



CISO's Guide To Shutting Down Attacks Using The Dark Web

October 23, 2019

Agenda

- The Dark Web: What's At Stake
- Gain Visibility, Take Control
- Leveraging Splunk & Phantom
- Key Recommendations

Agenda

- **The Dark Web: What's At Stake**
- Gain Visibility, Take Control
- Leveraging Splunk & Phantom
- Key Recommendations

What Do We Know About The Dark Web?

1 - 2 - 3

Desert Eagle 357 Mag GOLD
TIGER STRIPE

Features:
Manufacturer: Magnum Research

1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11

Remington Defense XM110
SASS 308

This rifle was one of the designs that Remington Defense submitted for the Military SASS trials. This is a very nice

1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11

Barrett M107A1 20" CQ FDE 50
BMG QDL Suppressor

It has the upgraded muzzle brake which gives you less recoil, and enables you to stay on target for faster, more

(28 GRAMS) Critical x AK47 - TOP-SHELF WEED!
HIGH & FLAVOR!! AAA+++ INDOOR GROWN

28g 30
1lbs 15

Decommissioned Soviet submarine

Product	Price	Quantity
Submarine	\$1.7 mn = 2951.388 ₺	1 X Buy now



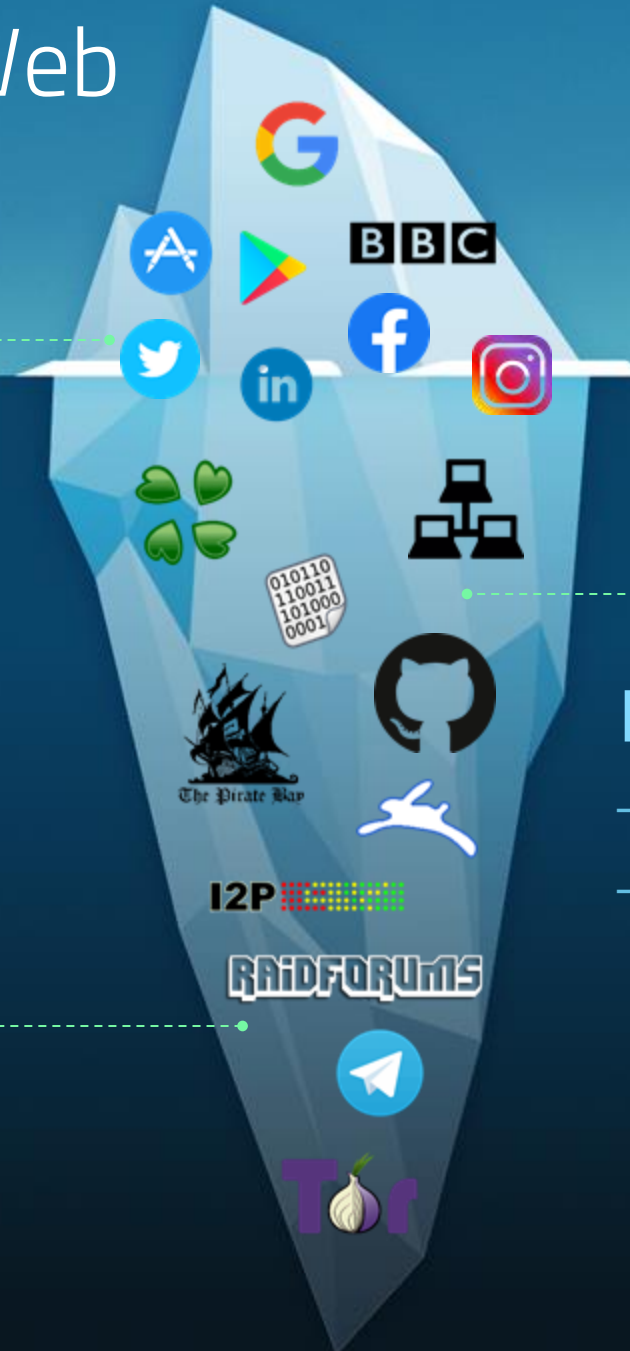
The Clear, Deep, and Dark Web

Clear Web

- Search engines
- Media, blogs, etc.

Dark Web

- Anonymous, closed sources, Telegram groups, invite-only (sometimes)
- Tor, P2P, hacker forums, criminal marketplaces, C2s, etc.



Deep Web

- Unindexed by search engines
- Webmail, online banking, corporate intranets, walled gardens, etc.

