

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

DomainTools Iris

Welcome to DomainTools Iris. From here, you can open an existing investigation, create a new one, or simply begin searching.



Note: input your terms to start a new investigation

[Show All Investigations](#)

pdfpump.net

Pivot Engine Stats

View: Default [.CSV](#)

Advanced Back Filters: pdfpump.net

Domain Risk Score Email

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

Page 1 of 1 (1 record total)

Domain Profile Whois History Hosting History

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

Nov 10, 2015 (2 months ago)

PDFPump.net Free online pdf search engine

PDF PUMP One of the best file search engine

Sample: New age book 2013.0 Abrammos Today Over: 125,352 Pdf Files

PDFPump.net was created to support Internet users with various sorts of literature - fiction, scientific works, tutorials, instructions, guides and many other e-books that can download any user who adores reading. We can provide all book lovers with all these files on the best terms.

We understand how valuable reading is. A book is one of the first means of passing knowledge and experiencing the world. It is a great source of inspiration and would always have great power. Nevertheless, within time, some information can be lost or passed in another form, depending on personal opinion and understanding of the matter of the narrator. As the printed word had been invented, such things were not possible.

Thanks to a simple paper book many generations received a tremendous possibility to learn the history, thoughts and development of their ancestors, and consequently, this had a positive reflection for future generations. It is actually difficult to determine how important the power of book is. Because of such reasons we created PDFPump.net. We wish to provide everyone with a possibility of reading and developing him- or herself. Reading develops not only our language and increases vocabulary; it enhances our thinking and helps to express our feelings and thoughts in beautiful and understandable way.

With the rapid development of modern technologies, paper books have reached a new level - digital format, and with this purpose we have initiated our online fellowship. We want to provide our clients with all sorts of literature. E-books are more affordable and it is easier to find them, especially with the help of our site.

Just remember how difficult it can be at times to find the required book. There is probably no real book lover who had not faced problems with purchasing a book, either online or in real life. It is really disappointing to be annoyed when you run all over the city through all existing book stores and libraries just to find out that the needed literature is not available. Or, perhaps, you have found it, but its cost is too expensive. Using our services, you can easily avoid all those problems. Our book storage has tremendous stores of any literature direction. On this site you will find almost any book you need. You can search for it by title, author, genre, year of publication, etc. And the most important thing is that you will definitely find what is required. Our library storage updates every 24 hours, so we have a continuous live streaming of all novelties in the world of literature.

We download about 10,000 of new files and can provide our users with all that is needed. Each document is converted into very popular and dependable format - PDF. This is a very practical digital format of e-books and it can be opened and viewed by special programs, which are usually installed on personal computers.

Notwithstanding, this is not all, inasmuch as we still have a lot to offer our customers. Except wide range of various literature, you can sufficiently save your money and time. Our searching system acts very quickly and you will get the results of the desired materials in the shortest terms. Just type in the title or the author and within a blink of an eye you will receive all possible exemplars of your request. But this is not all. We also save your time when you need to download a book. This process also runs pretty fast, because the size of all our files is diminutive. Accessing our documents will not require much space on your device.

Another great advantage of our fellowship is our price policy. All our services are free. You have no need of paying for anything on PDFPump.net. Such advantage is really worthy in comparison of high prices for books at shops. No matter what you wish, some manuals or tutorials, you can get it here chargeless. You may be also sure that your device would be secured from dangerous viruses. Our advanced anti-virus system

Search History

Last updated: a few seconds ago

PDFPump.net

With the rapid development of modern technologies, paper books have reached a new level - digital format, and with this purpose we have initiated our online fellowship. We want to provide our clients with all sorts of literature. E-books are more affordable and it is easier to find them, especially with the help of our site.

Just remember how difficult it can be at times to find the required book. There is probably no real book lover who had not faced problems with purchasing a book, either online or in real life. It is really disappointing to be annoyed when you run all over the city through all existing book stores and libraries just to find out that the needed literature is not available. Or, perhaps, you have found it, but its cost is too expensive. Using our services, you can easily avoid all those problems. Our book storage has tremendous stores of any literature direction. On this site you will find almost any book you need. You can search for it by title, author, genre, year of publication, etc. And the most important thing is that you will definitely find what is required. Our library storage updates every 24 hours, so we have a continuous live streaming of all novelties in the world of literature.

We download about 10,000 of new files and can provide our users with all that is needed. Each document is converted into very popular and dependable format - PDF. This is a very practical digital format of e-books and it can be opened and viewed by special programs, which are usually installed on personal computers.

Notwithstanding, this is not all, inasmuch as we still have a lot to offer our customers. Except wide range of various literature, you can sufficiently save your money and time. Our searching system acts very quickly and you will get the results of the desired materials in the shortest terms. Just type in the title or the author and within a blink of an eye you will receive all possible exemplars of your request. But this is not all. We also save your time when you need to download a book. This process also runs pretty fast, because the size of all our files is diminutive. Accessing our documents will not require much space on your device.

Another great advantage of our fellowship is our price policy. All our services are free. You have no need of paying for anything on PDFPump.net. Such advantage is really worthy in comparison of high prices for books at shops. No matter what you wish, some manuals or tutorials, you can get it here chargeless. You may be also sure that your device would be secured from dangerous viruses. Our advanced anti-virus system

Pivot Engine Stats

View: Default

 [.CSV](#)

Domain	Risk Score	Email	Email Domain						
pdfpump.net	20.42	<table><tr><td>Address</td><td>Type(s)</td></tr><tr><td>contact@privacyprotect.org</td><td>Admin, Registrant, Technical</td></tr><tr><td>abuse-contact@publicdomainregistry.com</td><td>Whois</td></tr></table>	Address	Type(s)	contact@privacyprotect.org	Admin, Registrant, Technical	abuse-contact@publicdomainregistry.com	Whois	privacyprotect.org publicdomainregistry.com
Address	Type(s)								
contact@privacyprotect.org	Admin, Registrant, Technical								
abuse-contact@publicdomainregistry.com	Whois								



Pivot Engine Stats

View: Default

.CSV

Domain	Registrar Status	Create Date	Expiration Date	Name Server	IP										
pdfpump.net	.COM clientTransferProhibited	2015-10-15 <i>(97 days old)</i>	2016-10-15 <i>(in 9 months)</i>	<table><tr><td>Hostname</td><td>IP Information</td></tr><tr><td>ns1.pdfpump.net</td><td>199.80.54.171</td></tr><tr><td>ns2.pdfpump.net</td><td>199.80.54.183</td></tr></table>	Hostname	IP Information	ns1.pdfpump.net	199.80.54.171	ns2.pdfpump.net	199.80.54.183	<table><tr><td>IP</td><td>ISP</td></tr><tr><td>199.80.54.171</td><td>W2</td></tr></table>	IP	ISP	199.80.54.171	W2
Hostname	IP Information														
ns1.pdfpump.net	199.80.54.171														
ns2.pdfpump.net	199.80.54.183														
IP	ISP														
199.80.54.171	W2														



Pivot Engine Stats

View: Default

[.CSV](#)

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

Hostname	IP Information
ns1.pdfpump.net	199.80.54.171
ns2.pdfpump.net	

Filters X

[Narrow Search](#) [Expand Search](#) [New Search](#) [Exclude](#)

IP Tools

[IP Profile](#) [Ping](#) [Traceroute](#) [PTR](#)

~ 3 domains share this value.





Pivot Engine

Stats

View: Default

.CSV

Domain	Risk Score	Email	Email Domains						
pdfpump.com	20.42	<table><tr><td>Address</td><td>Type(s)</td></tr><tr><td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr><tr><td>abuse-contact@publicdomainregistry.com</td><td>Whois</td></tr></table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	abuse-contact@publicdomainregistry.com	Whois	kvaz.com publicdomain
Address	Type(s)								
link@kvaz.com	Admin, Registrant, Technical								
abuse-contact@publicdomainregistry.com	Whois								
pdfpump.net	20.42	<table><tr><td>Address</td><td>Type(s)</td></tr><tr><td>contact@privacyprotect.org</td><td>Admin, Registrant, Technical</td></tr><tr><td>abuse-contact@publicdomainregistry.com</td><td>Whois</td></tr></table>	Address	Type(s)	contact@privacyprotect.org	Admin, Registrant, Technical	abuse-contact@publicdomainregistry.com	Whois	privacyprotect publicdomain
Address	Type(s)								
contact@privacyprotect.org	Admin, Registrant, Technical								
abuse-contact@publicdomainregistry.com	Whois								
pdfpump.org	16.67	<table><tr><td>Address</td><td>Type(s)</td></tr><tr><td>contact@privacyprotect.org</td><td>Admin, Registrant, Technical</td></tr></table>	Address	Type(s)	contact@privacyprotect.org	Admin, Registrant, Technical	privacyprotect		
Address	Type(s)								
contact@privacyprotect.org	Admin, Registrant, Technical								





Pivot Engine

Stats



View: Default

.CSV



Domain	Risk Score	Email	Email Domains
--------	------------	-------	---------------

pdfpump.com	20.42	<table><thead><tr><th>Address</th><th>Type(s)</th></tr></thead><tbody><tr><td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr></tbody></table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	kvaz.com publicdomain
Address	Type(s)						
link@kvaz.com	Admin, Registrant, Technical						

pdfpump.net	20	<table><thead><tr><th>Address</th><th>Type(s)</th></tr></thead><tbody><tr><td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr></tbody></table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	privacyprotect publicdomain
Address	Type(s)						
link@kvaz.com	Admin, Registrant, Technical						

pdfpump.org	16	<table><thead><tr><th>Address</th><th>Type(s)</th></tr></thead><tbody><tr><td>contact@privacyprotect.org</td><td>Admin, Registrant, Technical</td></tr></tbody></table>	Address	Type(s)	contact@privacyprotect.org	Admin, Registrant, Technical	privacyprotect
Address	Type(s)						
contact@privacyprotect.org	Admin, Registrant, Technical						

Filters

[Narrow Search](#)[Expand Search](#)[New Search](#)[Exclude](#)

~ 380 domains share this value.



