycle Needs CTI at Every Stage



Why is Uplevel Awesome?

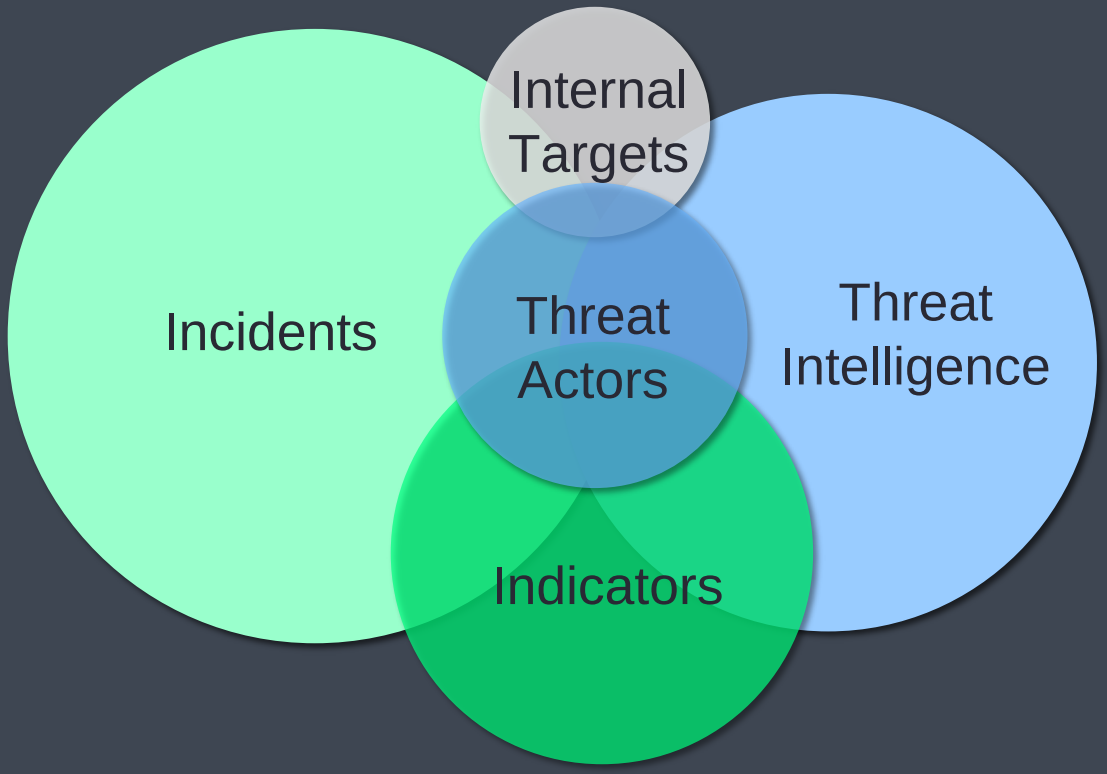
Top 5 Reasons

Reason #5:
Uplevel is Built By Practitioners For Practitioners

Cybersecurity Operational Expertise

Cybersecurity Data Analysis Expertise

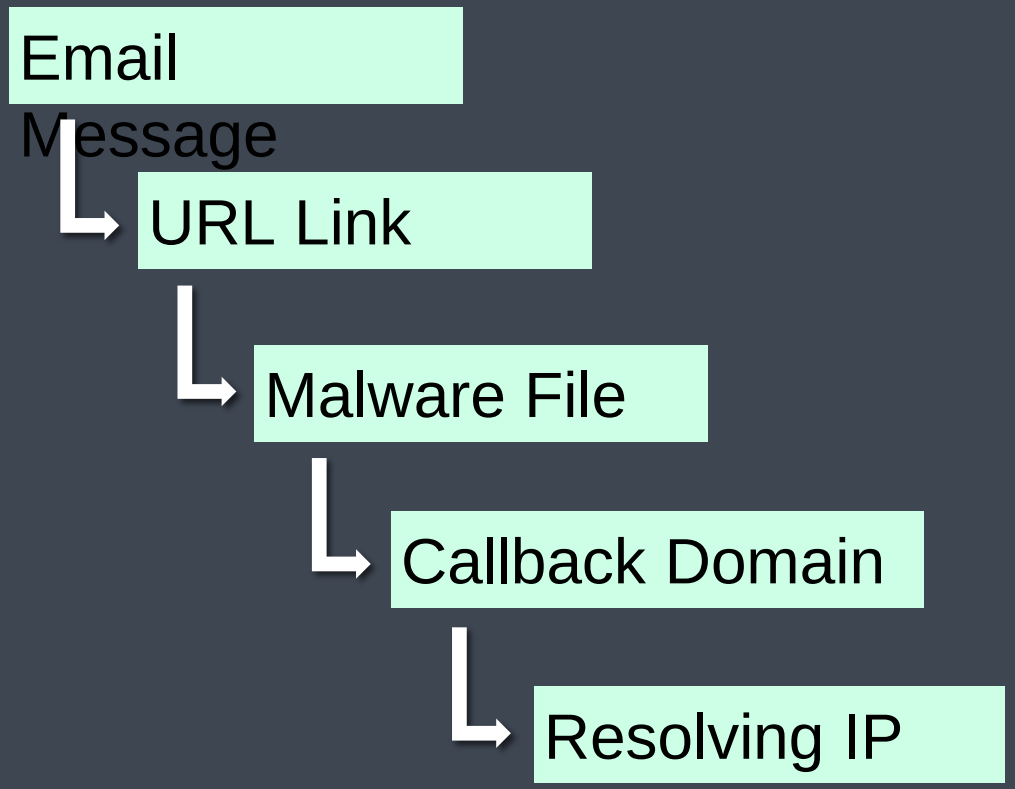
Reason #4:
Uplevel Integrates Incident Management and Threat Intel Management into One System