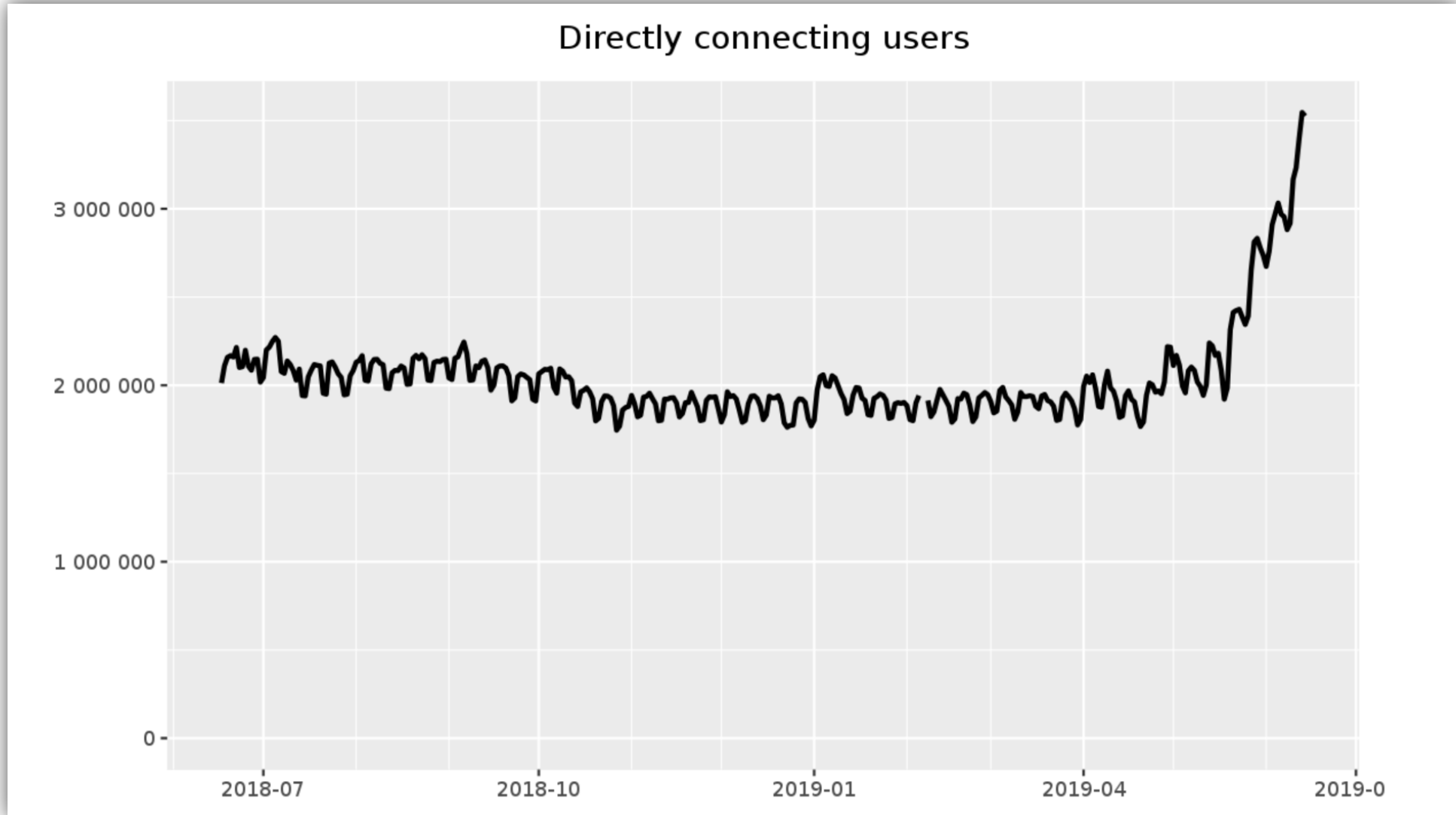
How Tor Works



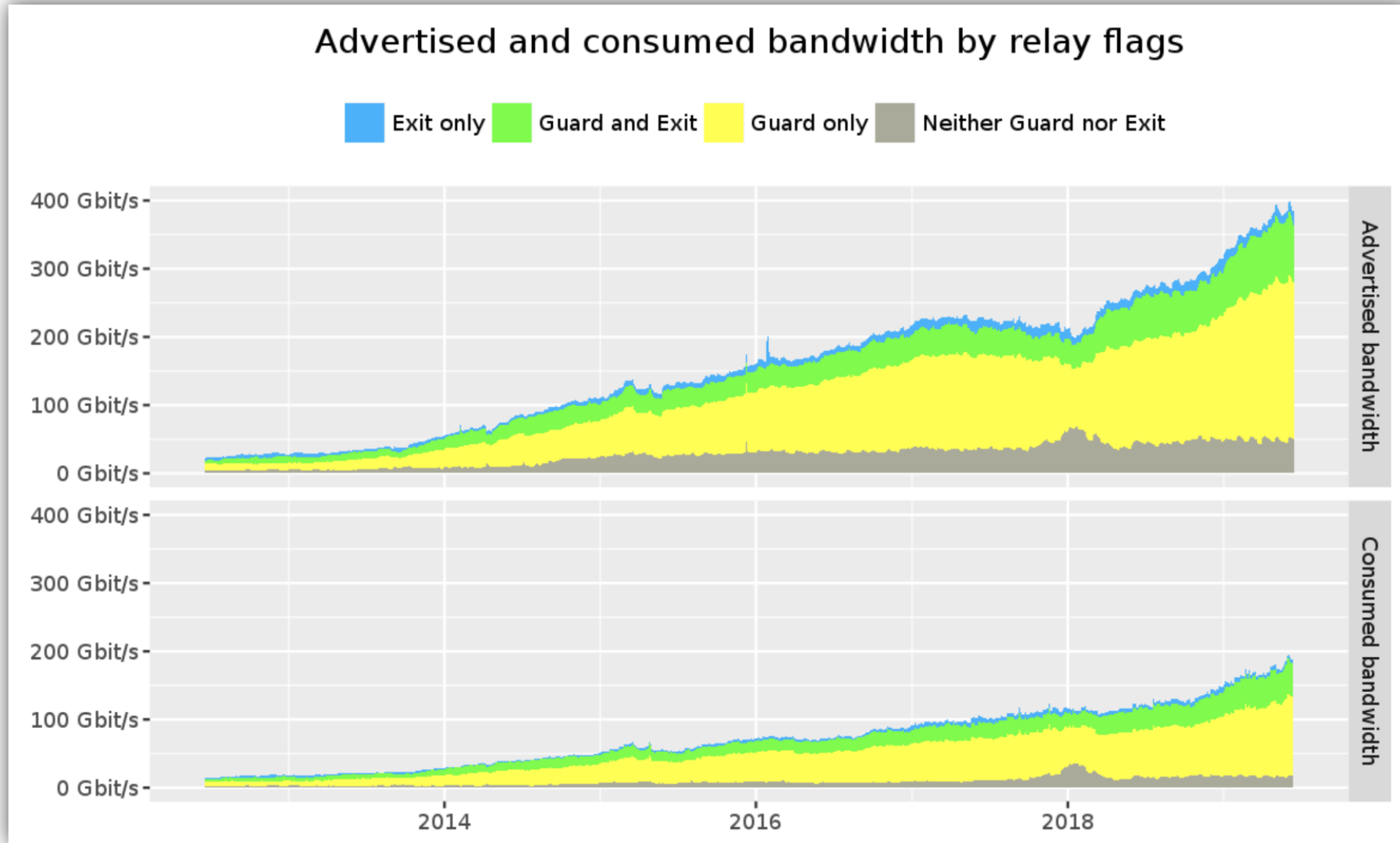
RED links are encrypted
BLUE links are in the clear.



Tor Usage Statistics



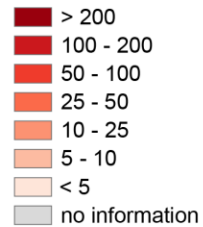
Tor Usage Statistics



Tor Usage Statistics

The anonymous Internet

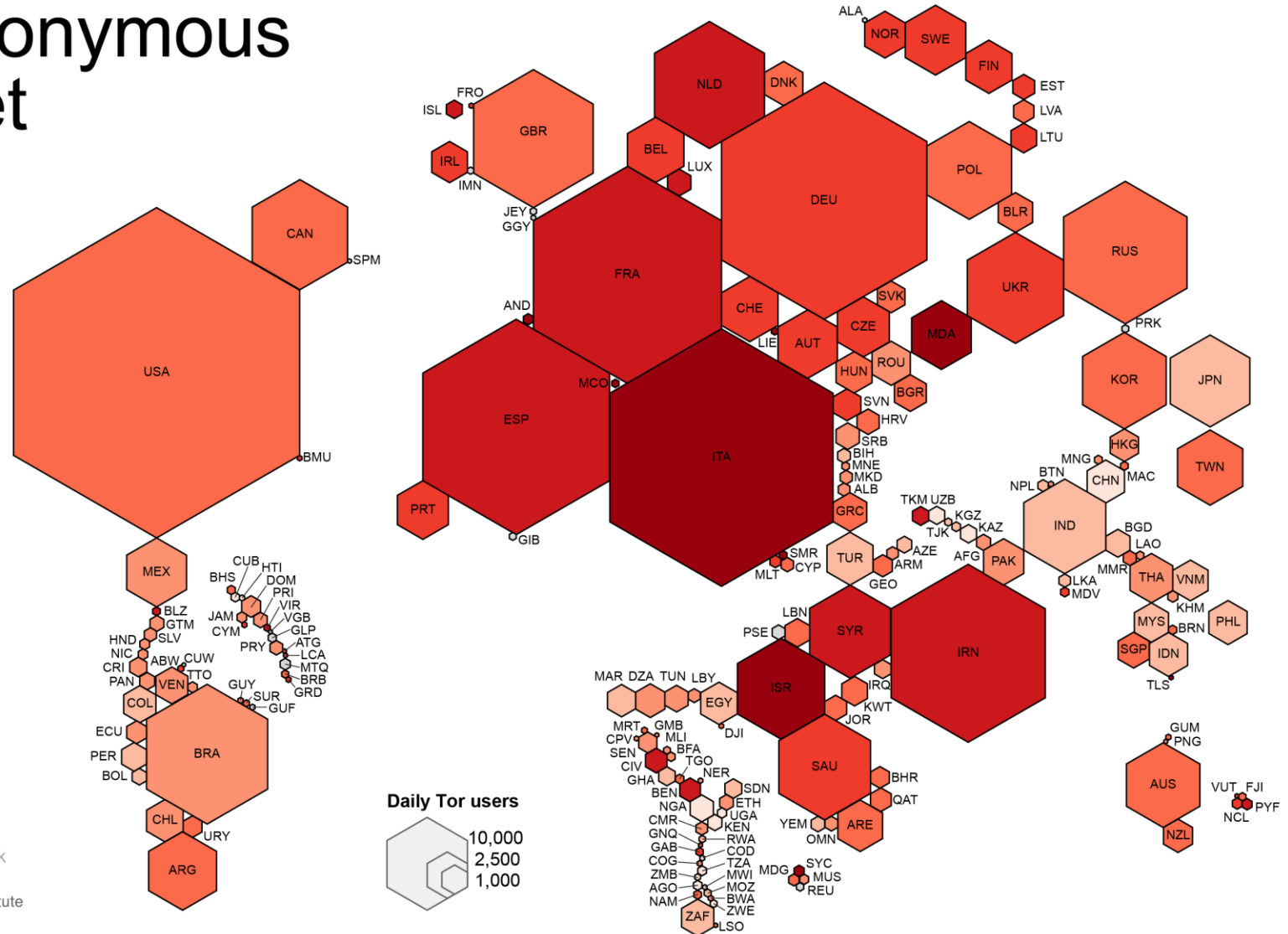
Daily Tor users
per 100,000
Internet users



Average number of
Tor users per day
calculated between
August 2012 and
July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham
(@geoplace) and
Stefano De Sabbata
(@maps4thought)
Internet Geographies at
the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk



The User Experience Can Match Legitimate Sites

SSN/DOB Lookup

Home / Lookup / SSN/DOB Search

SEARCH OPTIONS

Full name + State ▾

Start search

* Search price: **FREE**. SSN/DOB Price: \$ 5

** Possible **DOB** format is yyyy/mmdd

SEARCH RESULTS

Show entries

Search:

SSN	DOB	Name	Address	Action
HIDDEN	19380900	JOHN M HOPKINS JOHN HOPKINS	68 Young Ave Croton On Hudson, NY 10520 203 Half Moon Bay Dr # 2 Croton On Hudson, NY 10520 203 HALF MOON BAY DR CROTON ON HUDSON, NY 10520	Buy record
HIDDEN	19410600 19410600	JOHN P HOPKINS JOHN HOPKINS JOHN PATRICK HOPKINS	553 Edison Ave Bronx, NY 10465 548 Edison Ave Brorox, NY 10465 Tanzman Rd Parksville, NY 12768 657 Tanzman Rd Parksville, NY 12768	Buy record
HIDDEN	19681200 19351800	JOHN J HOPKINS JOHN JAMES HOPKINS JOHN HOPKINS	52 E 20th St # O New York, NY 10003 11 Little Harbor Rd Mount Sinai, NY 11766 355 Staples St Farmingdale, NY 11735 41 Sheldon Pl Commack, NY 11725 453 E 14th St Apt 10F New York, NY 10009 16 Oak Ct Selden, NY 11784 PO Box 655 New York, NY 10009 451 E 14th St New York, NY 10009 302 Ravenswood Rd Hampstead, NC 28443 443 Golf Course Dr Hampstead, NC 28443	Buy record