DOMAINTOOLS


[Pivot Engine](#) [Stats](#)
View: Default ▼[.CSV](#)

Page 1 of 1 (130 records total) sorted by Risk Score Descending

< >

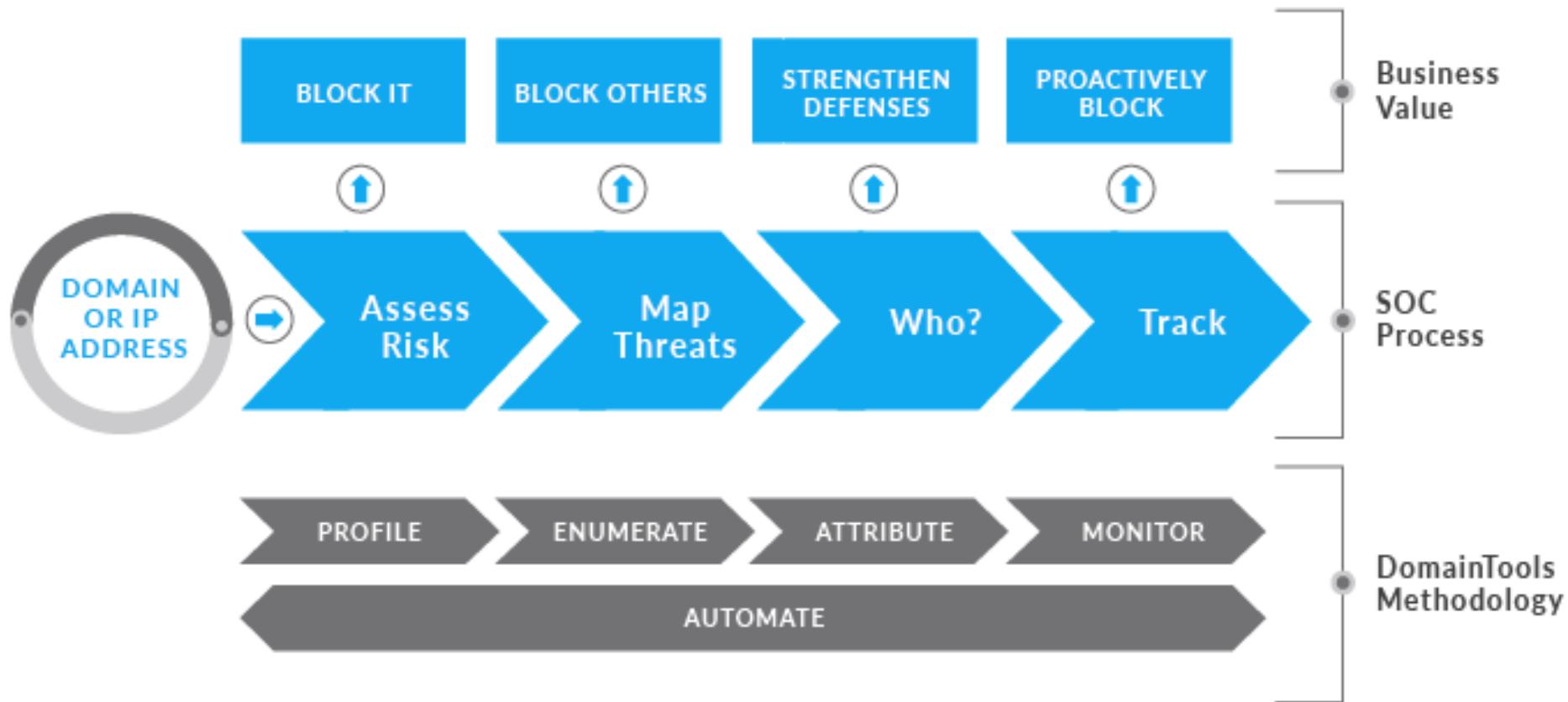
Domain	Risk Score	Email	Email Domain	Contact Information														
hasanweb.org	100	<table border="1"> <tr> <th>Address</th><th>Type(s)</th></tr> <tr> <td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr> <tr> <td>jp-info@123server.jp</td><td>DNS/SOA</td></tr> </table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	jp-info@123server.jp	DNS/SOA	123server.jp kvaz.com	<table border="1"> <tr> <th>Name</th><th>Organization</th><th>Address</th></tr> <tr> <td>Aleksej Kocyubenko</td><td></td><td>Druzhba Schastye, UA</td></tr> </table>	Name	Organization	Address	Aleksej Kocyubenko		Druzhba Schastye, UA		
Address	Type(s)																	
link@kvaz.com	Admin, Registrant, Technical																	
jp-info@123server.jp	DNS/SOA																	
Name	Organization	Address																
Aleksej Kocyubenko		Druzhba Schastye, UA																
lafrenierre.net	54.04	<table border="1"> <tr> <th>Address</th><th>Type(s)</th></tr> <tr> <td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr> <tr> <td>hostmaster@domainit.com</td><td>DNS/SOA</td></tr> <tr> <td>abuse@godaddy.com</td><td>Whois</td></tr> </table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	hostmaster@domainit.com	DNS/SOA	abuse@godaddy.com	Whois	domainit.com godaddy.com kvaz.com	<table border="1"> <tr> <th>Name</th><th>Organization</th><th>Address</th></tr> <tr> <td>Aleksey Kotsyubenko</td><td></td><td>kv. Energia Schastye, UA</td></tr> </table>	Name	Organization	Address	Aleksey Kotsyubenko		kv. Energia Schastye, UA
Address	Type(s)																	
link@kvaz.com	Admin, Registrant, Technical																	
hostmaster@domainit.com	DNS/SOA																	
abuse@godaddy.com	Whois																	
Name	Organization	Address																
Aleksey Kotsyubenko		kv. Energia Schastye, UA																
rnvsu.com	54.04	<table border="1"> <tr> <th>Address</th><th>Type(s)</th></tr> <tr> <td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr> <tr> <td>webmaster@hastydns.com</td><td>SSL</td></tr> <tr> <td>abuse@godaddy.com</td><td>Whois</td></tr> </table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	webmaster@hastydns.com	SSL	abuse@godaddy.com	Whois	godaddy.com hastydns.com kvaz.com	<table border="1"> <tr> <th>Name</th><th>Organization</th><th>Address</th></tr> <tr> <td>Aleksey Kotsyubenko</td><td></td><td>kv. Energia Schastye, UA</td></tr> </table>	Name	Organization	Address	Aleksey Kotsyubenko		kv. Energia Schastye, UA
Address	Type(s)																	
link@kvaz.com	Admin, Registrant, Technical																	
webmaster@hastydns.com	SSL																	
abuse@godaddy.com	Whois																	
Name	Organization	Address																
Aleksey Kotsyubenko		kv. Energia Schastye, UA																
denniswolfe.com	54.04	<table border="1"> <tr> <th>Address</th><th>Type(s)</th></tr> <tr> <td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr> <tr> <td>abuse@opticaljungle.com</td><td>DNS/SOA</td></tr> <tr> <td>abuse@godaddy.com</td><td>Whois</td></tr> </table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	abuse@opticaljungle.com	DNS/SOA	abuse@godaddy.com	Whois	godaddy.com kvaz.com opticaljungle.com	<table border="1"> <tr> <th>Name</th><th>Organization</th><th>Address</th></tr> <tr> <td>Aleksey Kotsyubenko</td><td></td><td>kv. Energia Schastye, UA</td></tr> </table>	Name	Organization	Address	Aleksey Kotsyubenko		kv. Energia Schastye, UA
Address	Type(s)																	
link@kvaz.com	Admin, Registrant, Technical																	
abuse@opticaljungle.com	DNS/SOA																	
abuse@godaddy.com	Whois																	
Name	Organization	Address																
Aleksey Kotsyubenko		kv. Energia Schastye, UA																
seljo.org	54.04	<table border="1"> <tr> <th>Address</th><th>Type(s)</th></tr> <tr> <td>link@kvaz.com</td><td>Admin, Registrant, Technical</td></tr> <tr> <td>akcus@bih.net.ba</td><td>DNS/SOA</td></tr> <tr> <td>info@parallels.com</td><td>ccI</td></tr> </table>	Address	Type(s)	link@kvaz.com	Admin, Registrant, Technical	akcus@bih.net.ba	DNS/SOA	info@parallels.com	ccI	bih.net.ba kvaz.com parallels.com	<table border="1"> <tr> <th>Name</th><th>Organization</th><th>Address</th></tr> <tr> <td>Aleksey Kotsyubenko</td><td></td><td>kv. Energia Schastye, UA</td></tr> </table>	Name	Organization	Address	Aleksey Kotsyubenko		kv. Energia Schastye, UA
Address	Type(s)																	
link@kvaz.com	Admin, Registrant, Technical																	
akcus@bih.net.ba	DNS/SOA																	
info@parallels.com	ccI																	
Name	Organization	Address																
Aleksey Kotsyubenko		kv. Energia Schastye, UA																

Iris Overview

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

Threat Intelligence Kumite!