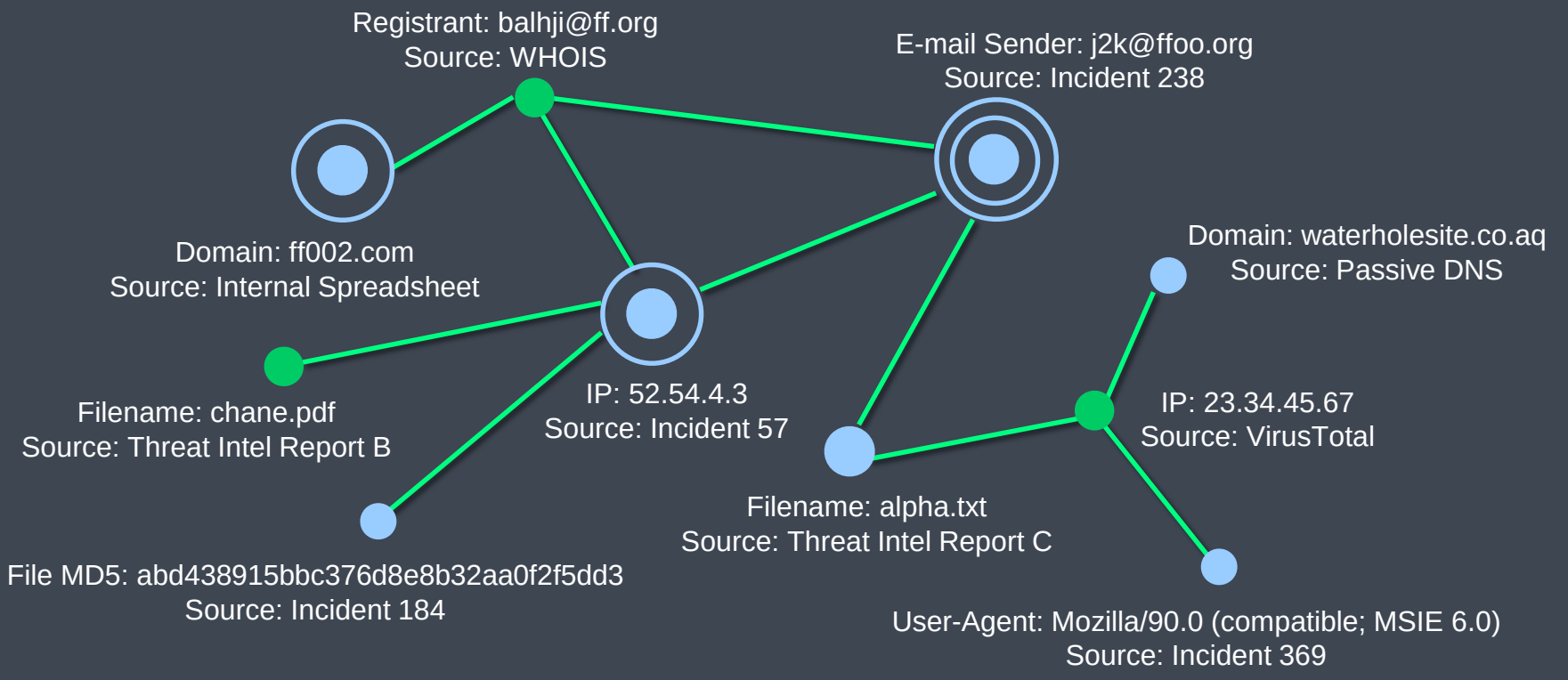
- Collaborative
- Comprehensive
- Consistent

Reason #3:
Uplevel Preserves Context

- Sources
- Relationships
- Confidence Levels



Reason #2:
Uplevel Provides Graph Intelligence



Reason #1:
Uplevel Automates Tasks So Analysts Can Focus on the Interesting and Challenging Work

- Workflow orchestration
  - Integrations with a variety of tools
  - Enterprise-specific processes
- Data enrichment
  - Threat intelligence feeds
  - Open source information

UPLEVEL

roselle@uplevelsecurity.com
646-470-4206

www.uplevelsecurity.com
@uplevelsecurity