INTSIGHTS
Defend Forward™

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

October 23, 2019

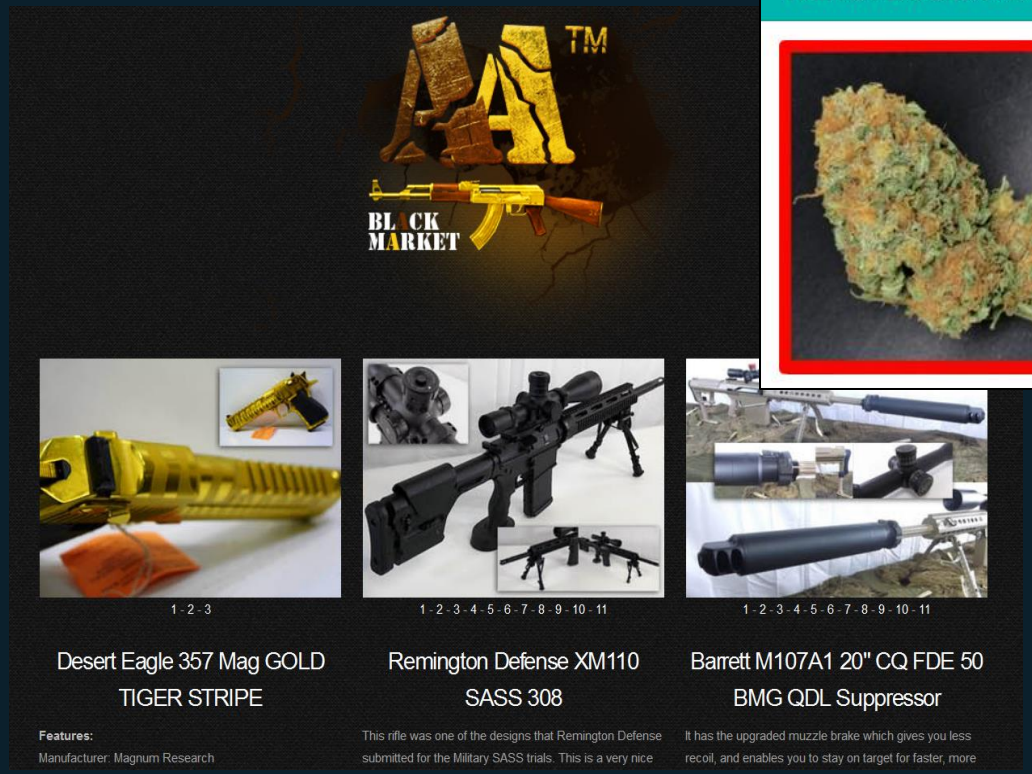
Agenda

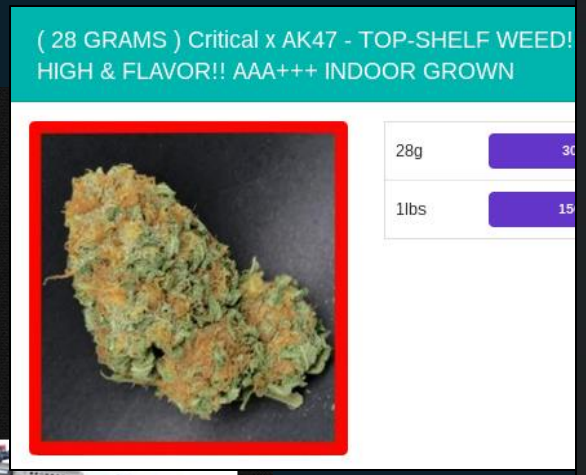
- The Dark Web: What's At Stake
- Gain Visibility, Take Control
- Leveraging Splunk & Phantom
- Key Recommendations

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?





The Clear, Deep, and Dark Web

Clear Web

- Search engines
- Media, blogs, etc.

Deep Web

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

Dark Web

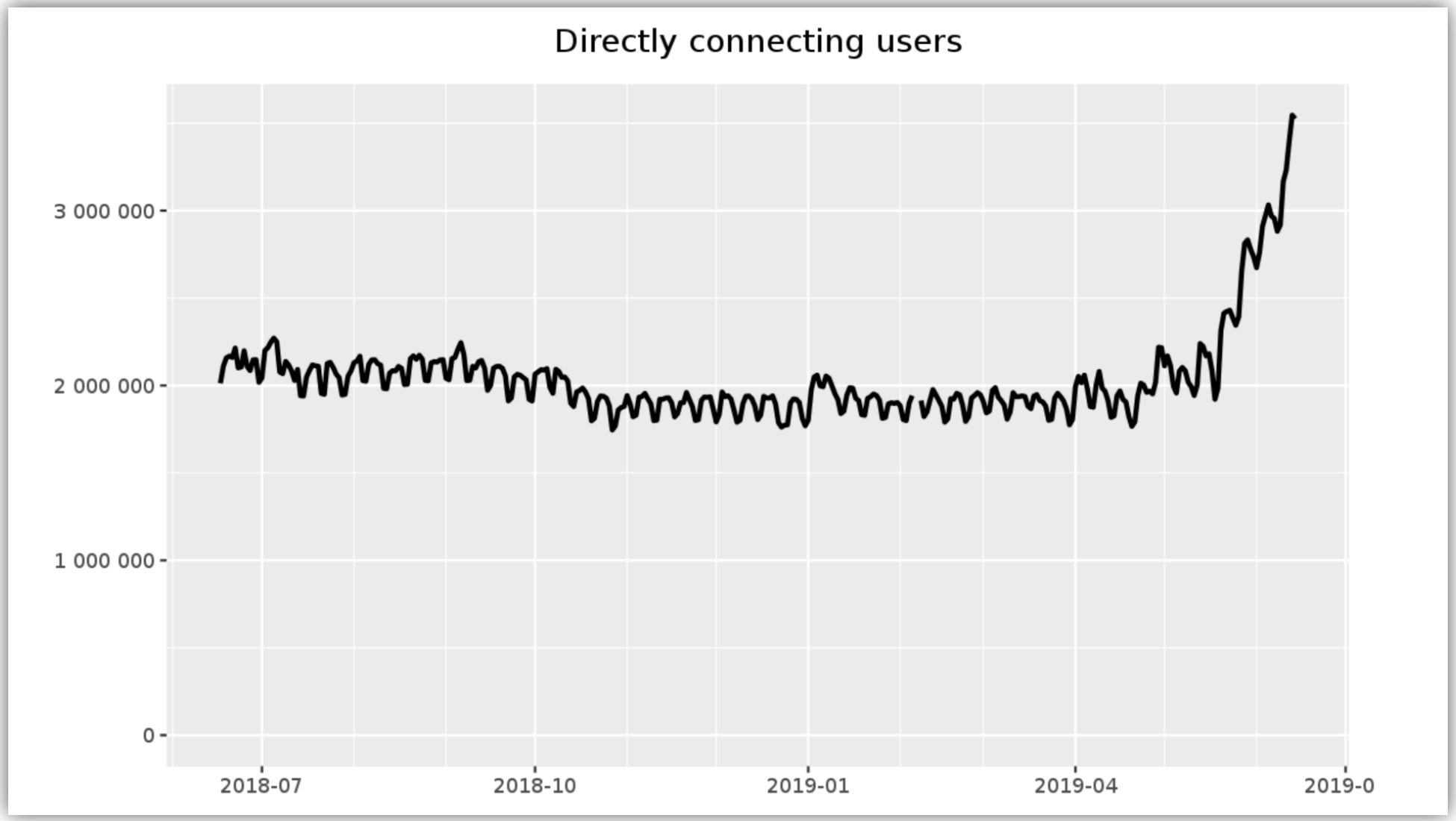
- Anonymous, closed sources, Telegram groups, invite-only (sometimes)
- Tor, P2P, hacker forums, criminal marketplaces, C2s, etc.

How Tor Works

User's TOR client picks a random path to destination server.