SANS CTI Summit 2016
Matt Kodama, VP Products

A blurry background image of a person wearing over-ear headphones, looking at a screen. The colors are warm and golden.

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



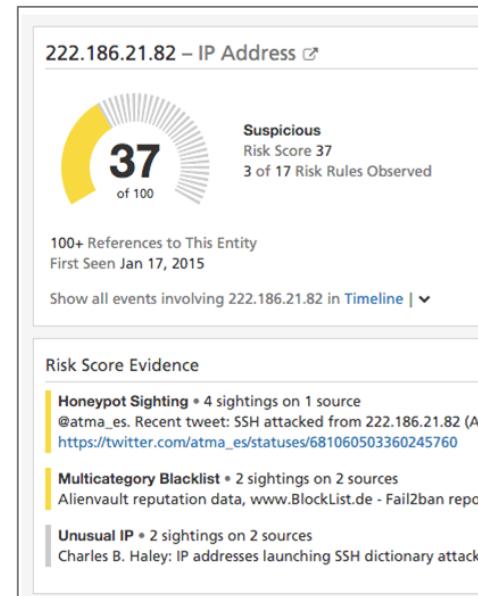
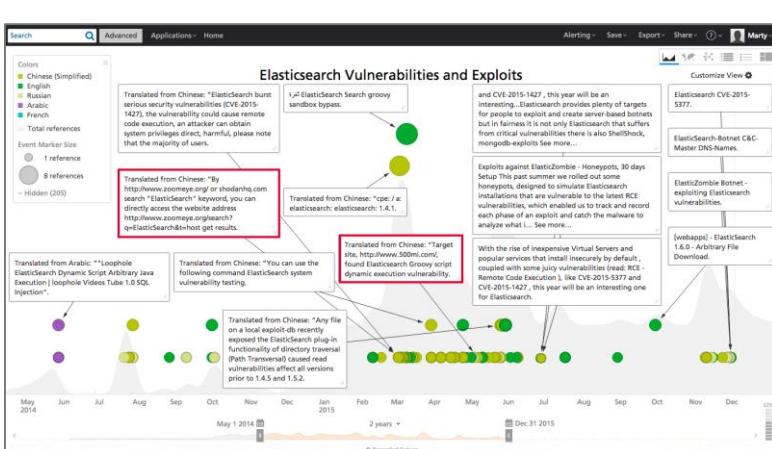
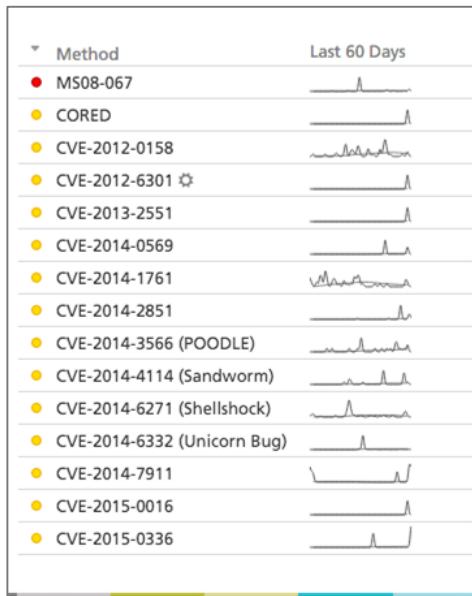
Index
in real-time.
Organize for
threat research.

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



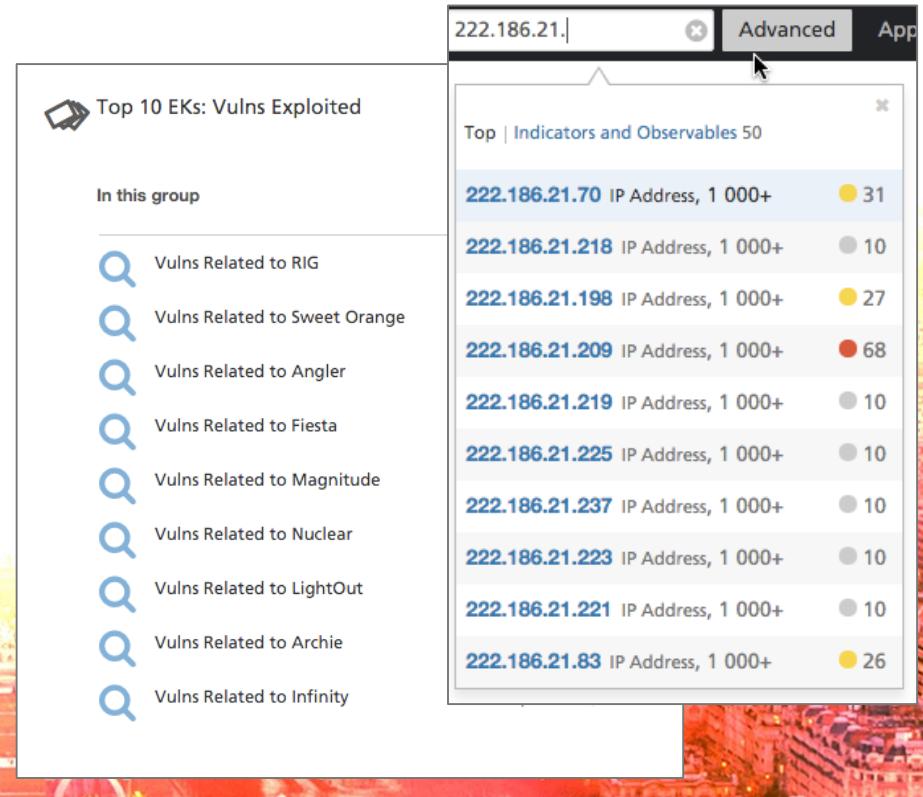
Patented Web Intelligence Engine

Big Data + Data Science + Machine Learning



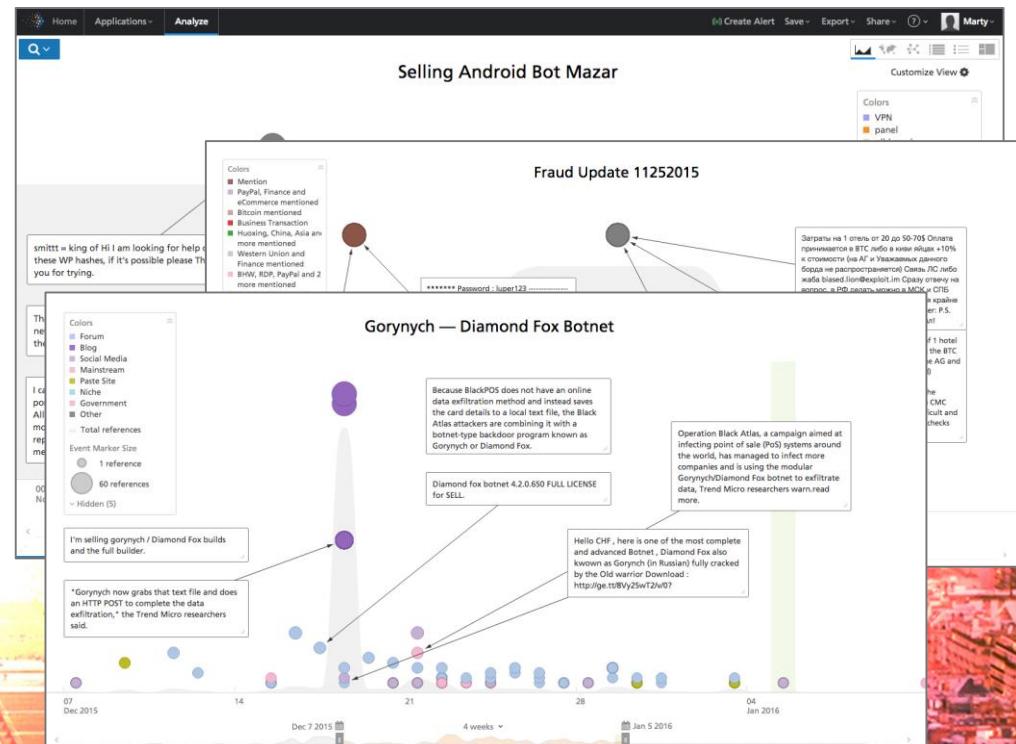
Works for Threat Intel teams like us

- 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

The screenshot shows the DomainTools Whois Record page for the domain `AirportWake-Money.com`. The main page displays the Whois Record, including the registration contact email (`yingw90@yahoo.com`), registrant information (private), and domain status (Registered And No Web). A modal window is open, showing a PasteBin entry titled "Bedep campaign" with the following content:

```
«All observed domains are registered to Gennadily Borisov (yingw90@yahoo.com) Mar 25, 2015, 16:02 • PasteBin • A Guest Flag for review • Save this reference http://pastebin.com/cLSHWfT5 • Show more details»
```