Even Farmers Turn To The Dark Web



Threats are mounting



278%

Products for sale on black markets



297%

Phishing websites



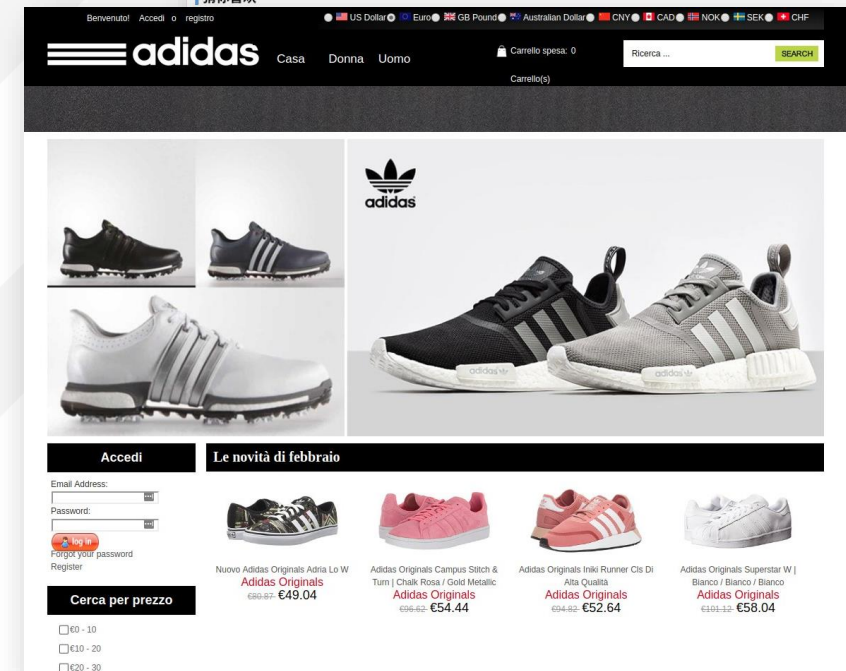
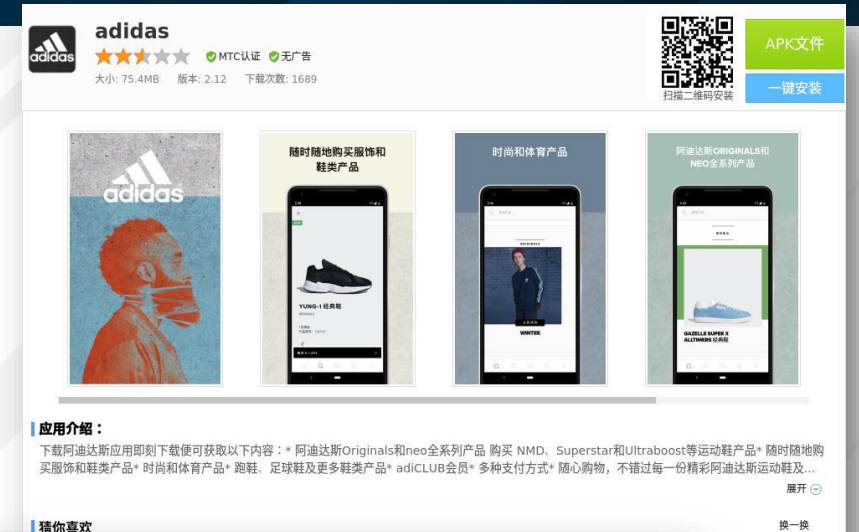
171%

Compromised employee credentials



149%

Stolen credit cards for sale on dark web



Agenda

- The Dark Web: What's At Stake
- **Gain Visibility, Take Control**
- Leveraging Splunk & Phantom
- Key Recommendations