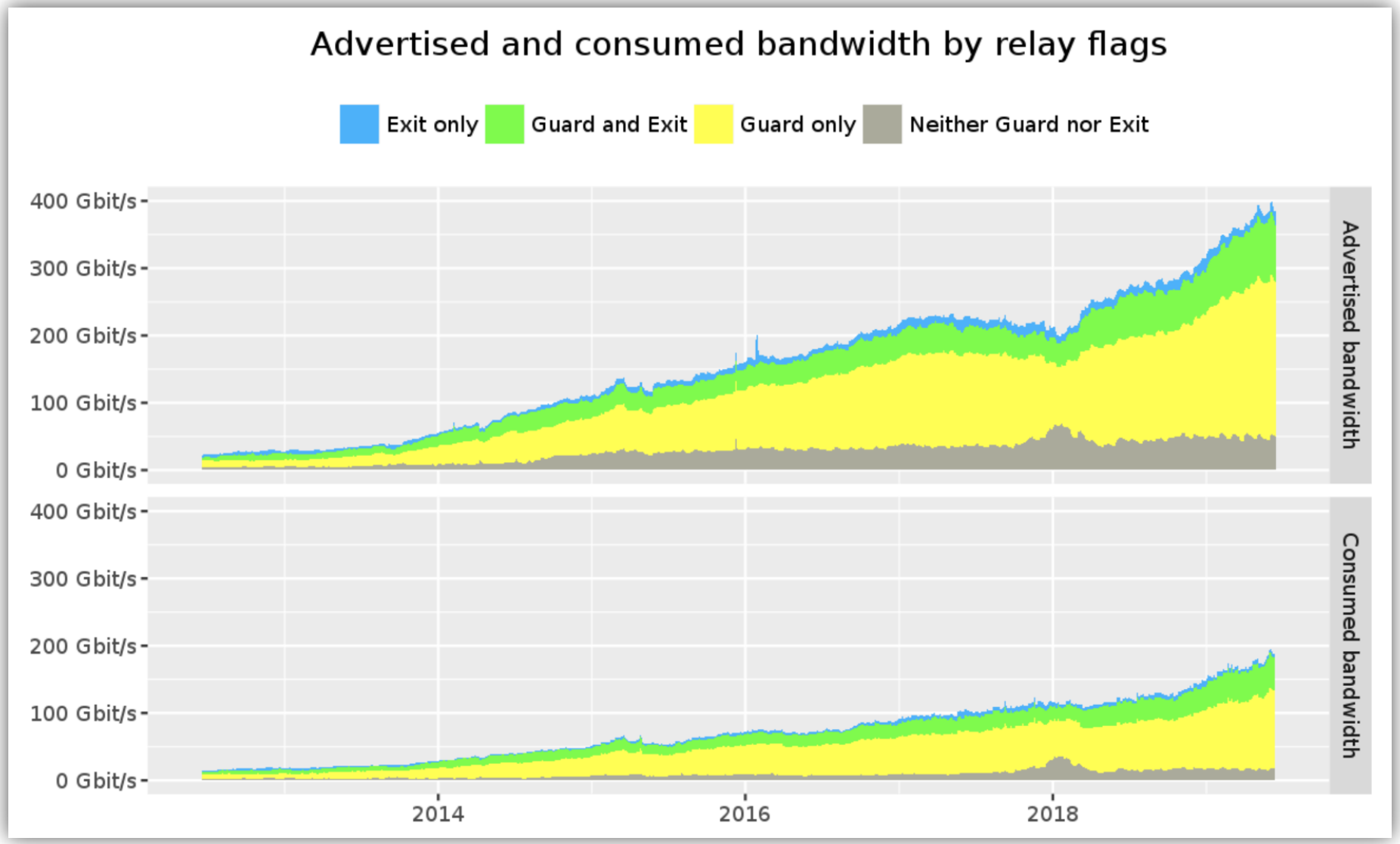
RED links are encrypted
BLUE links are in the clear.

Tor Usage Statistics



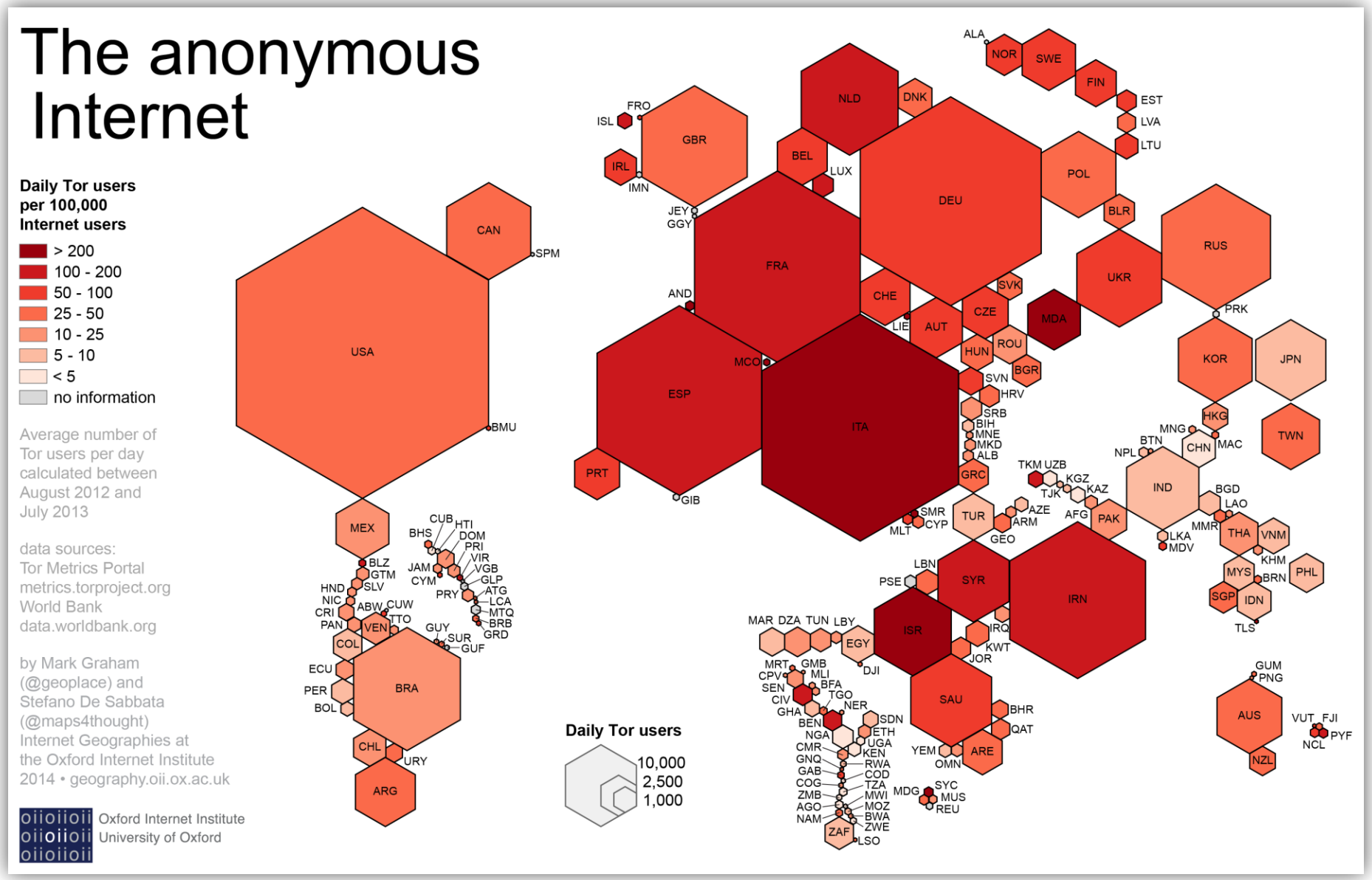
Source: The Tor project – https://metrics.torproject.org/