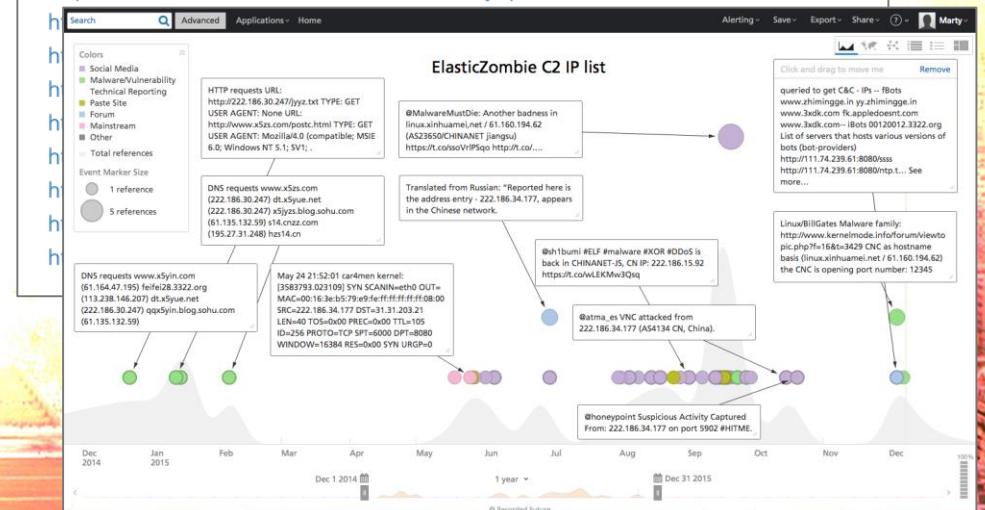
The modal also lists other domains mentioned in the campaign, such as `AirportLimoHire.com`, `TorontoAirportHotel.com`, and `OrlandoAirportHotels.com`. The PasteBin entry continues with a list of observed traffic patterns and referrers.

Improves our defensive controls

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

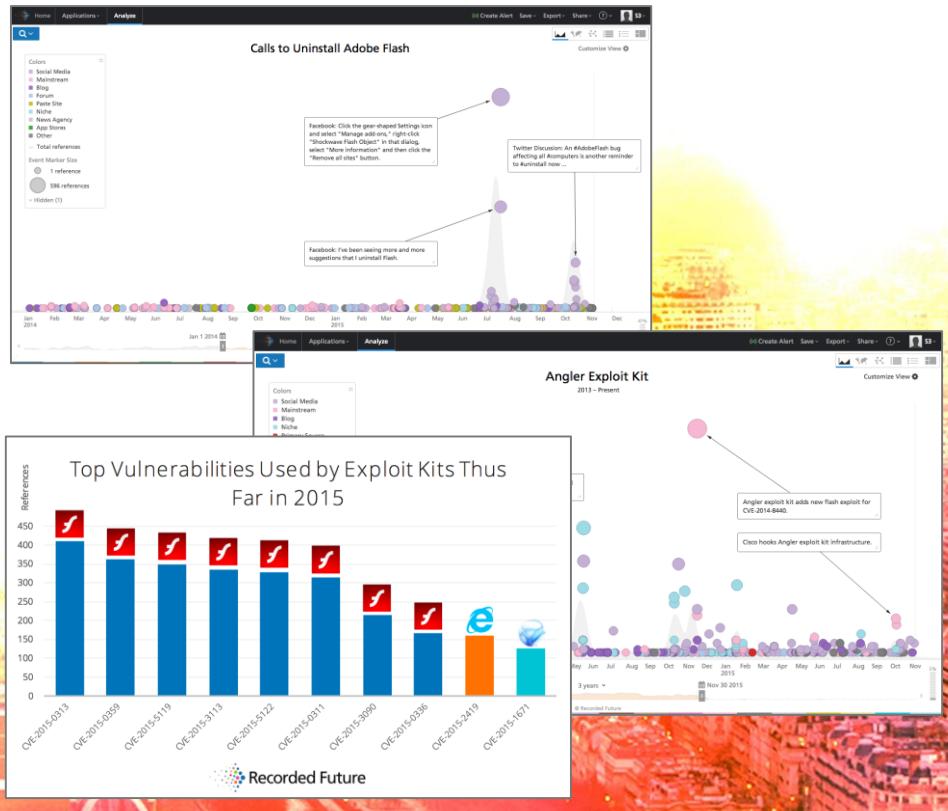
ElasticZombie C2 IP address results from the Recorded Future API enrichment script:

<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>



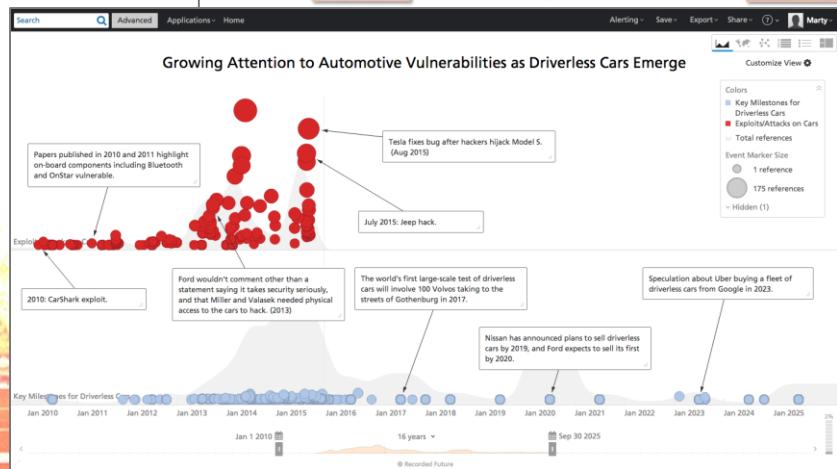
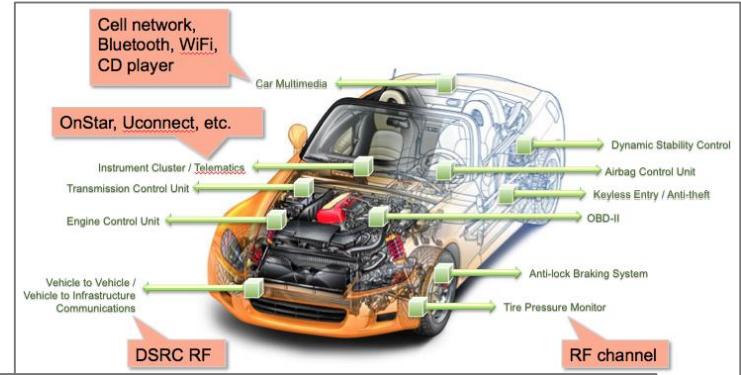
Empowers other security teams