Our attack surface keeps growing



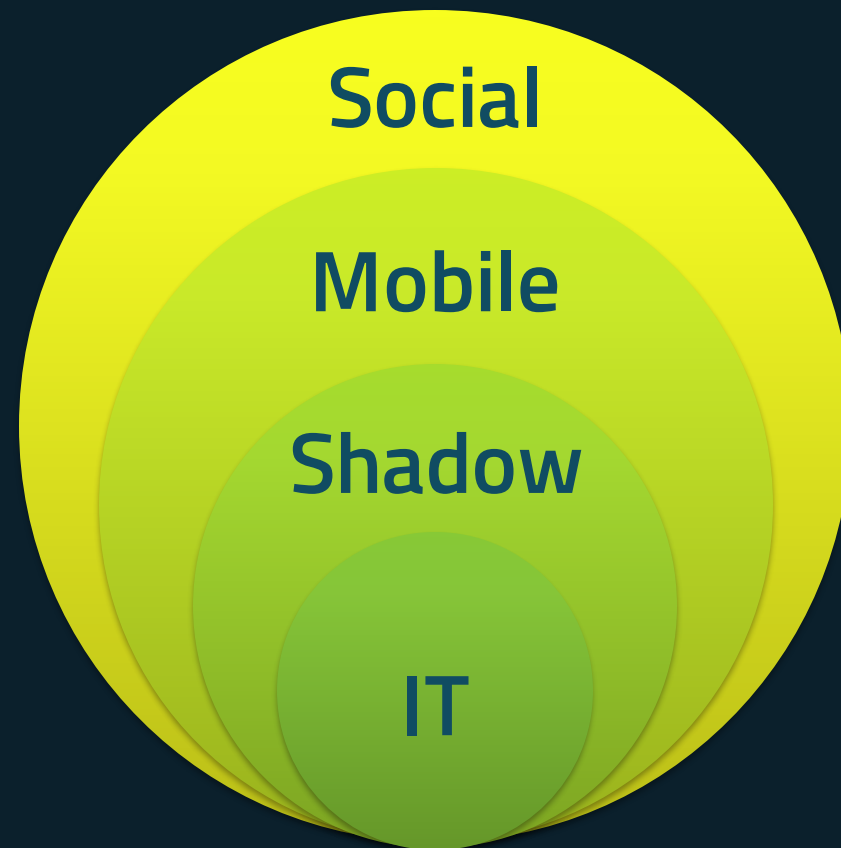
Our attack surface keeps growing



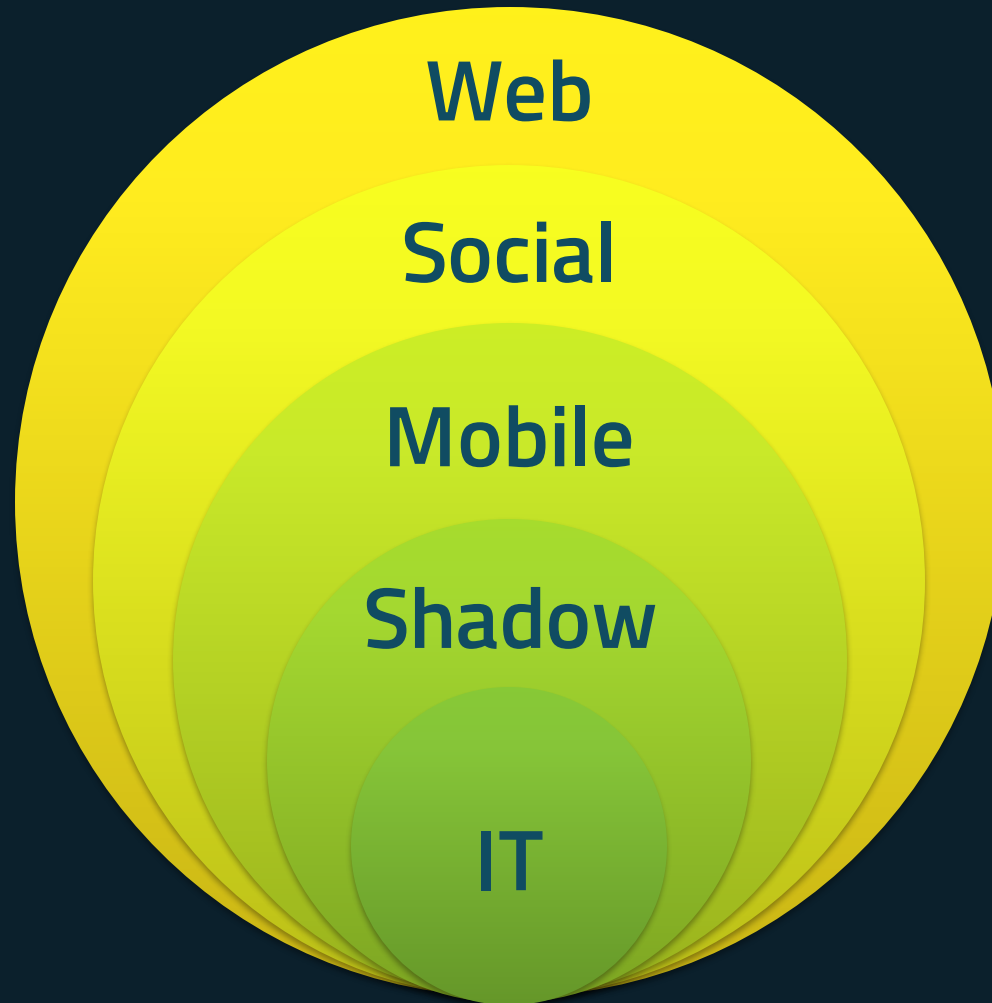
Our attack surface keeps growing



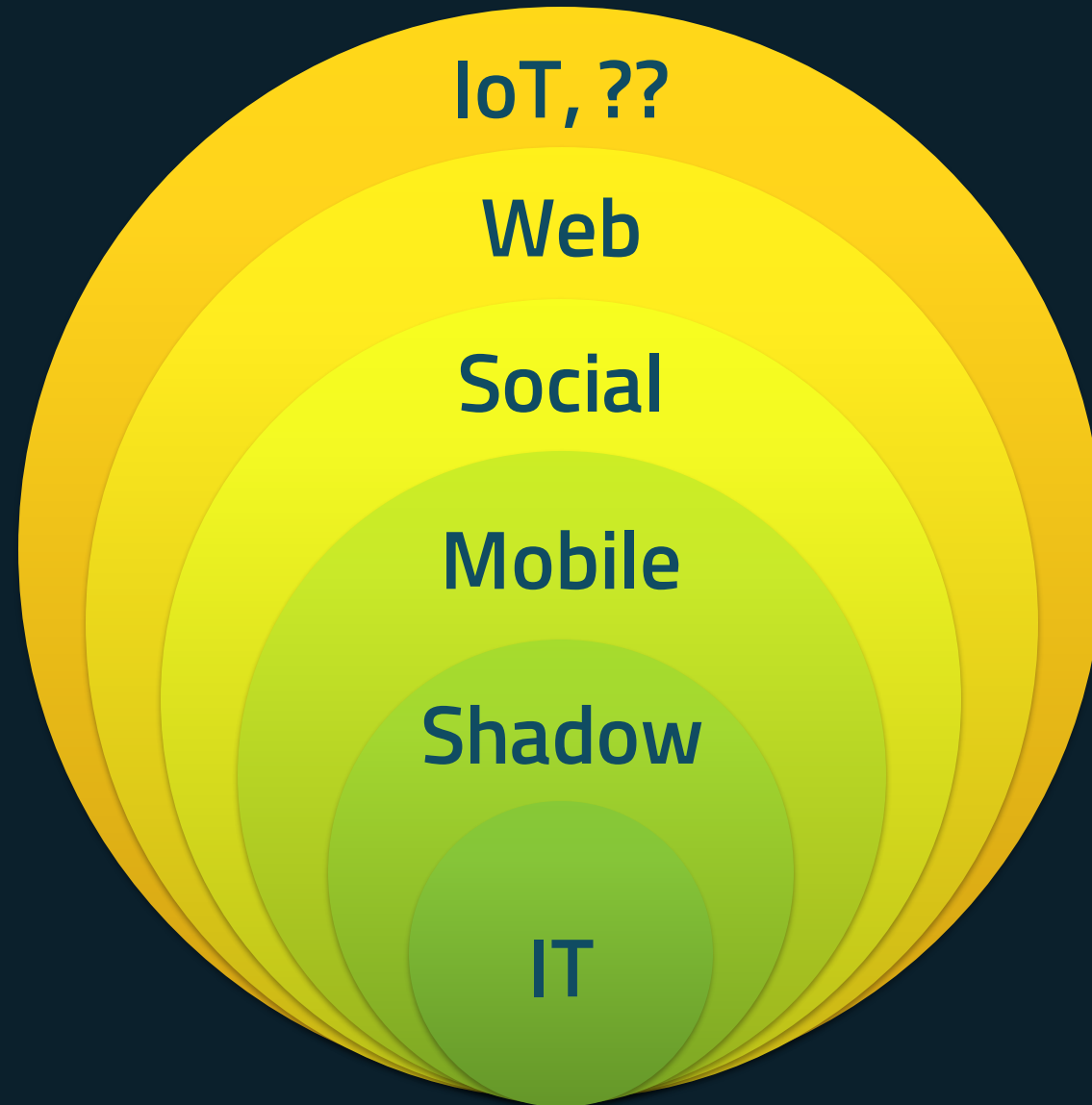
Our attack surface keeps growing



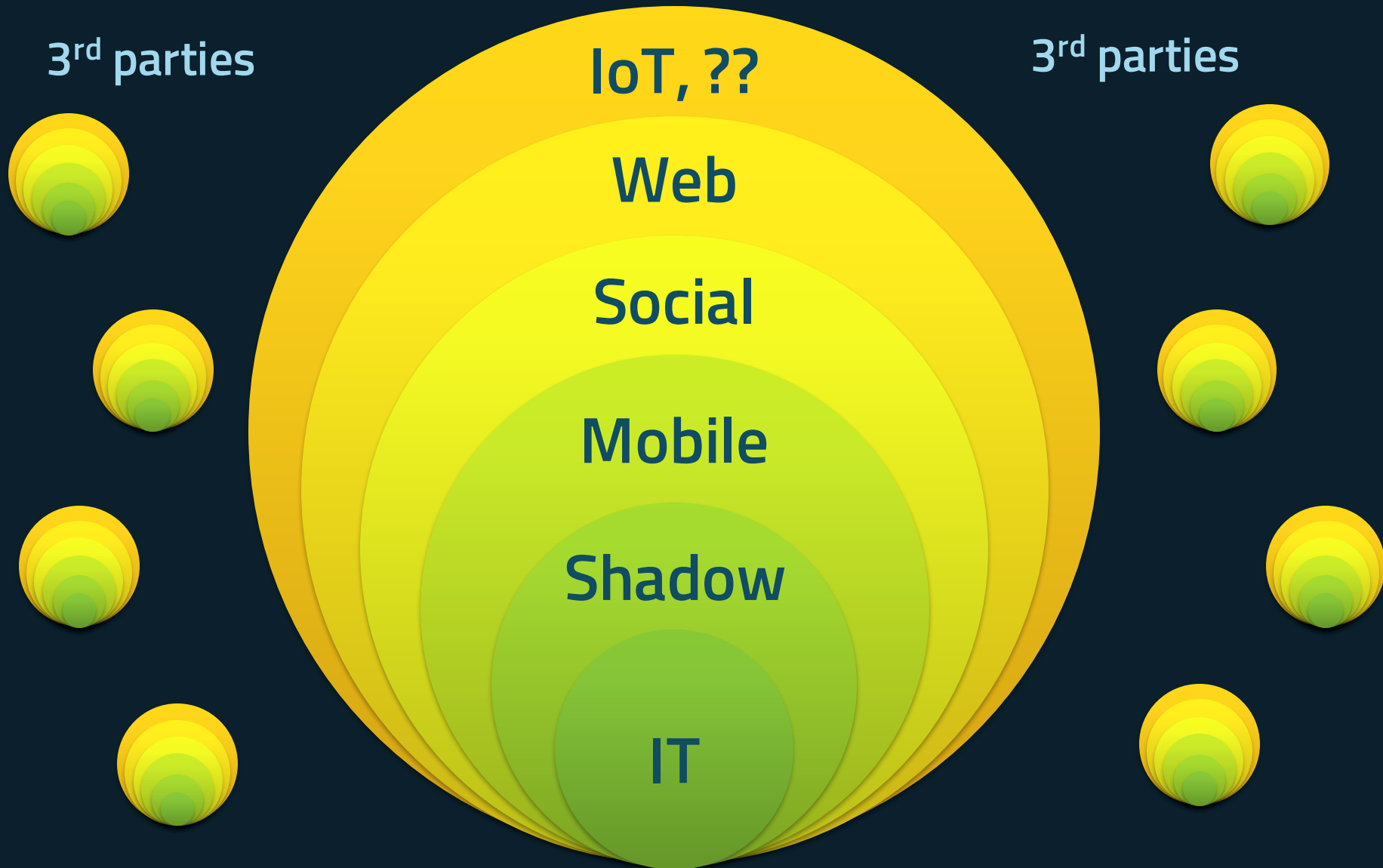
Our attack surface keeps growing



Our attack surface keeps growing



Our attack surface keeps growing



Our attack surface keeps growing

4th parties

3rd parties

IoT, ??