Tor Usage Statistics

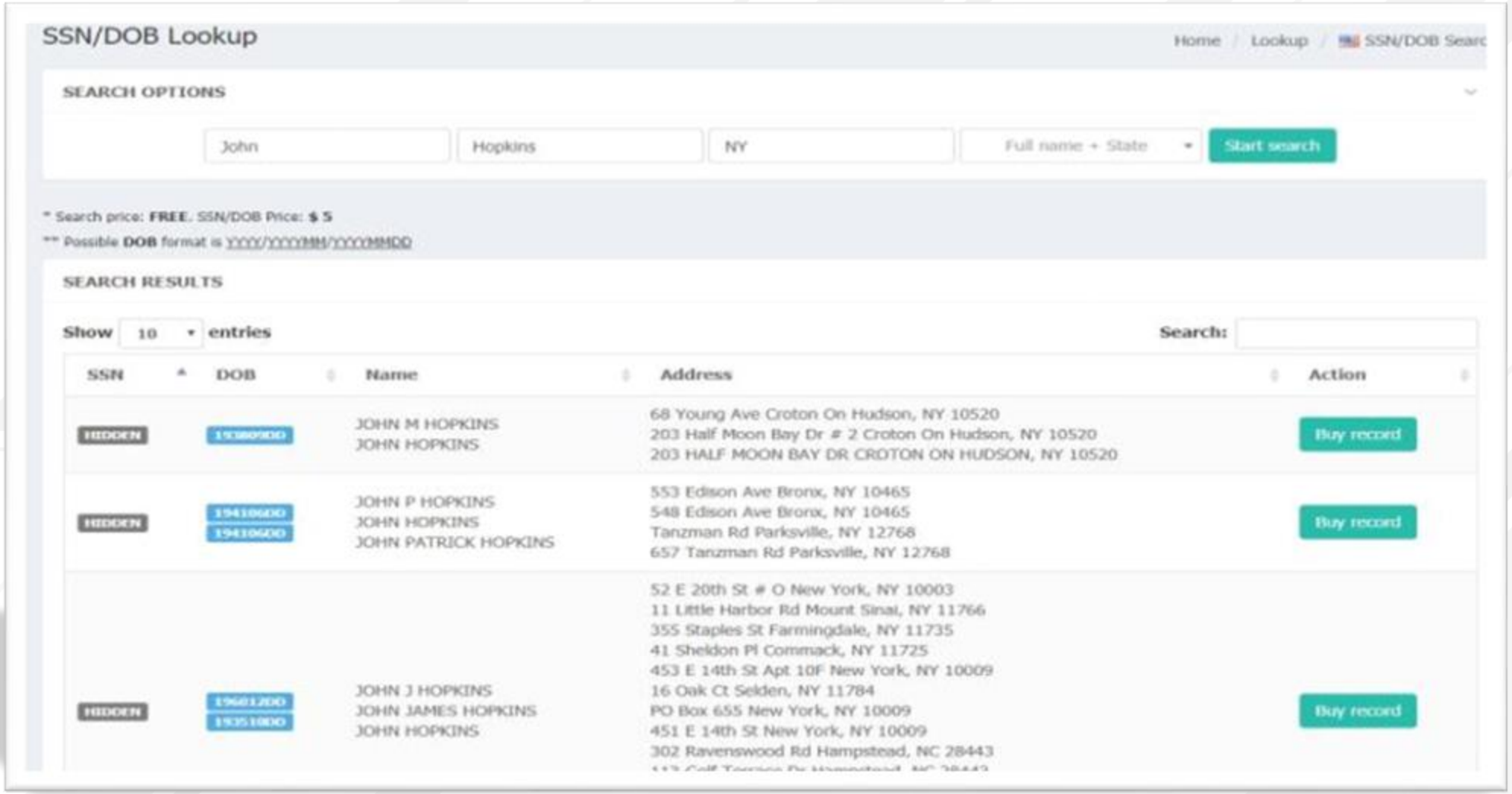


Source: The Tor project – https://metrics.torproject.org/

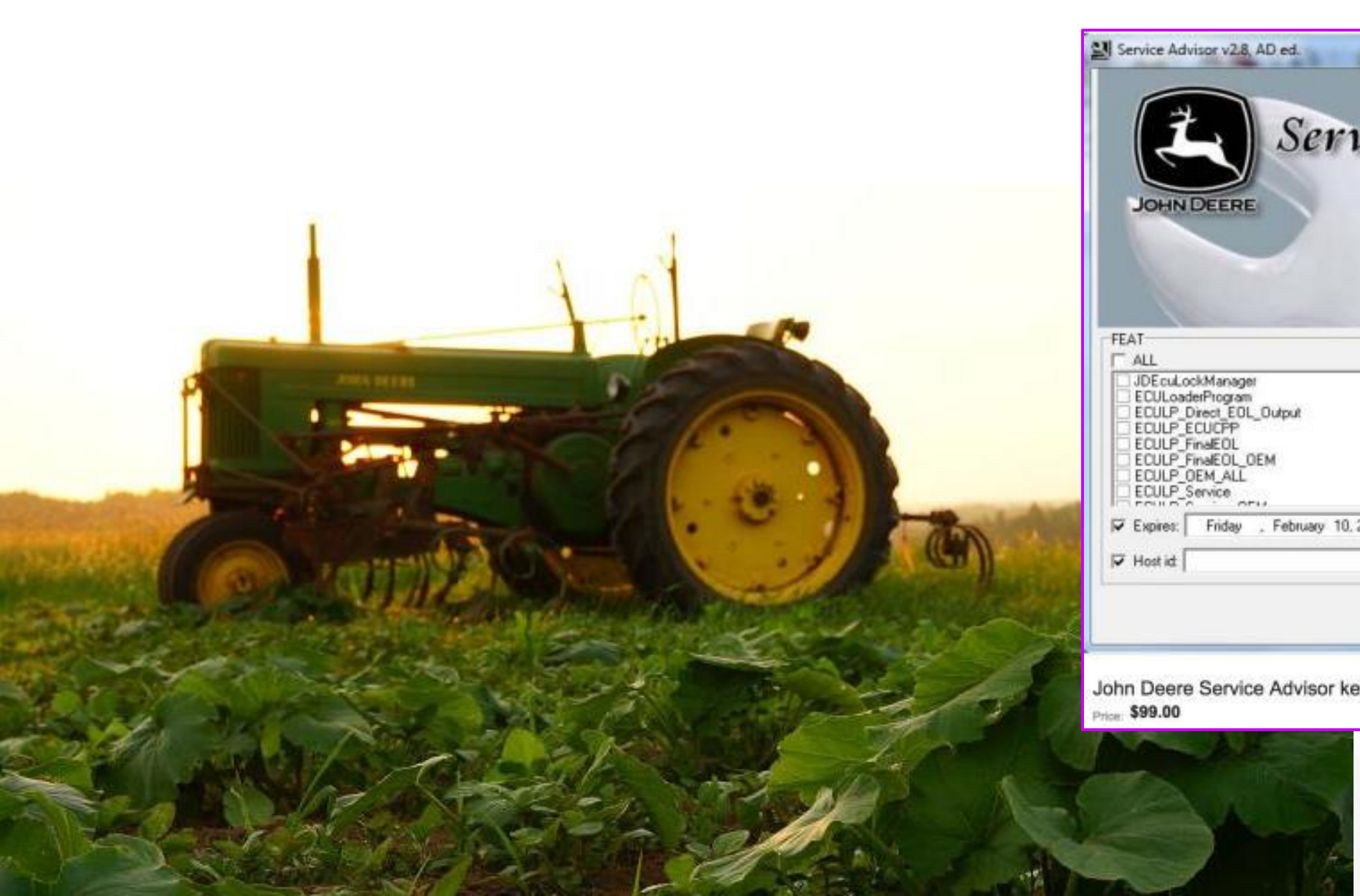
Tor Usage Statistics



The User Experience Can Match Legitimate Sites



Even Farmers Turn To The Dark Web



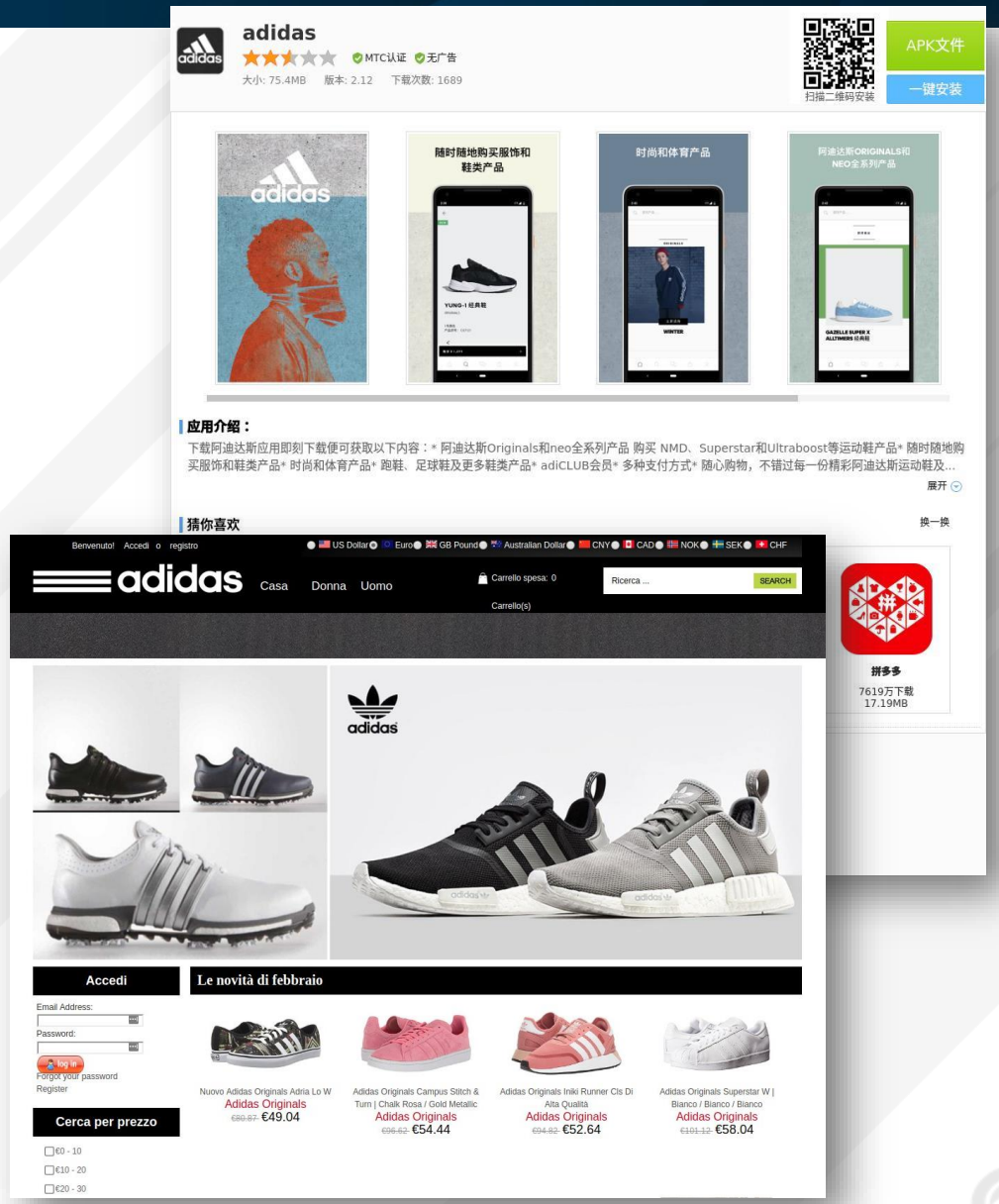
Threats are mounting