- 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





CYBER DAILY

Get Trending Threat Insights Delivered to Your
Inbox With Our Free Cyber Daily

<http://go.recordedfuture.com/cyber-daily>

SANS

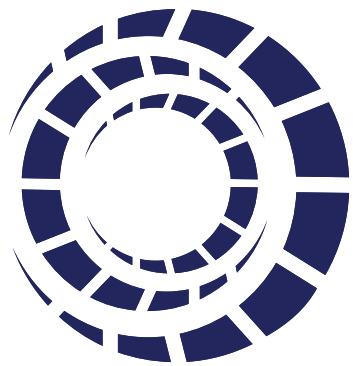
Cyber Threat
Intelligence

SUMMIT & TRAINING



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

Jess Parnell, Centripetal Networks

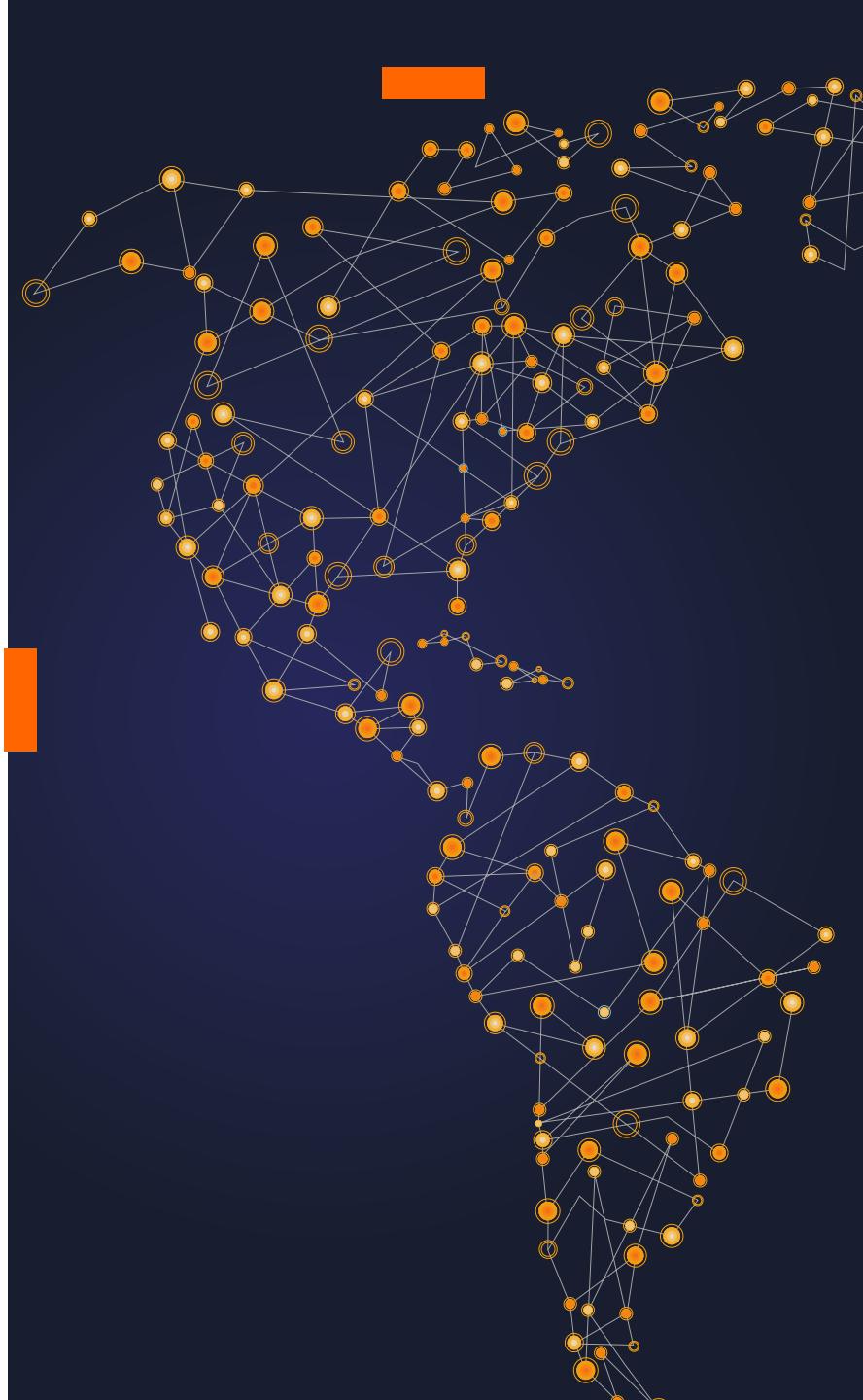


CENTRIPETAL NETWORKS

We Turn Intelligence Into Action™

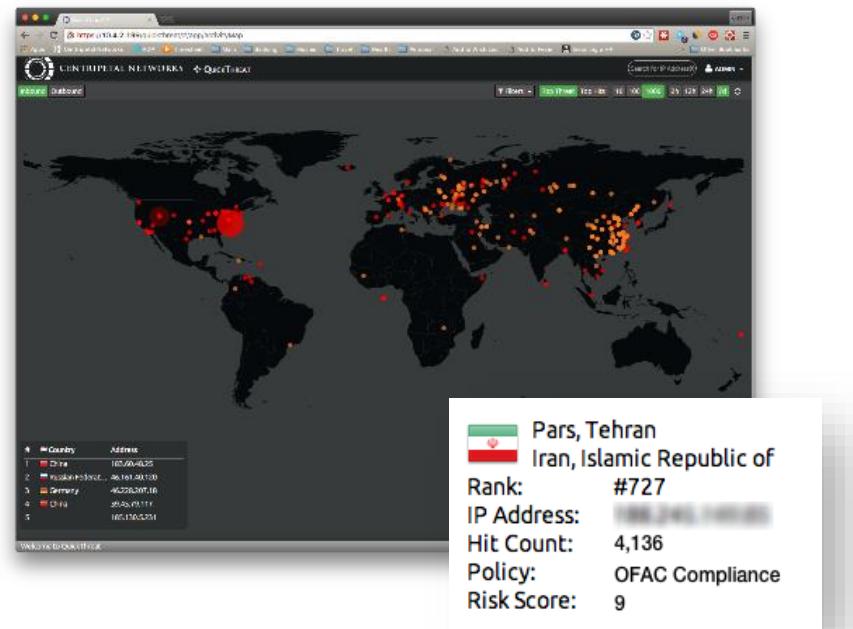
Jess Parnell

Director of Information Security



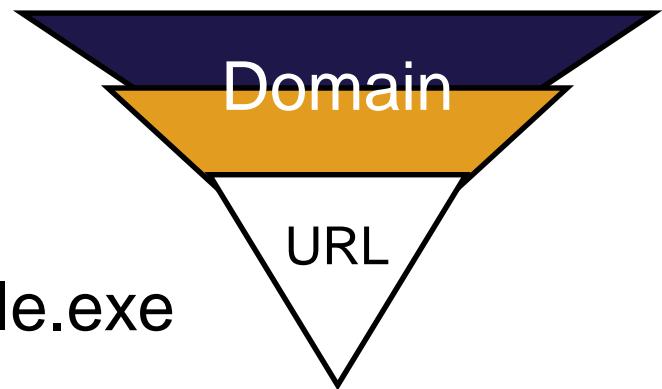
Layered Active Blocking & Logging

- 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



Pyramid of IOCs

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

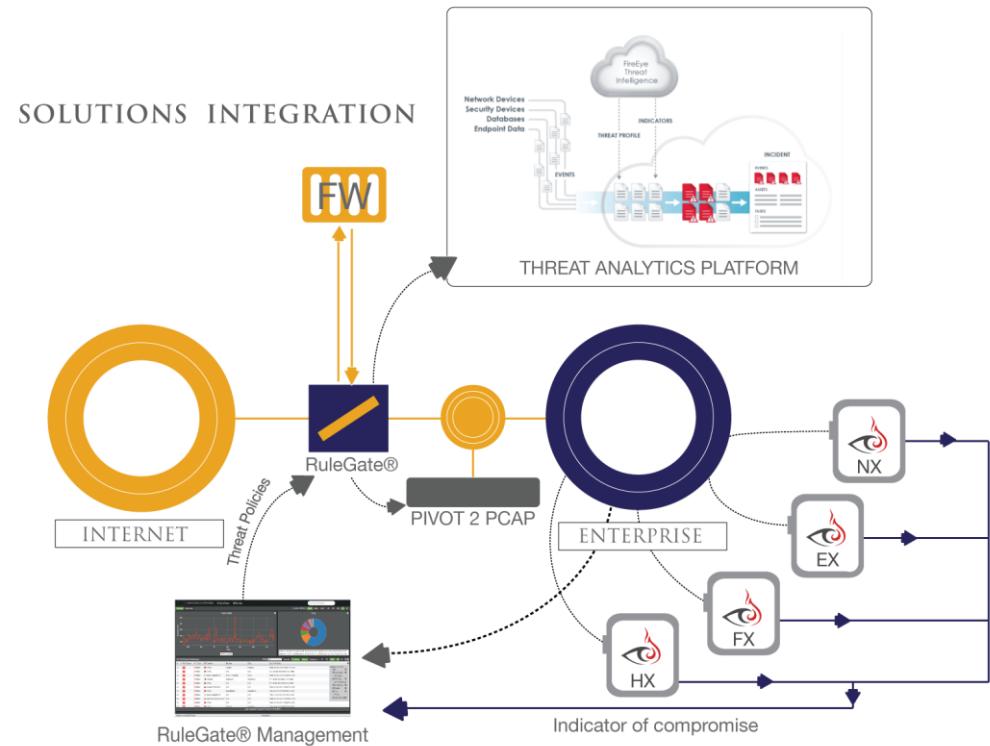


Ref: <https://www.passivetotal.org/pasive/opm-learning.org>

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

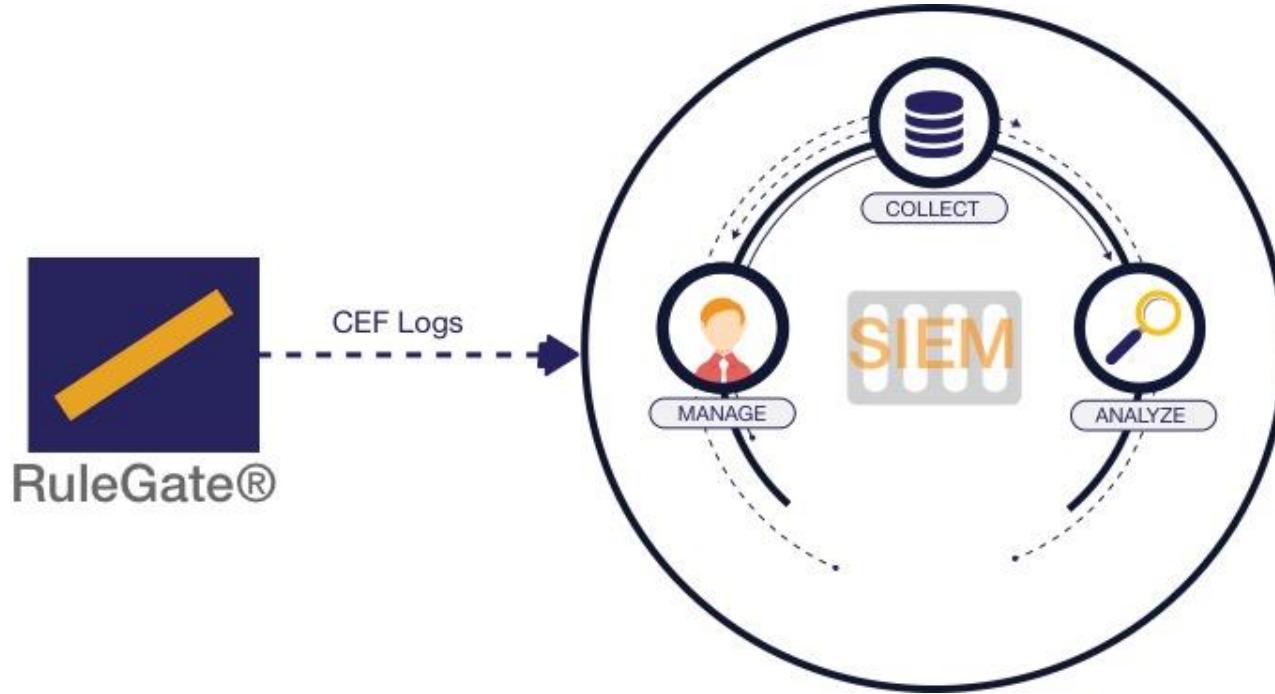
Actively Block on New Threats Discovered