Web

Social

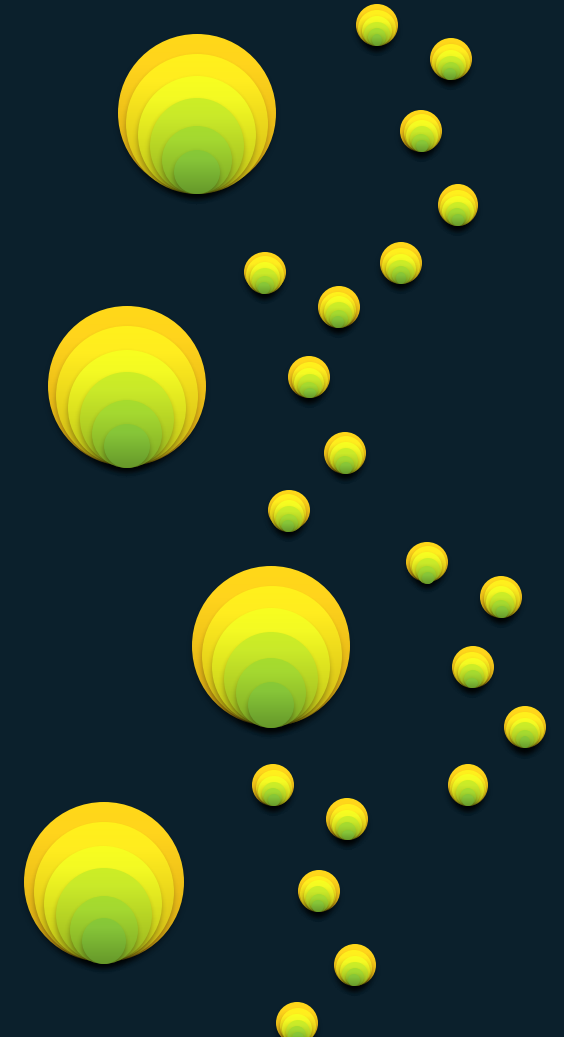
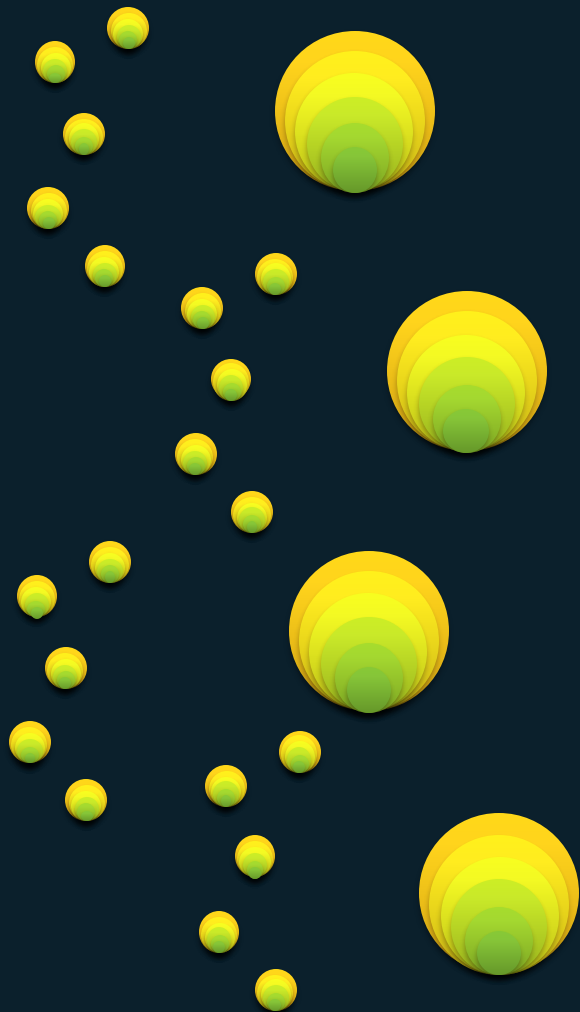
Mobile