278% Products for sale on black markets

297% Phishing websites

171% Compromised employee credentials

149% Stolen credit cards for sale on dark web



Agenda

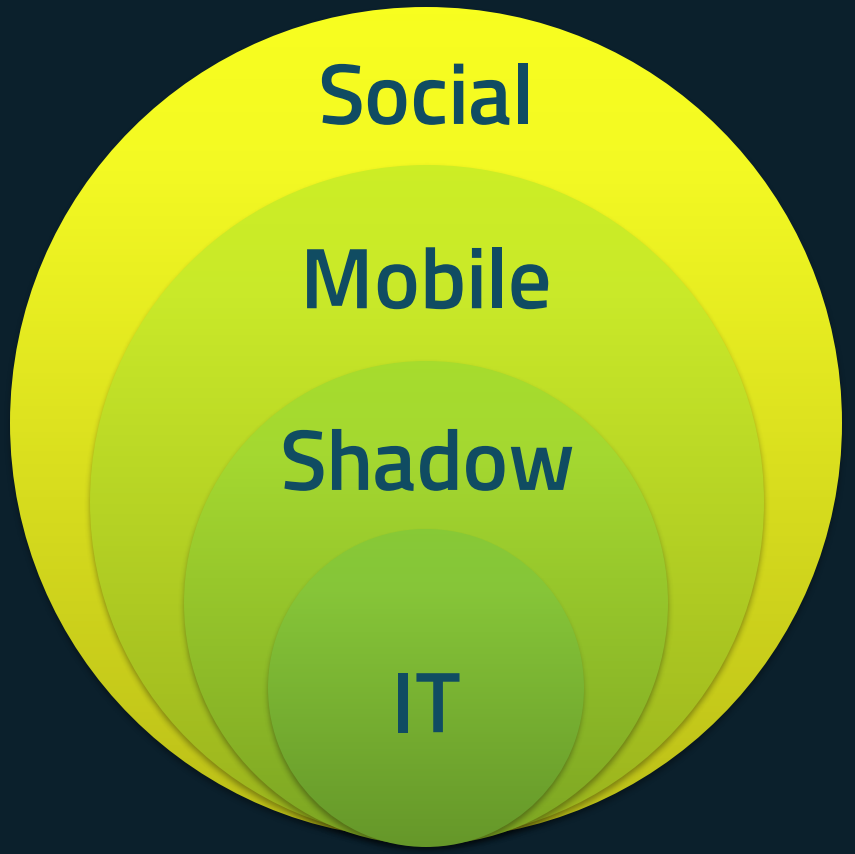
- The Dark Web: What's At Stake
- **Gain Visibility, Take Control**
- Leveraging Splunk & Phantom
- Key Recommendations