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



CENTRIPETAL
NETWORKS

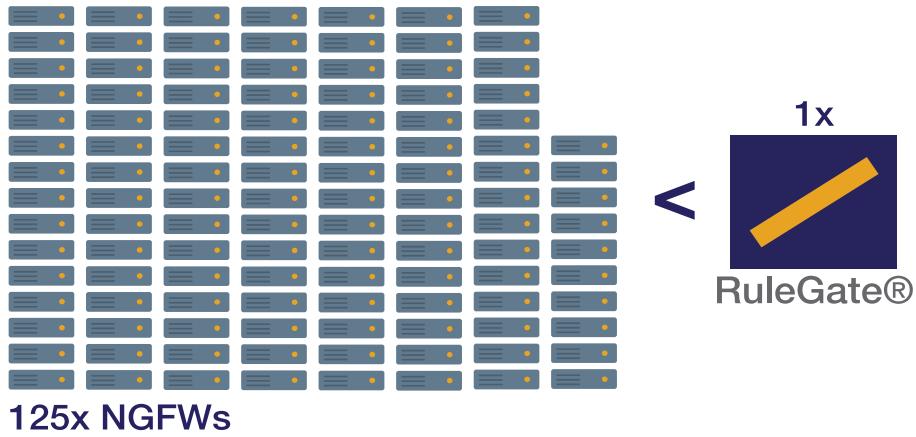
Send to SIEM: Correlate End-User



- 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

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

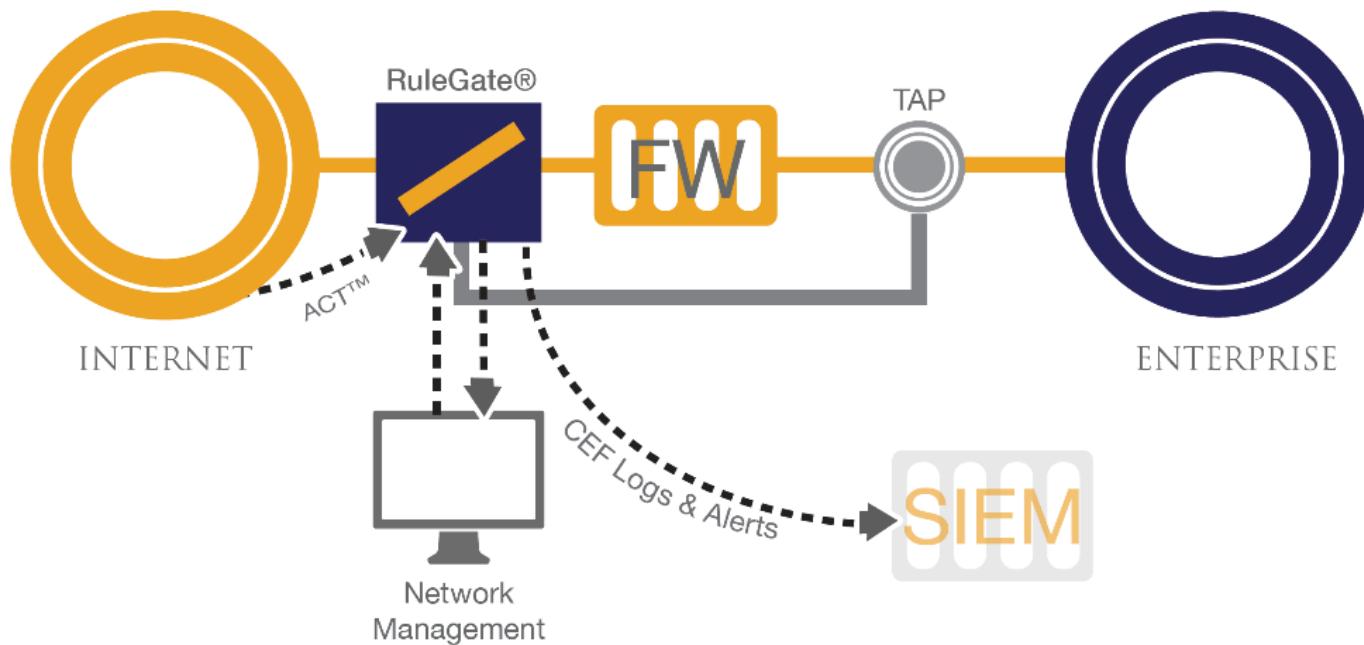


SIEM is purely for analysis, and has no Active Blocking capability



Is the RuleGate a Threat Intelligence Platform (TIP)?

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



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

Commercial Intelligence



iDEFENSE

powered by VERISIGN

Enterprise Intelligence



Industry Intelligence



(not an exhaustive list of Centripetal intelligence sources)



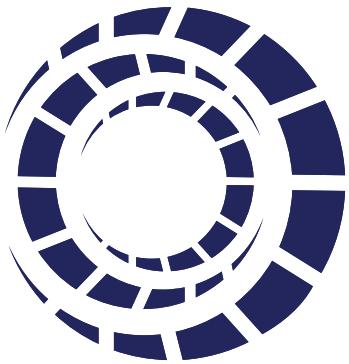
CENTRIPETAL
NETWORKS

You will NOT be overwhelmed with Actionable Intelligence

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

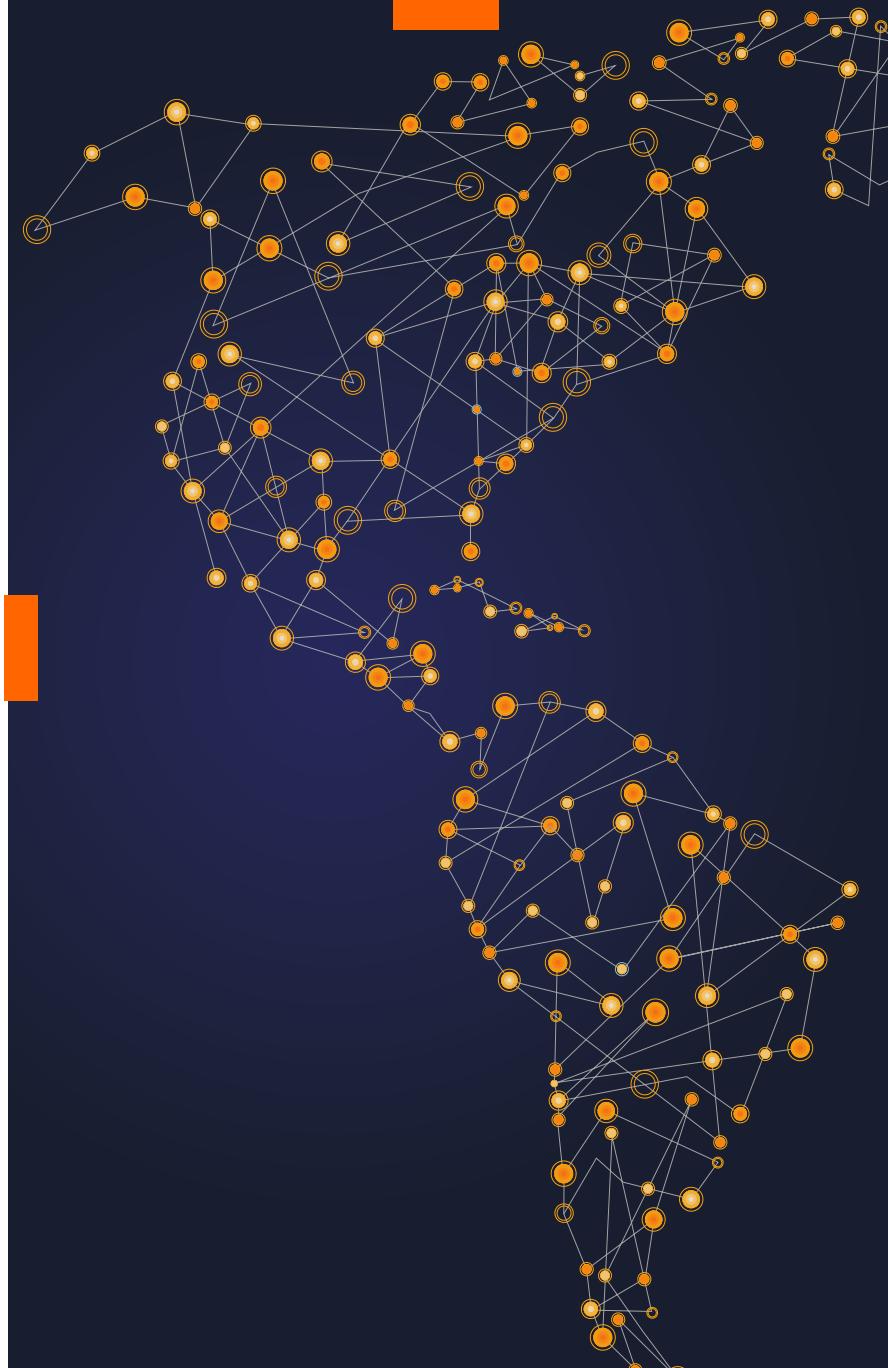
The screenshot displays the QuickThreat® software interface. At the top, there's a correlation table showing data for IP 185.112.102.211. Below it is a detailed threat analysis card for the IP address 185.112.102.211, which is identified as being from MediaServicesPlus Ltd. in Russia. The card indicates the IP is actively malicious, first seen on Dec 3 2015, last seen on Dec 17 2015, and has a threat score of 2 (out of 7). It also shows icons for scanning host and malware IP. To the right of the card is a map of Moscow with a location marker.