Shadow

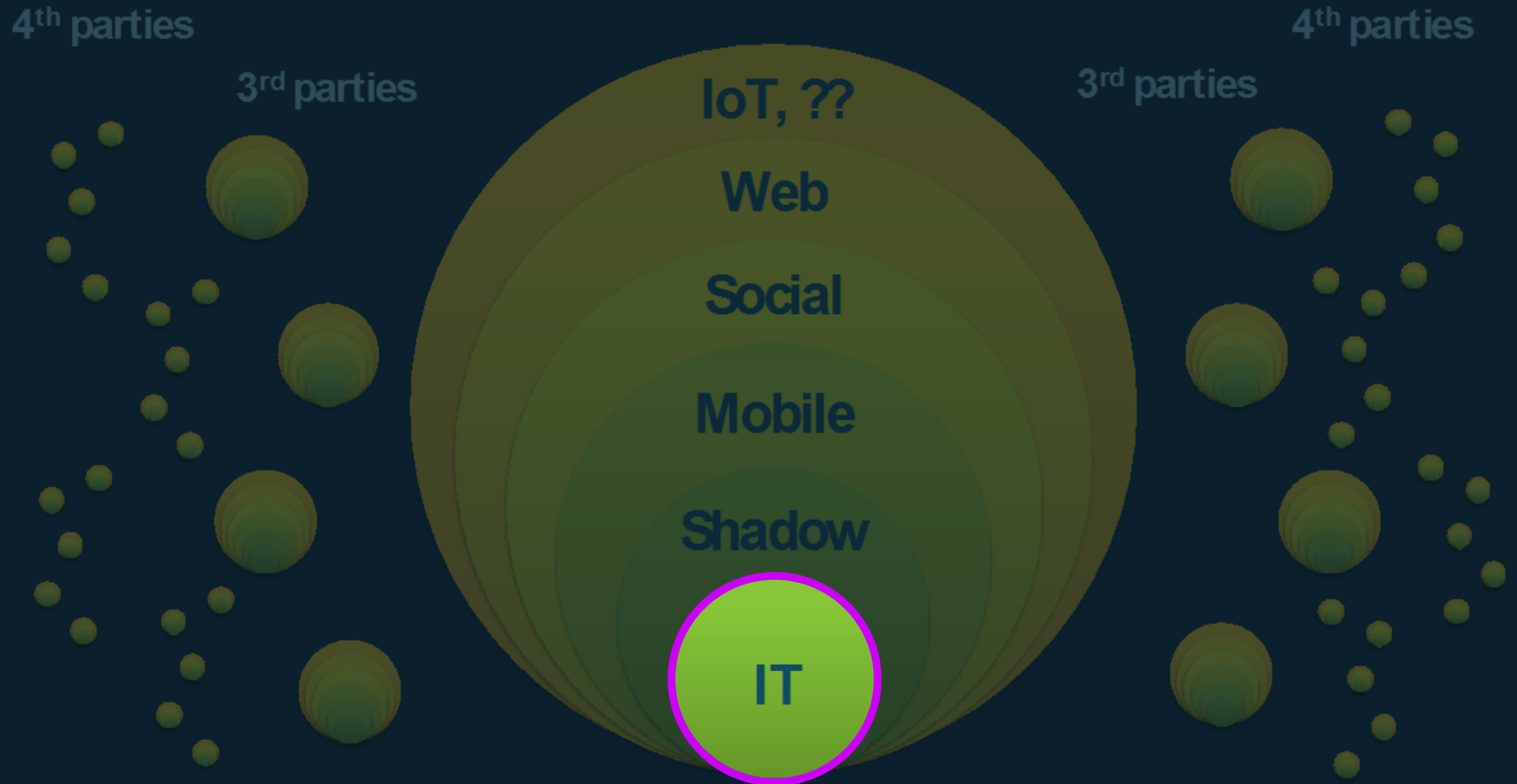
IT

3rd parties

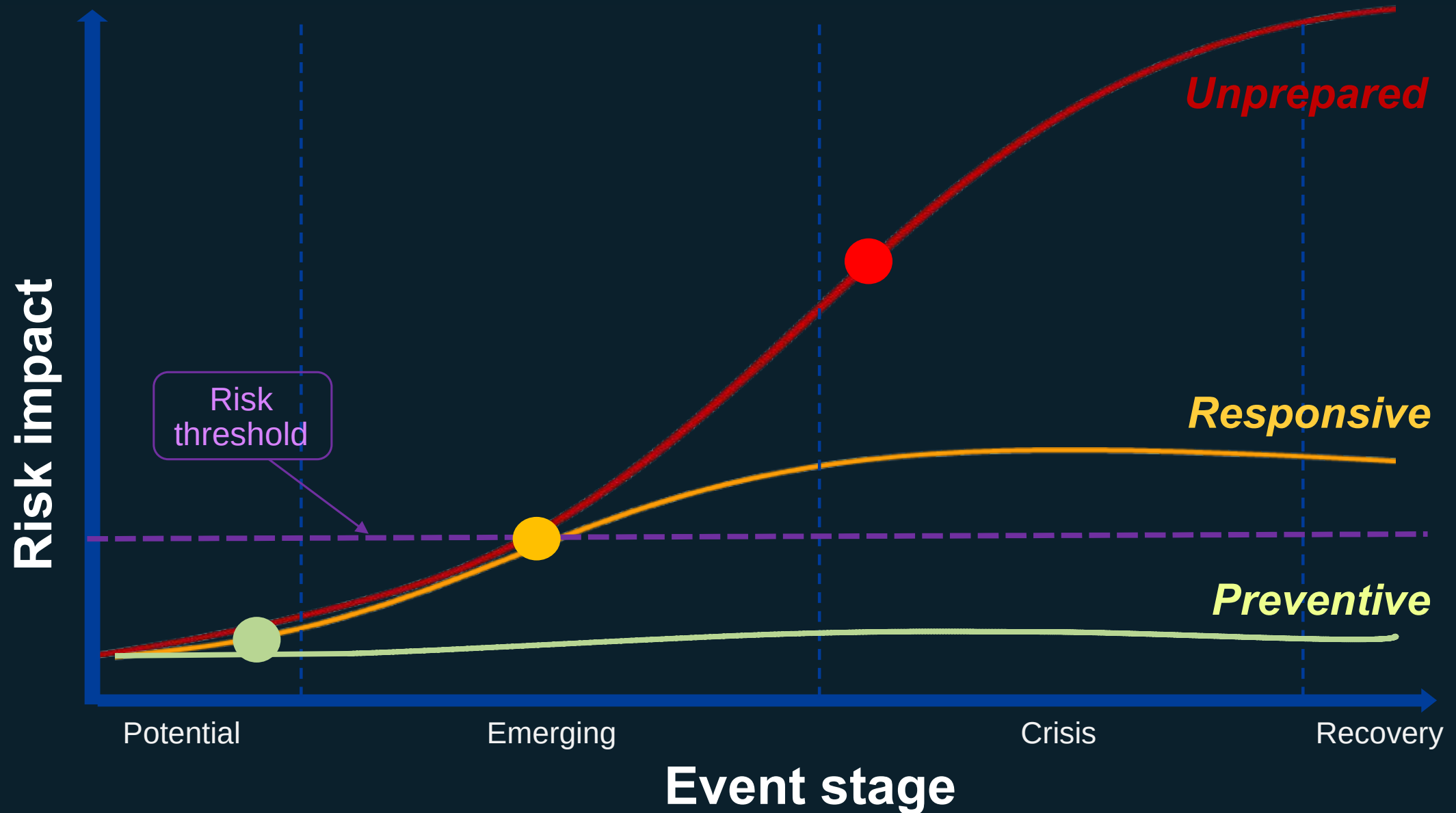
4th parties



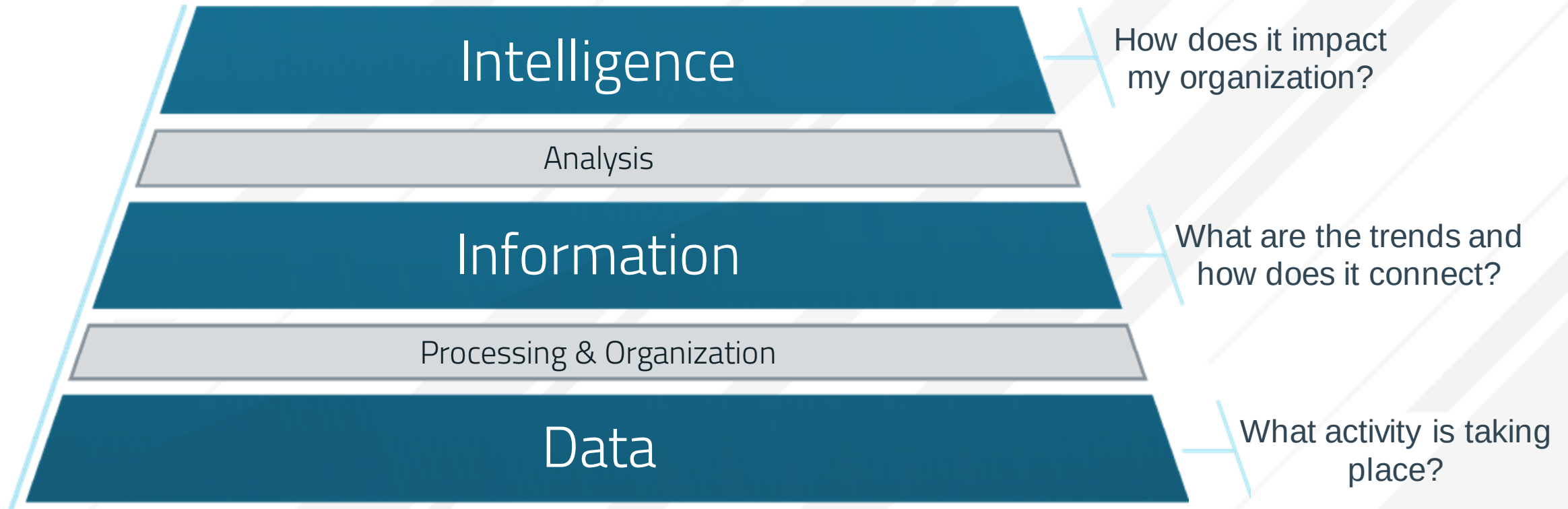
Lack Of *Visibility*, Lack Of *Control*



Reduce The "Mean-time-to-Remediate"



Turning External Data Into External "Intelligence"



What you'll uncover: Compromised Credentials

Username	Email	Password
dan	dan	5:secure. whitepages.com:9F840EA6E04 B22541
anna_	anna_	:secur e.whitepages.com:DEF6EC192 37202C11
stacy_	stacy_	:secur e.whitepages.com:DED686393 7FD1DE41
stacy_	stacy_	:www. whitepages.com:0645FE59D8C 00A264
tom_	tom	:secur e.whitepages.com:EDD913E5B A52F9621
robert_	robert_	:secur e.whitepages.com:2CD2BEAD C6368D281
robert_	robert	:www. whitepages.com:6DAECCE7DA 5802884
sue_	sue_	:secur e.whitepages.com:8EF60451C 7A816201
yaneke	yanek	:secure. whitepages.com:371F12B58A6 83C981

Employee credentials

Shop	Balance	Points	Type	Country	CC	Bank	Info	Last order	Mail access	Seller	Price (\$):
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-	L0quer0	1.5

Customer logins

```
*****BankLogins Prices:
Bank Logins Prices USA, UK, CA, AU, EU...other countries

* Bank USA: ( [REDACTED] ...)
. Balance 3000$ = 150$
. Balance 5000$ = 250$
. Balance 8000$ = 400$
. Balance 12000$ = 600$
. Balance 15000$ = 800$

* Bank UK: ( [REDACTED] ...)
. Balance 5000 GBP = 200$
. Balance 10000 GBP = 500$
. Balance 16000 GBP = 700$
. Balance 20000 GBP = 1000$

+ Bank To Bank Transfer To Any USA Bank
+ Bank To Bank Transfer To Any UK Bank
+ Bank To Bank Transfer To Any Euro Country Bank
+ Amount To Pay For That Depend On Amount You Want To Transfer
+ With Account Bank Login : Username + Password Number
+ I always check the balance and login details before selling

- You can contact me for more and many Bank Logins you need.
- Have all details for login and I can transfer balance to your account

Bank To Bank Transfer To Any Usa Bank

Bank To Bank Transfer To Any Uk Bank

Bank To Bank Transfer To Any Euro Country Bank

Amount To Pay For That Depend On Amount You Want To Transfer
```

Bank accounts



What you'll uncover: Stolen credit & gift cards



MONSTER Carder's GigaPack -The \$\$\$ MAKER! -NEW 2016- + FREE Gift by SoftkingUS -Antidetect FF Browse

USD 7.99
1 0.0193

In stock

Vendor: **SoftKingUS** [+11][0] 20+

Class: Digital

Delivery: Instant Delivery

Quantity: 1

Buy Now

[Question](#) [Report](#)

Also available:

MONSTER Carder's GigaPack -The \$\$\$ MAKER! -NEW 2016- + FREE Gift by SoftkingUS -Antidetect FF Browse **USD 7.99** 1 0.0193

[Details](#) [Feedback](#)

Description

Want to cashout REAL MONEY?
Want to be a successful carder?
Want relevant resources and guides to make a killing with carding?

-----CHECK ALL POSTAGE OPTIONS FOR PACKS OPTION !!!!-----
The most complete collection from the most famous carders the darknet has ever seen !!!

Now YOU can have all you NEED to make REAL MONEY !!!