Our attack surface keeps growing

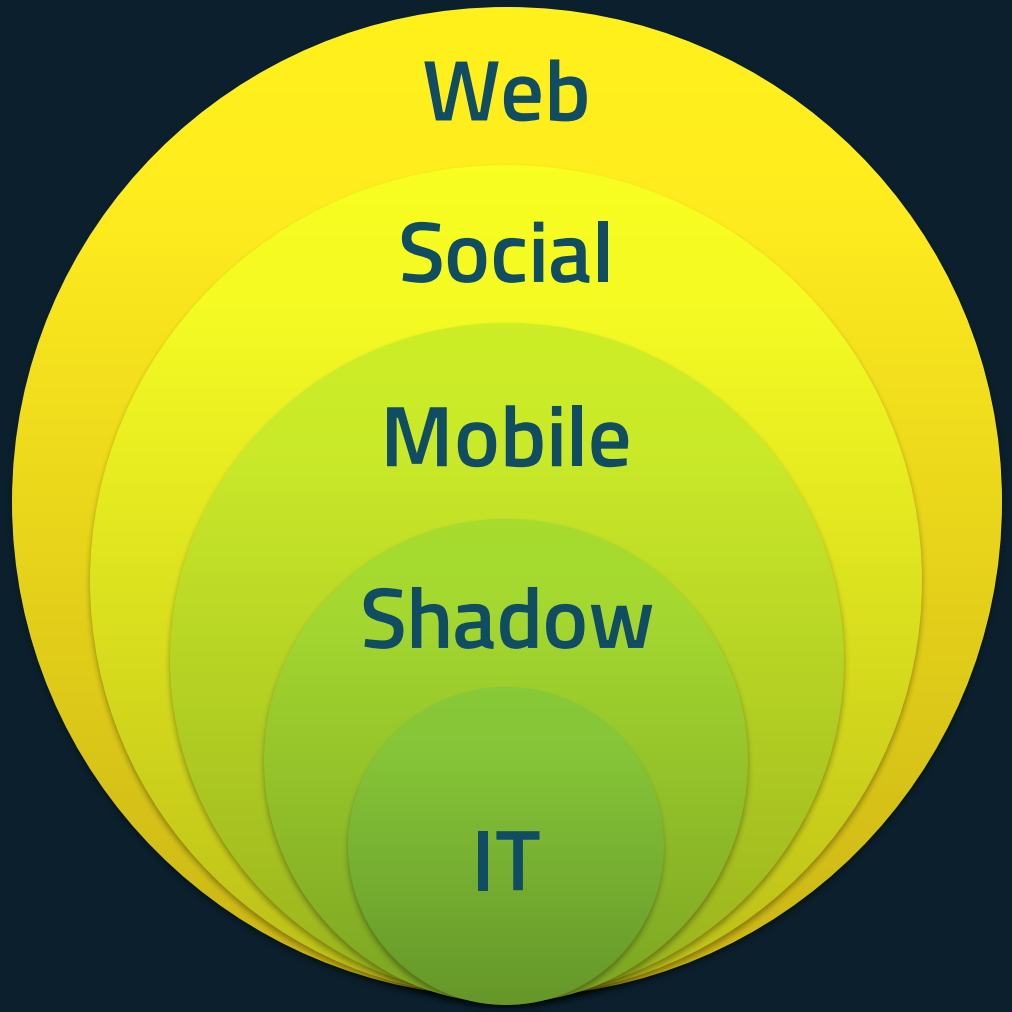
Our attack surface keeps growing

Our attack surface keeps growing

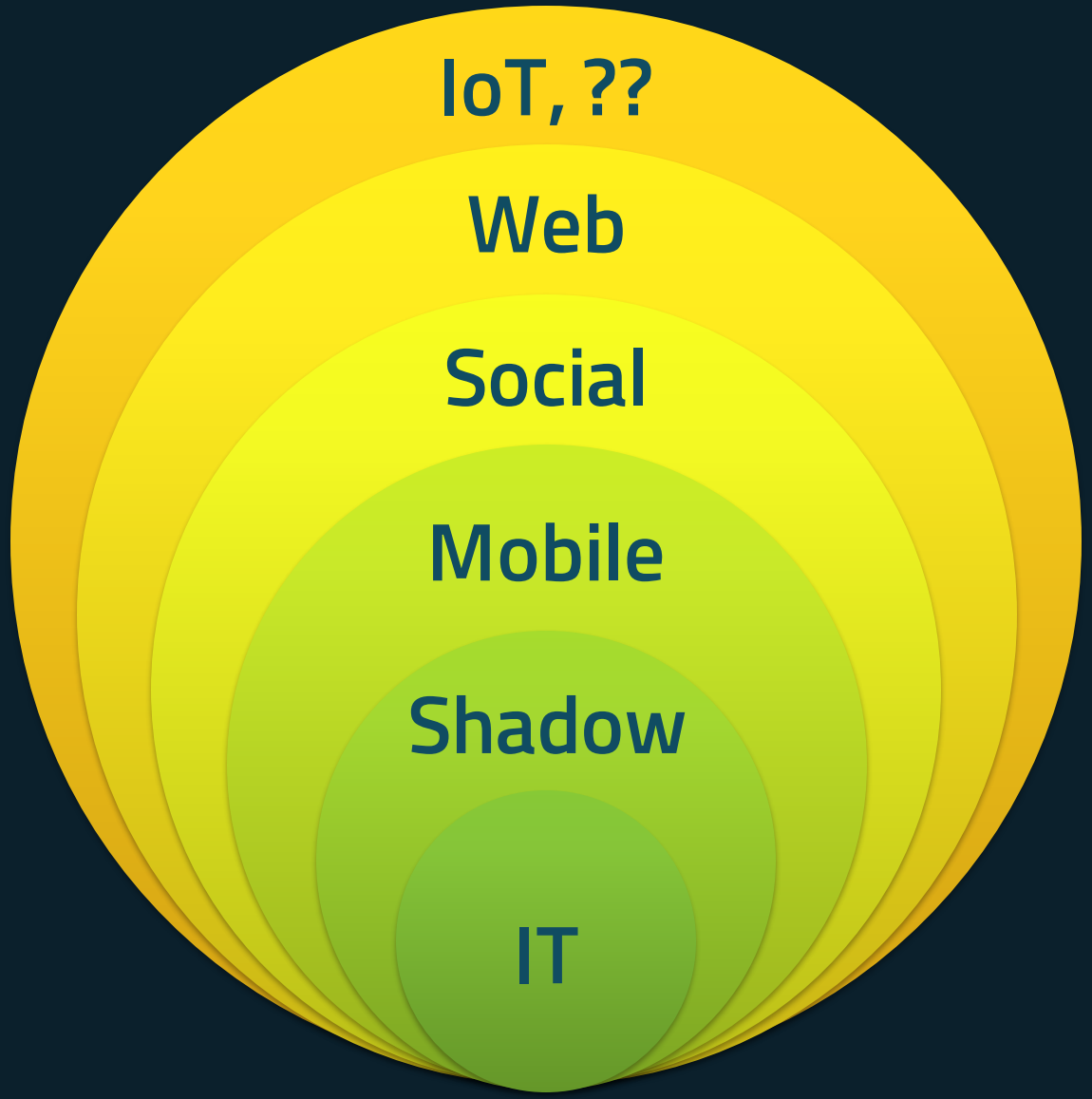
Our attack surface keeps growing



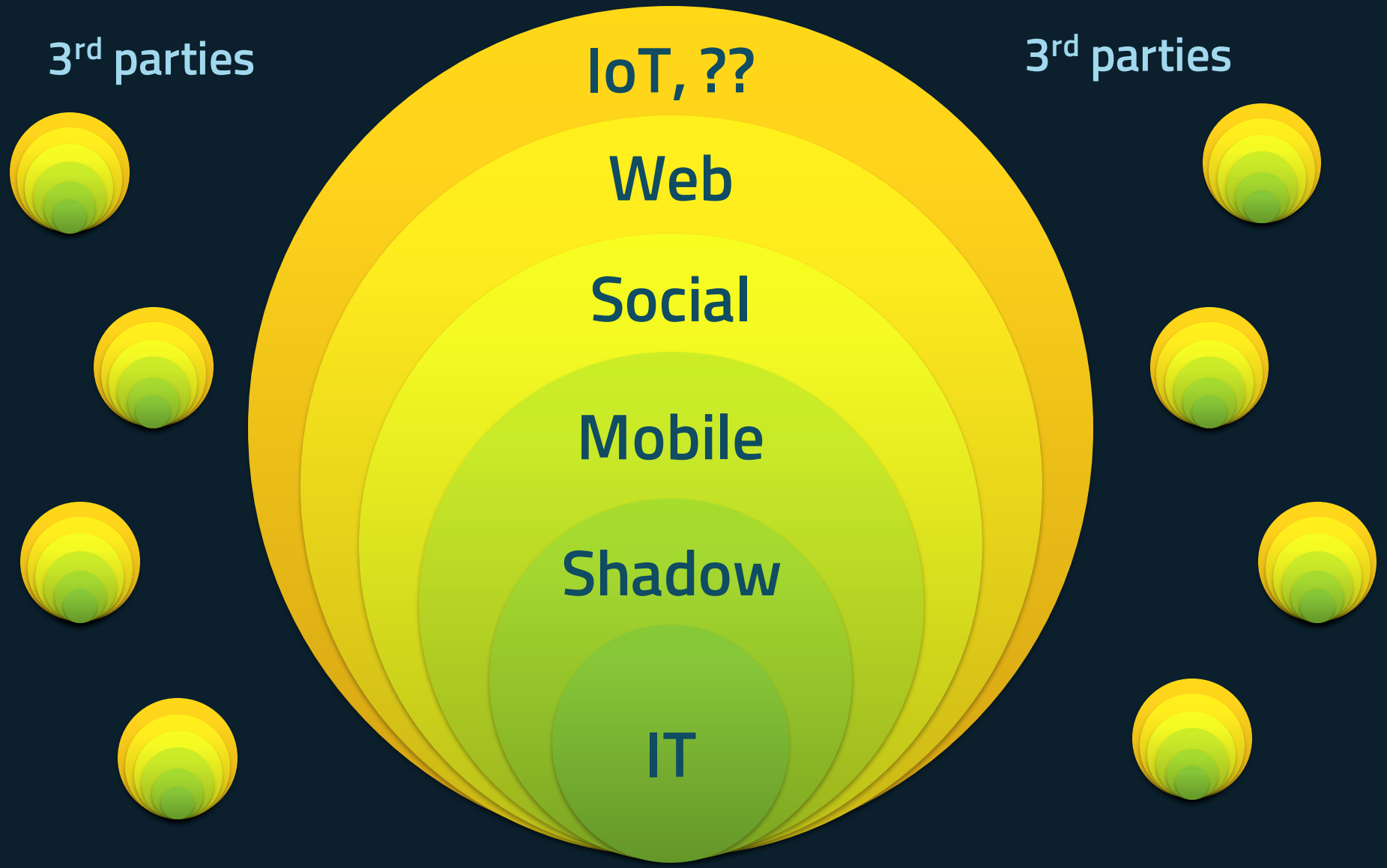
Our attack surface keeps growing



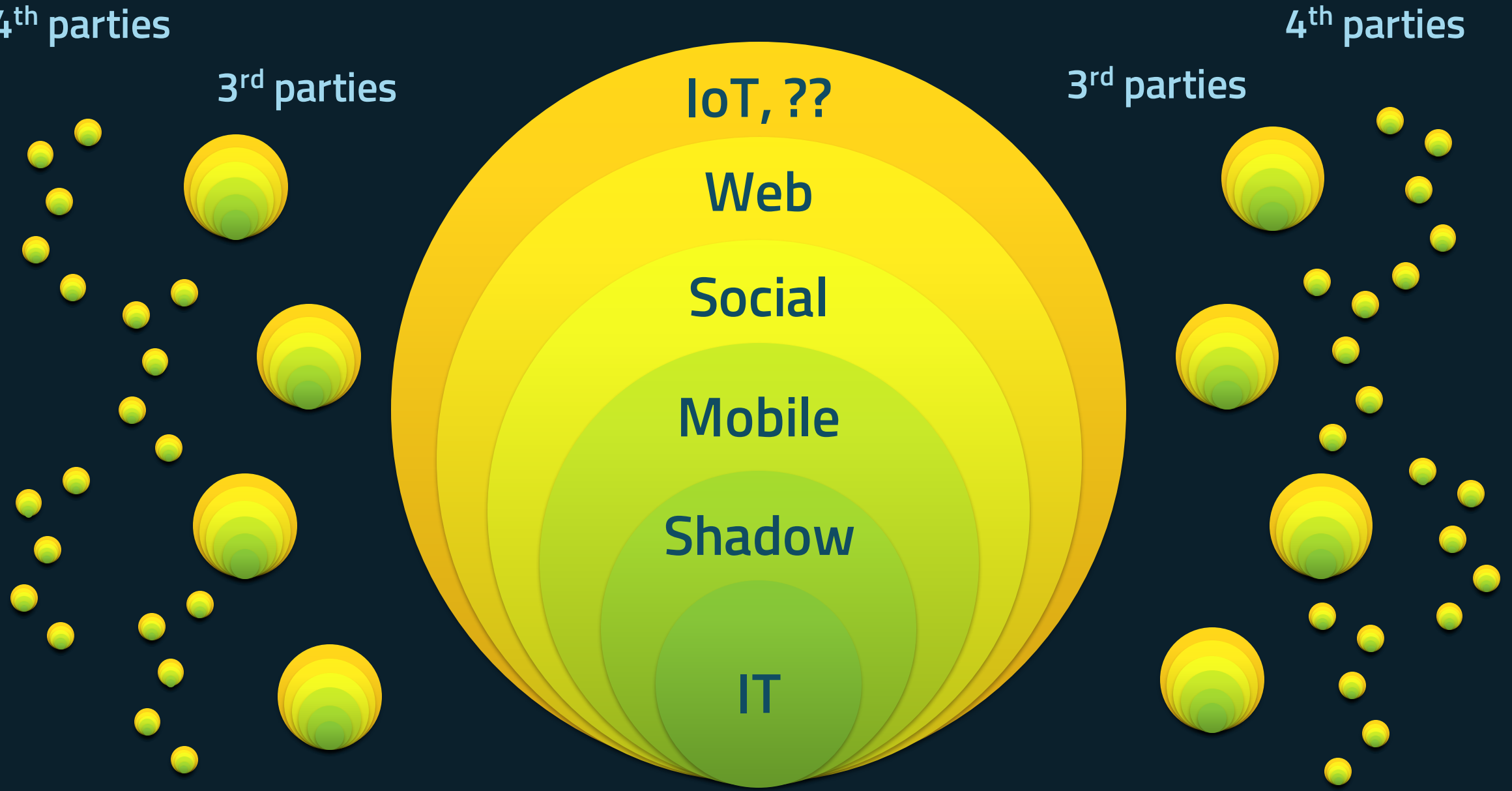
Our attack surface keeps growing



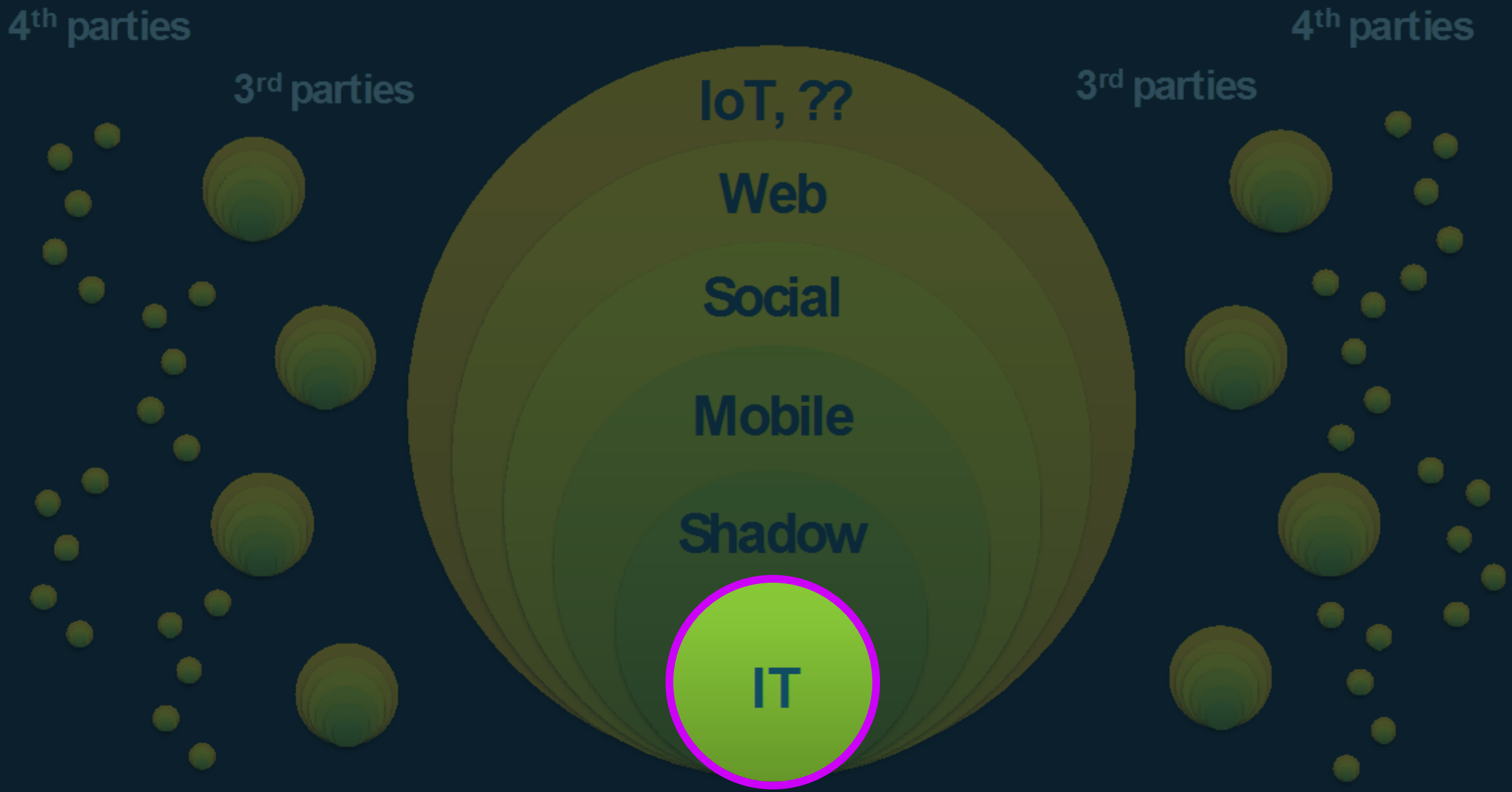
Our attack surface keeps growing



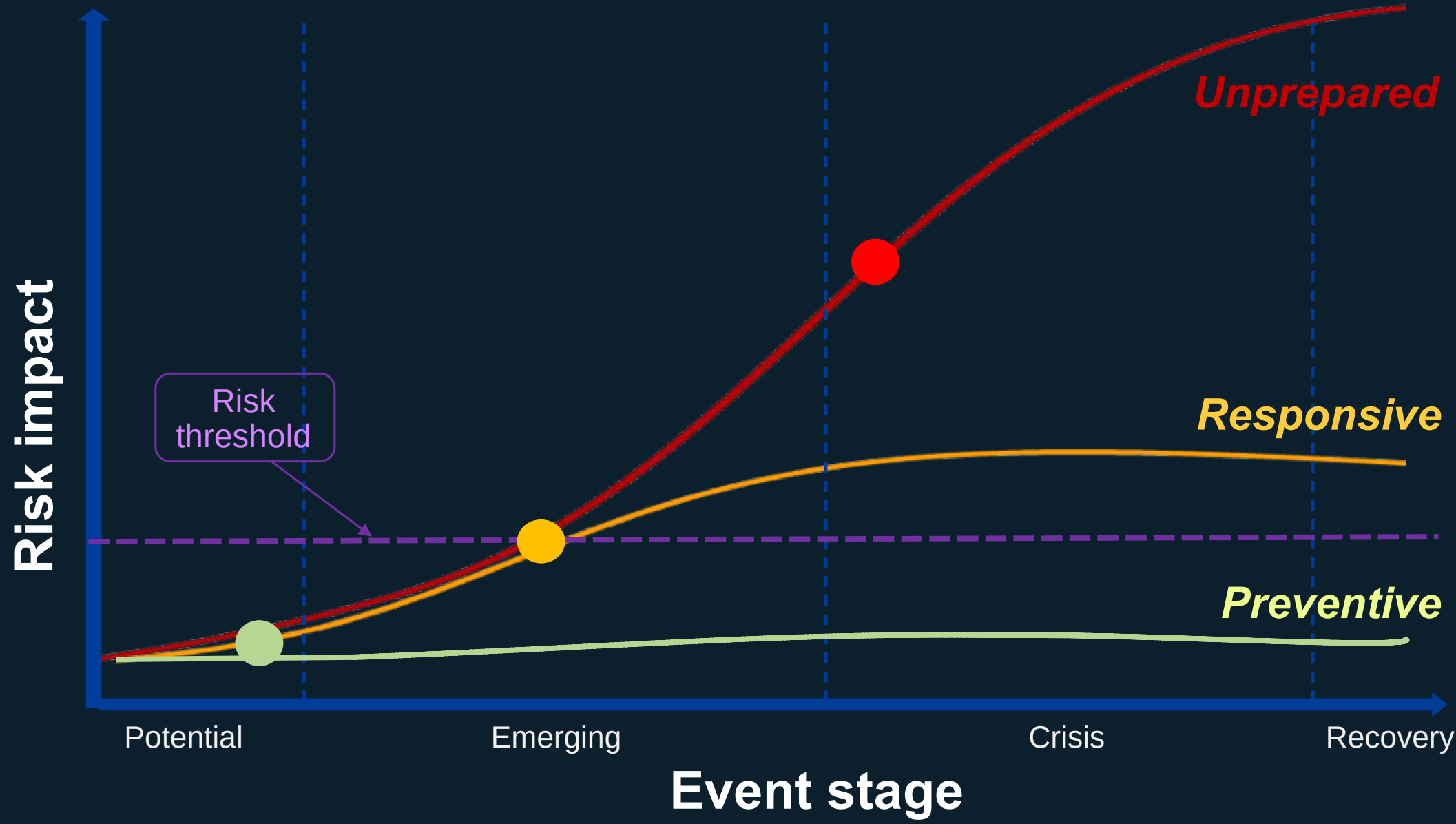