QuickThreat® - Pivot to Source



CENTRIPETAL NETWORKS

Thank You



SANS

Cyber Threat
Intelligence

SUMMIT & TRAINING



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

Roselle Safran, UpLevel Security

UPLEVEL



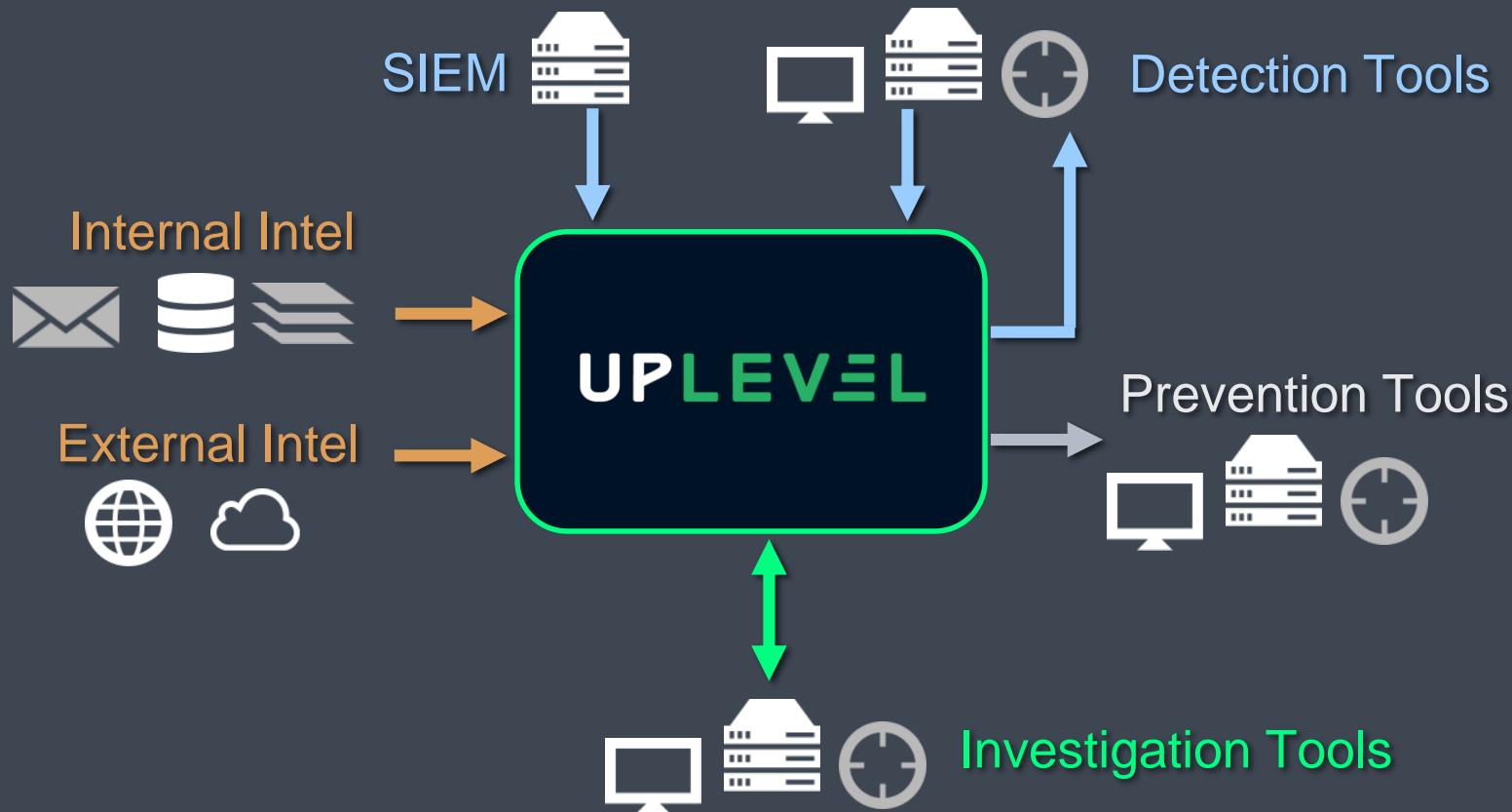
www.uplevelsecurity.com

@uplevelsecurity

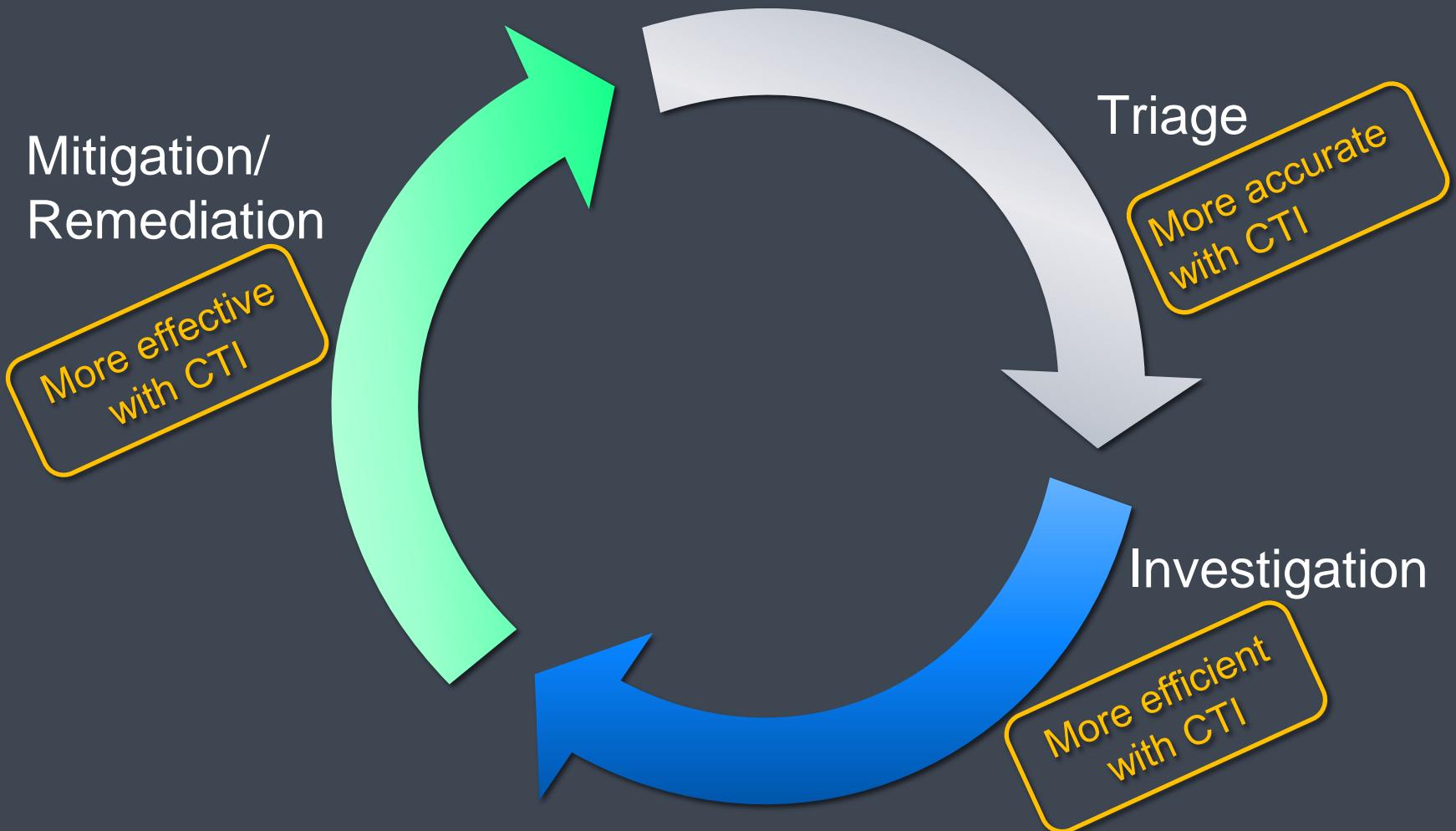


What is Uplevel?