PLASTIC
MARKETPLACE

CHOOSE PLASTIC:

All cards are with PIN-codes and full holder info!

What to do with this credit cards? - You can read the instructions [here](#).

BANK	CARD TYPE	QUANTITY	BALANCE	PRICE	ORDER
Bank of America	Visa Classic	1 card	1832.54 USD	0.0419 B	BUY NOW
Bank of America	Visa Gold	1 card	5390.00 USD	0.1216 B	BUY NOW
Bank of America	Visa Gold	1 card	2395.50 USD	0.0551 B	BUY NOW
Bank of America	Visa Classic	1 card	1583.21 USD	0.0338 B	BUY NOW
Bank of America	Visa Gold	1 card	2594.00 USD	0.0595 B	BUY NOW
JPMorgan Chase Bank	Visa Classic	1 card	980.00 USD	0.0223 B	BUY NOW



What You'll Uncover: Insider Threats

FRENCH BANK LOGS

Subscribe to this thread | print version

sw87

05.06.2017 01:38

Hi

byte

i want french bank log (BNP P

you can contact me on jabber

Group: User

Posts: 5

Registration: 05/06/2017

User No: 79 096

Activity: [other](#)

Reputation: [none](#) (0%)

ПРОФИЛЬ

ПМ

ЖАЛОБА

ВВЕРХ

sw87

05.05.2017 03:49

Hello,

I always look for a good worke

contact me pm and jabber.

thank you

byte

Group: User

Posts: 5

Registration: 05/06/2017

User No: 79 096

Activity: [other](#)

Reputation: [none](#) (0%)

ПРОФИЛЬ

ПМ

ЖАЛОБА

ВВЕРХ

Lampeduza Republic Constitution Vendors Escrow Private Note Services

Sign Out

The Republic of Lampeduza International Dumps, Cards, Workshop

Lampeduza Republic Official Domains: [Lampeduza.so](#) - [Lampeduza.La](#) - [Lampeduza.bz](#)

Need **[REDACTED]** Uk Insider

Started By Taggz, Feb 21 2015 06:26 PM

No replies to this topic

Taggz

Posted 21 February 2015 - 06:26 PM

Looking for a **[REDACTED]** instore insider, contact me for more information.

Legionarius

Posts: 40

Number: 22444



What External Exposures Are Threats To You?

- 1) Data leakage: strategic IP, customer & employee data, etc.
- 2) Malware-as-a-service, software exploits, phishing kits
- 3) Stolen and counterfeit products, gift cards, credit cards
- 4) Brand attacks: rogue apps, social media weaponization
- 5) Doxxing and digital extortion, Exec/VIP targeting
- 6) Compromised credentials, account takeover
- 7) Phishing attacks and domain squatting
- 8) Insider threats – hiring and coordination
- 9) Third-party and IT vendor risk



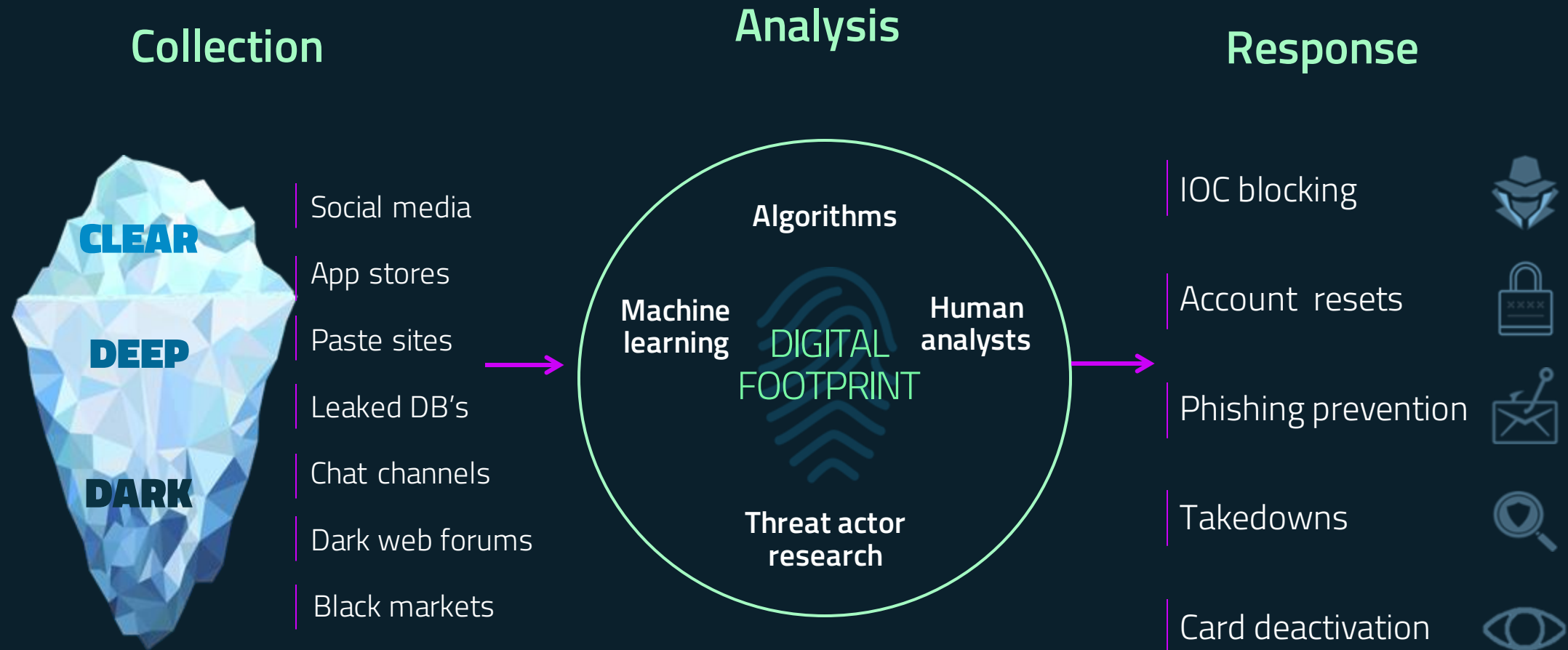
**WHAT ARE
YOU
LOOKING AT?**



Tailor threat
intelligence to your
business.



Tailor Your Threat Intelligence In Three Phases



Automate Your Response

- Execute takedown processes
 - Social networks
 - Mobile app stores
 - Registrars, domain hosting providers
- Streamline card deactivations, password resets, reprovisioning
- Automate credential validation checks and protocols
- Integrate endpoint, gateway, and perimeter defenses
- Prepare digital extortion decision trees, run scenario analyses



Agenda

- The Dark Web: What's At Stake
- Gain Visibility, Take Control
- **Leveraging Splunk & Phantom**
- Key Recommendations

The Emergence Of Phishing Kits

1)



Website cloned

2)



Credential-stealing
script run from login
page

3)



Credentials
collected in bulk

4)



Zip file uploaded
and unpacked for
reuse

5)