Our attack surface keeps growing



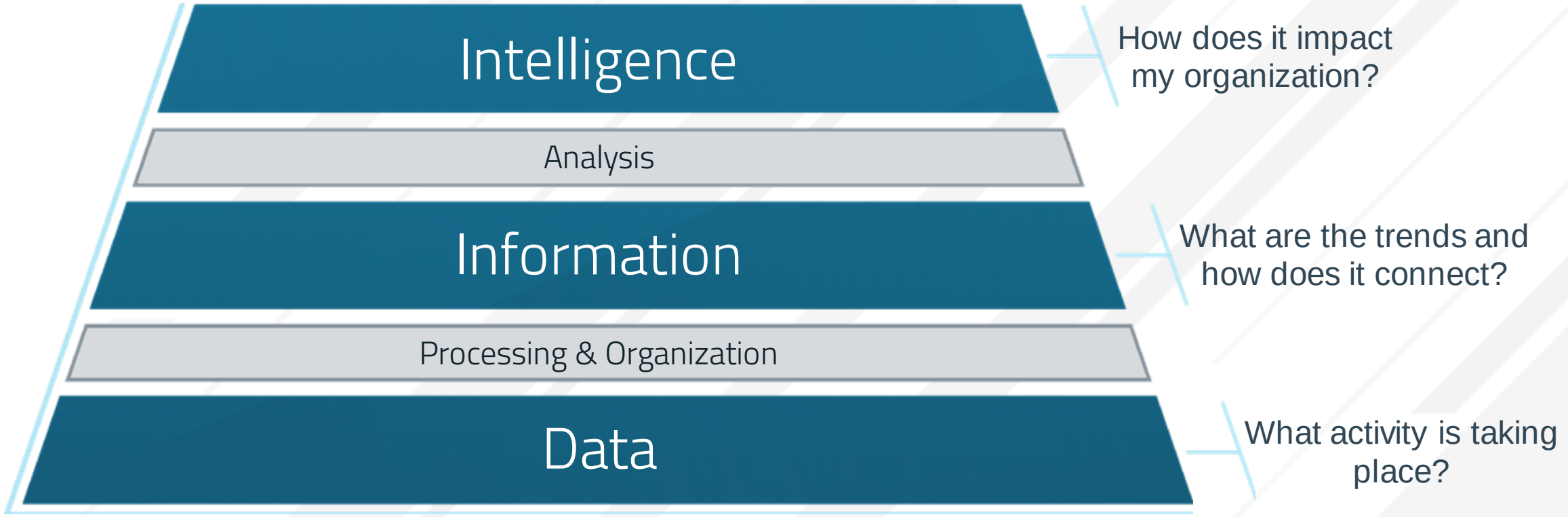
Lack Of *Visibility*, Lack Of *Control*



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:9F840EA6E04B22541
anna_	anna	secure.whitepages.com:DEF6EC19237202C11
stacy	stacy	:secure.whitepages.com:DED6863937FD1DE41
stacy	stacy	:www.whitepages.com:0645FE59D8C00A264
tom	tom	:secure.whitepages.com:EDD913E5BA52F9621
robert	robert	secure.whitepages.com:2CD2BEADC6368D281
robert	robert	':www.whitepages.com:6DAECEE7DA5802884