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

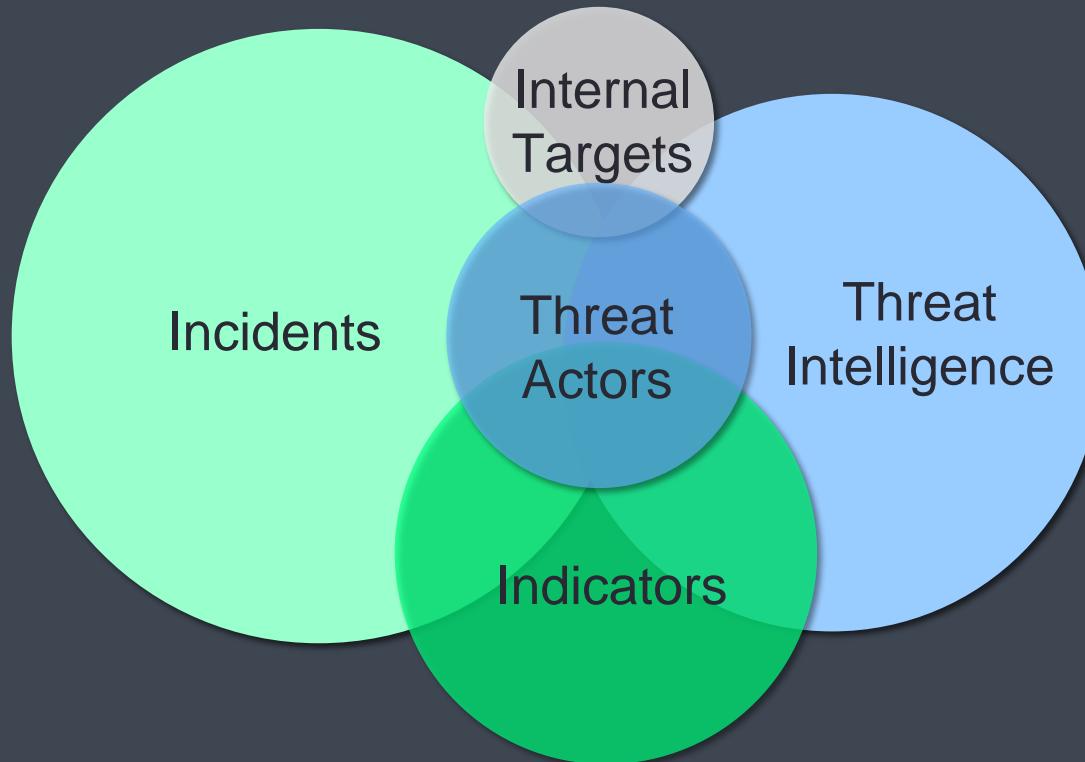
Cybersecurity Operational Expertise



Cybersecurity Data Analysis Expertise



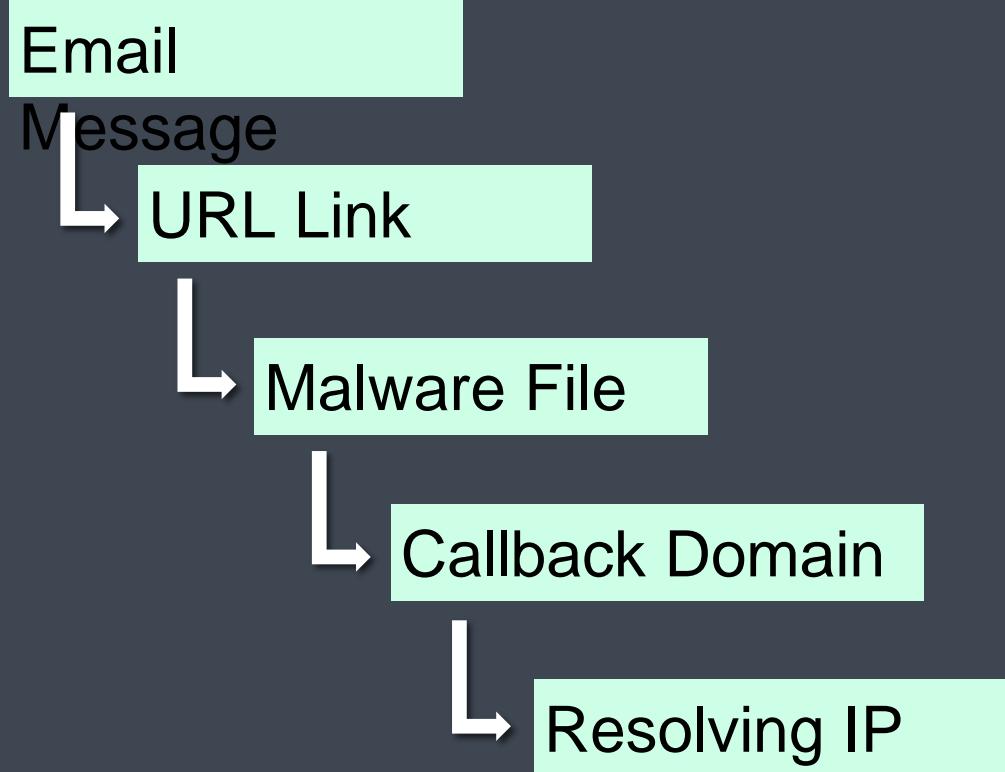
Reason #4: Uplevel Integrates Incident Management and Threat Intel Management into One System



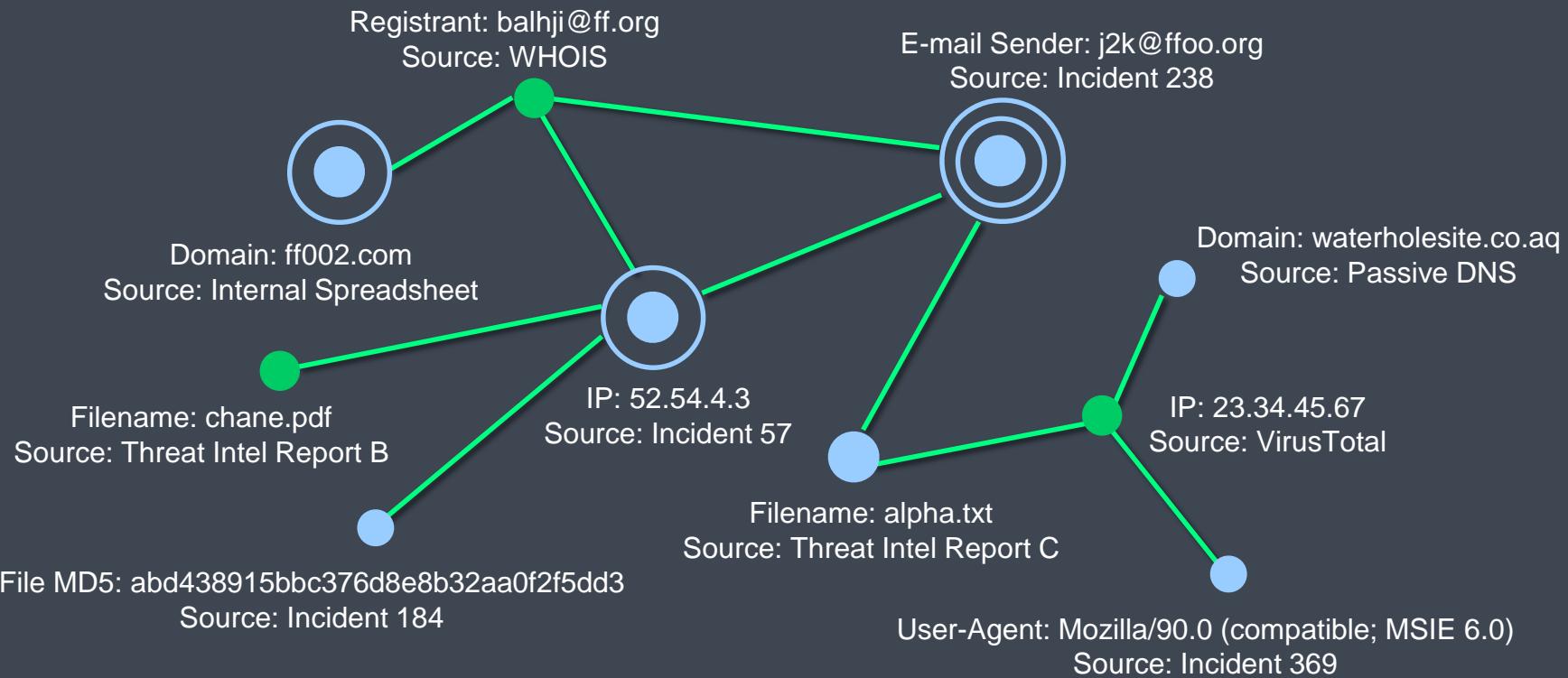
- Collaborative
 - Comprehensive
 - Consistent
-

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