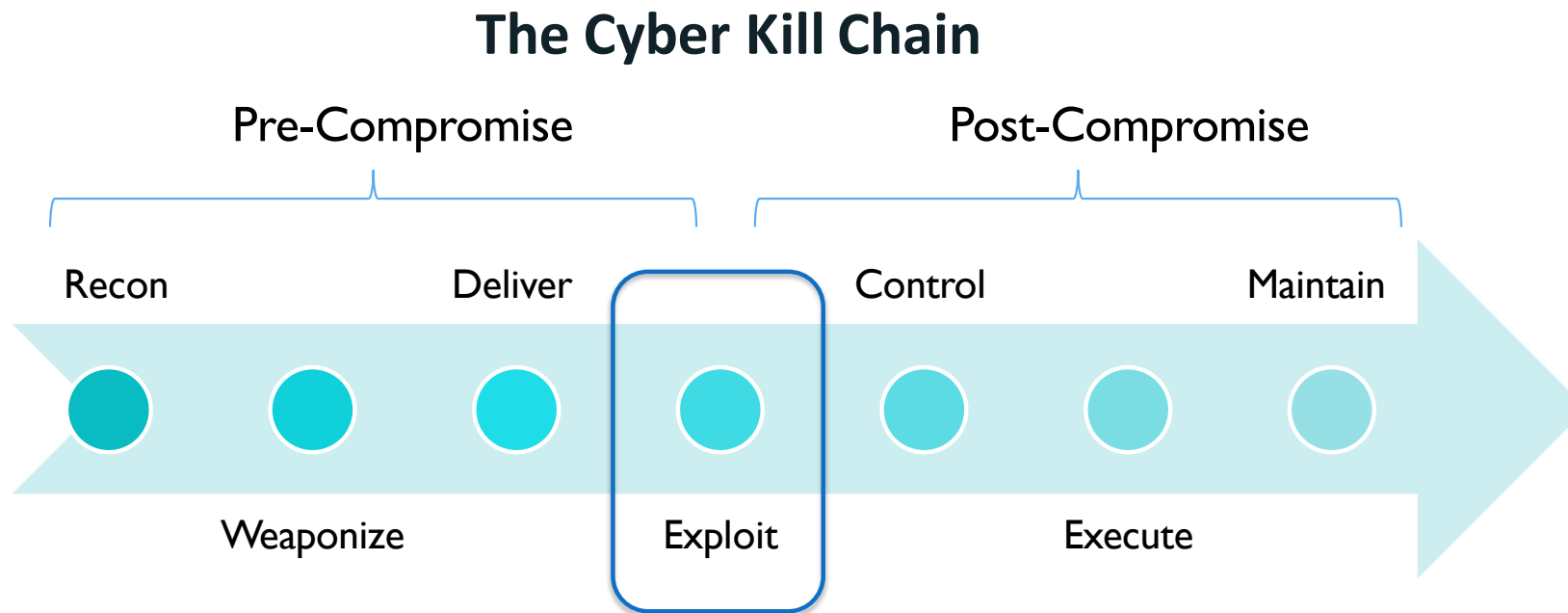


New phishing
campaign w/ spoofed
website

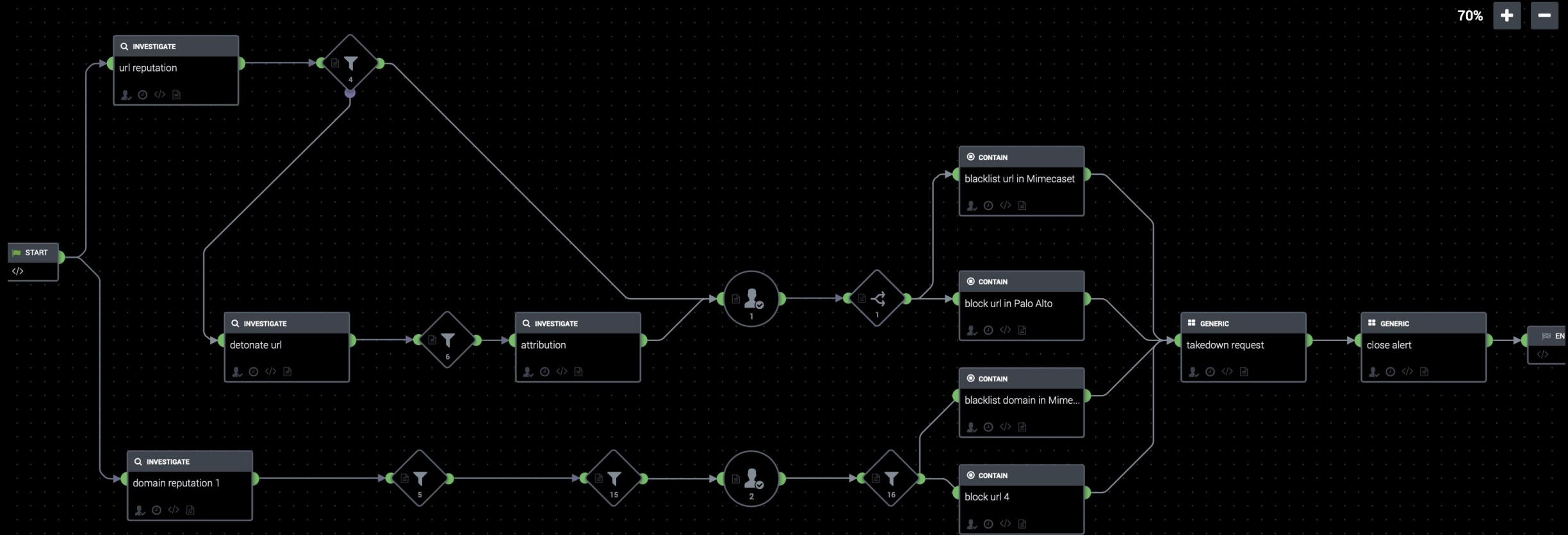


Shutdown Phishing Early In Attack Chain, Pre-Exploit

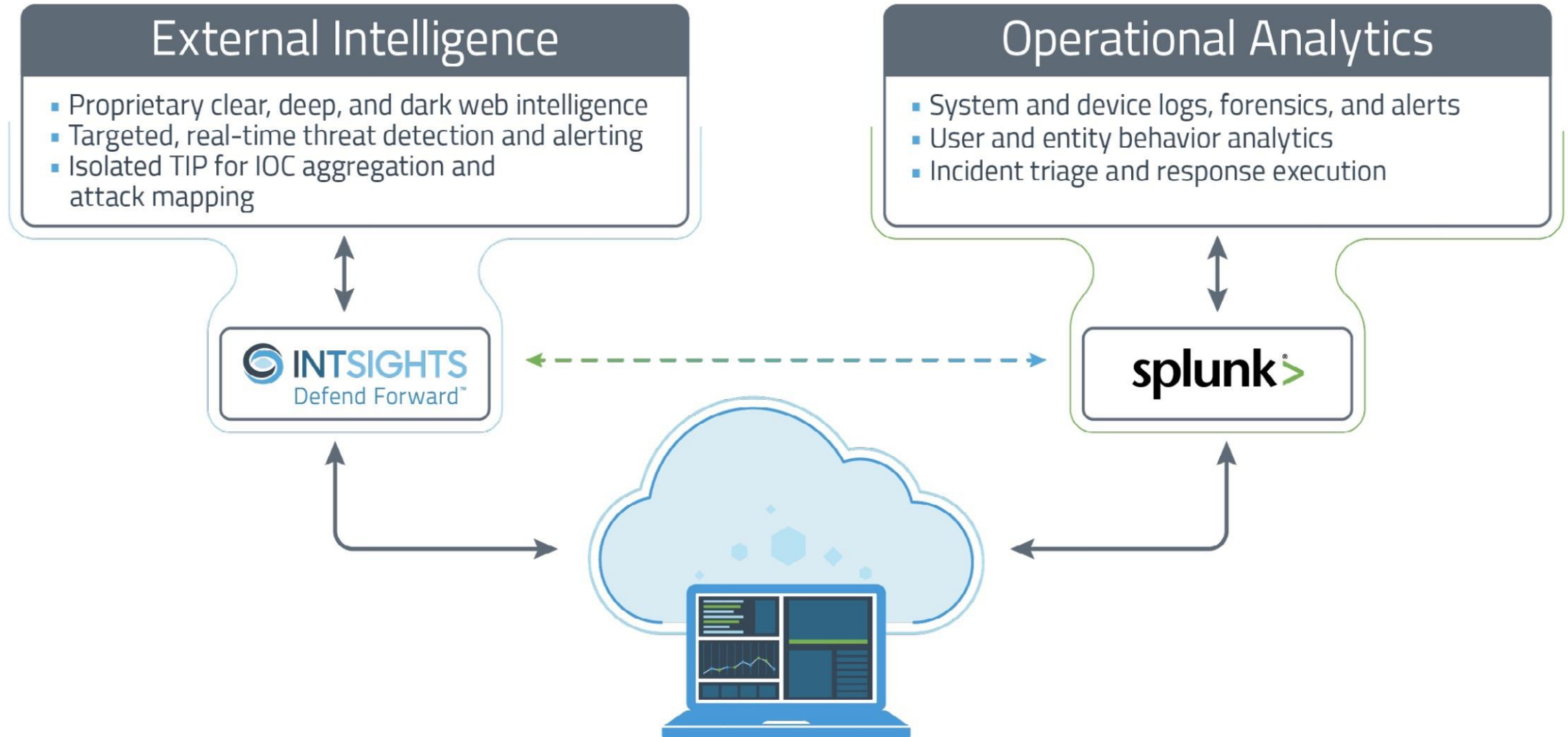
- Monitor suspicious domains *before* they're activated.
- Automate the takedown process.



Phantom Playbook: Phishing Detect & Respond



Splunk + IntSights For 360° Visibility



Agenda

- The Dark Web: What's At Stake
- Gain Visibility, Take Control
- Leveraging Splunk & Phantom
- **Key Recommendations**

Embedding ETI Into Your Security Program

- What immediate challenges do we want to solve?
- Where are our assets & exposures? What do attackers see?
- What can we integrate or automate to improve our remediation? Internally and externally?
- How can we leverage threat intelligence in the long-term?
- What are expected outcomes in 6 months, 1 year, 3 years?



Recommendations

- 1) External threat intel improves SecOps – but only if it's actionable and contextualized to your organization.
- 2) Define use-cases upfront; start with one or two.
- 3) Neutralize threats on their territory; mitigate risk pre-exploit.



Thank You!



Nick Hayes
VP, Strategy

nick.hayes@intsights.com
[@nickhayes10](https://twitter.com/nickhayes10)

Get a [live demo](#) at Booth #158!