sue	sue	secure.whitepages.com:8EF60451C7A816201
yaneke	yanek	:secure.whitepages.com:371F12B58A683C981

Employee credentials

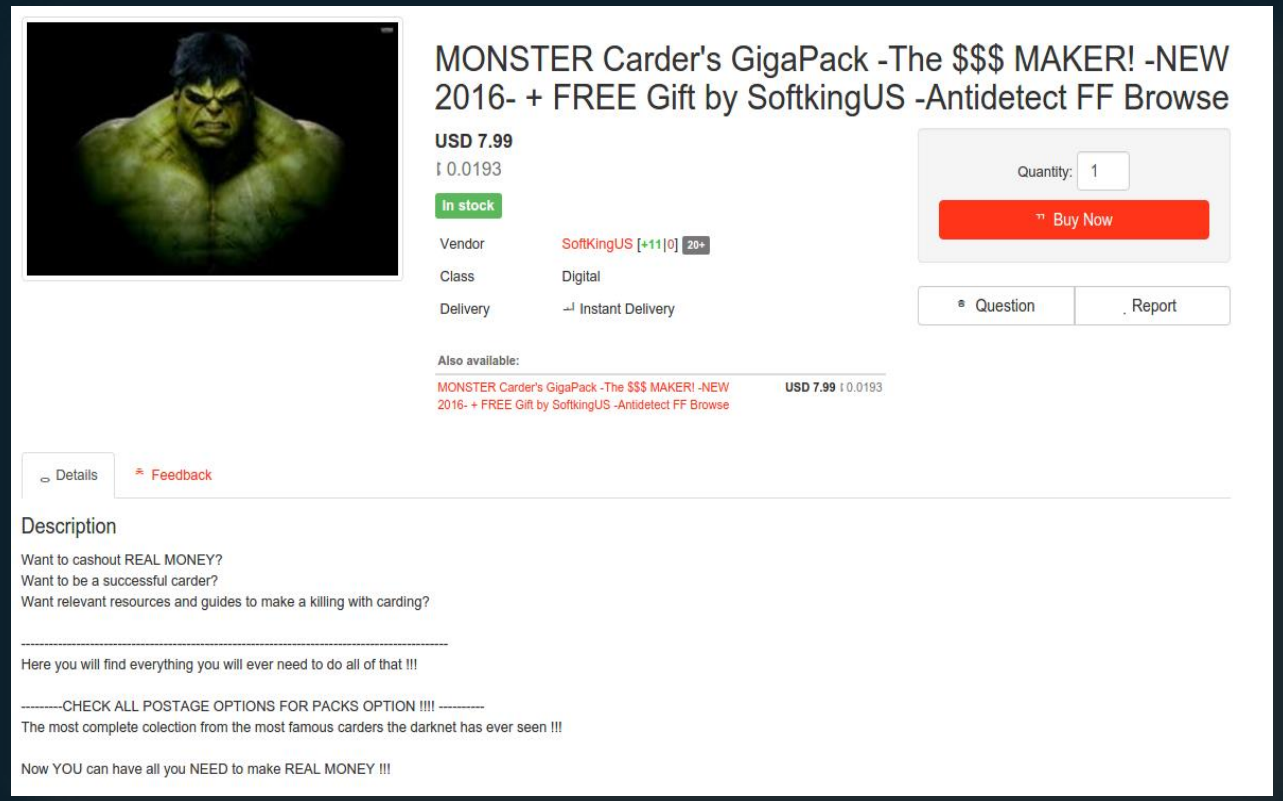
Shop	Balance	Points	Type	Country	CC	Bank	Info	Last order	Mail access	Seller	Price ($):
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[illegible]	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: ( [illegible] ...)
. Balance 3000$ = 150$
. Balance 5000$ = 250$
. Balance 8000$ = 400$
. Balance 12000$ = 600$
. Balance 15000$ = 800$

* Bank UK: ( [illegible] ...)
. 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

Ł 0.0193

In stock

Quantity: 1

Buy Now

Vendor	SoftKingUS [+11|0] 20+
Class	Digital
Delivery	Instant Delivery

Question | Report

Also available:

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

Details | Feedback

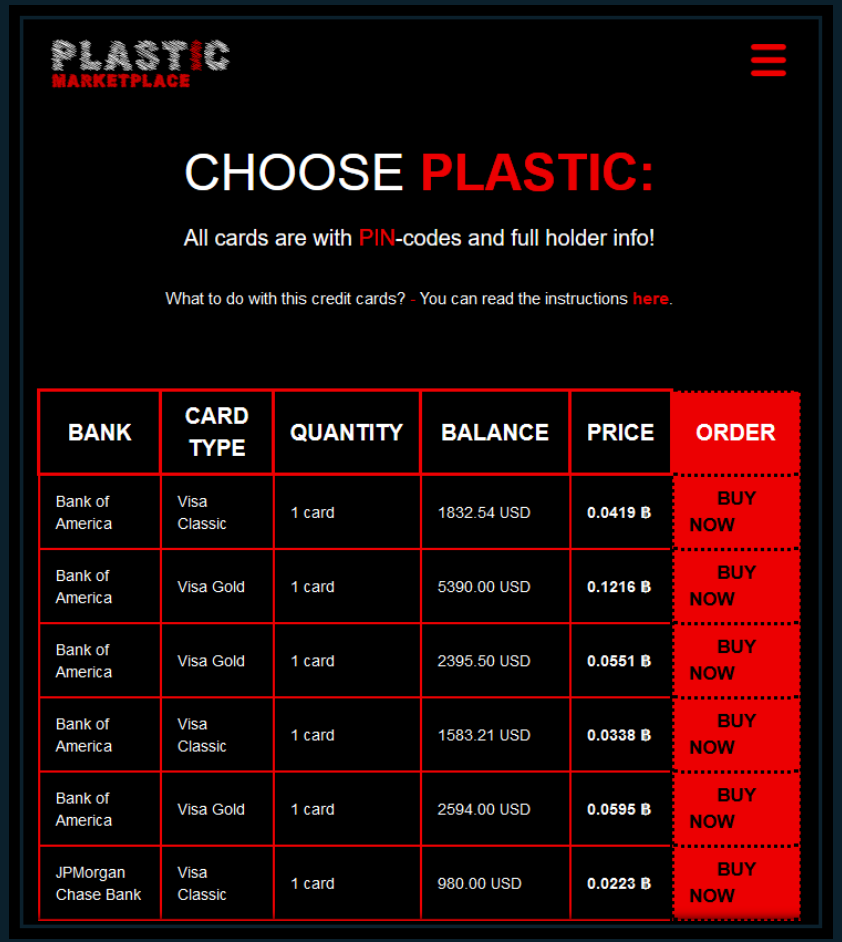
Description

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

Here you will find everything you will ever need to do all of that !!!

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

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



PLASTIC MARKETPLACE

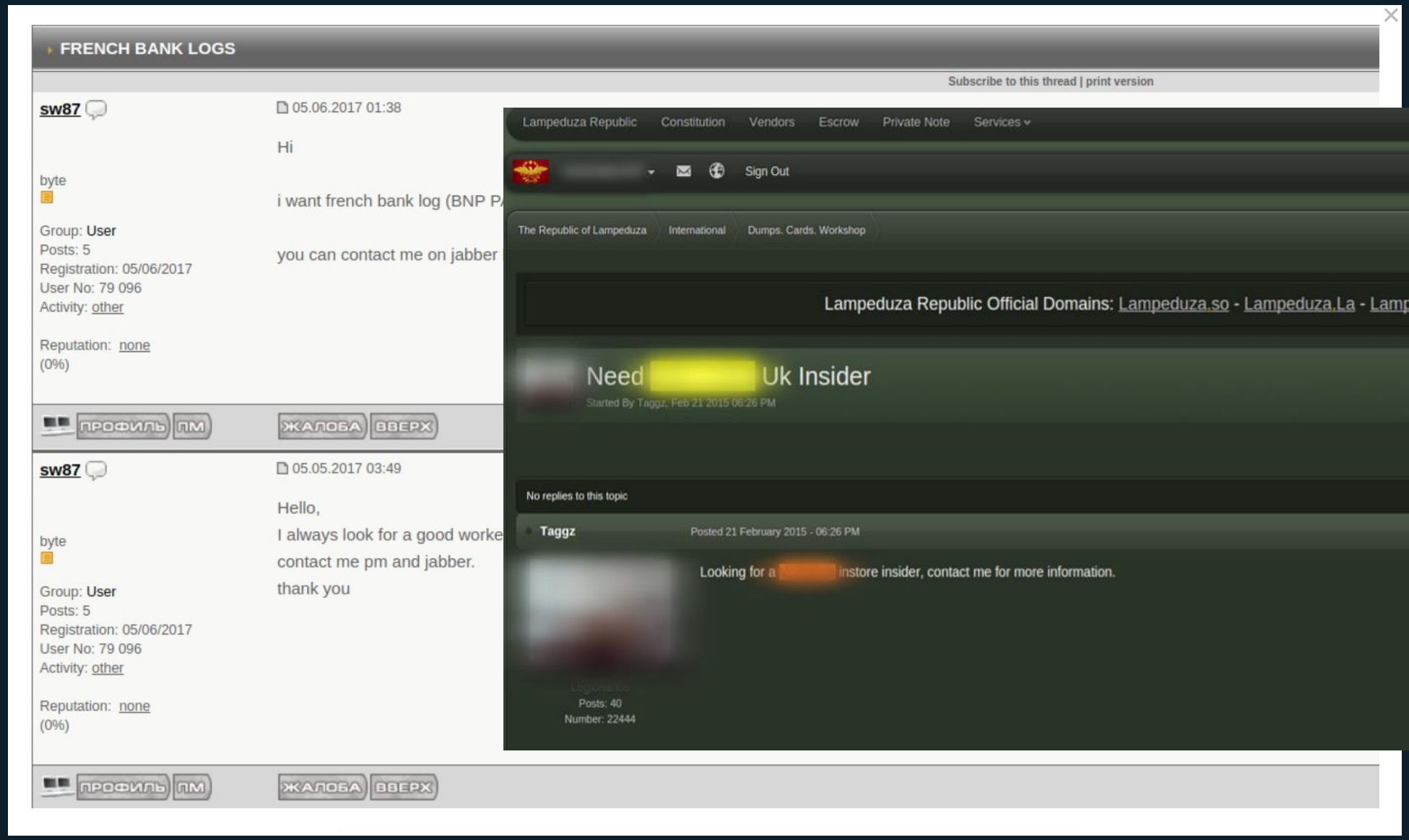
CHOOSE PLASTIC:

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 Ƀ**	BUY NOW
Bank of America	Visa Gold	1 card	5390.00 USD	**0.1216 Ƀ**	BUY NOW
Bank of America	Visa Gold	1 card	2395.50 USD	**0.0551 Ƀ**	BUY NOW
Bank of America	Visa Classic	1 card	1583.21 USD	**0.0338 Ƀ**	BUY NOW
Bank of America	Visa Gold	1 card	2594.00 USD	**0.0595 Ƀ**	BUY NOW
JPMorgan Chase Bank	Visa Classic	1 card	980.00 USD	**0.0223 Ƀ**	BUY NOW

What You'll Uncover: Insider Threats



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

Collection

- Social media
- App stores
- Paste sites
- Leaked DB's
- Chat channels
- Dark web forums
- Black markets

Analysis

Algorithms

Machine learning

DIGITAL FOOTPRINT

Human analysts

Threat actor research

Response

- IOC blocking
- Account resets
- Phishing prevention
- Takedowns
- Card deactivation

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)

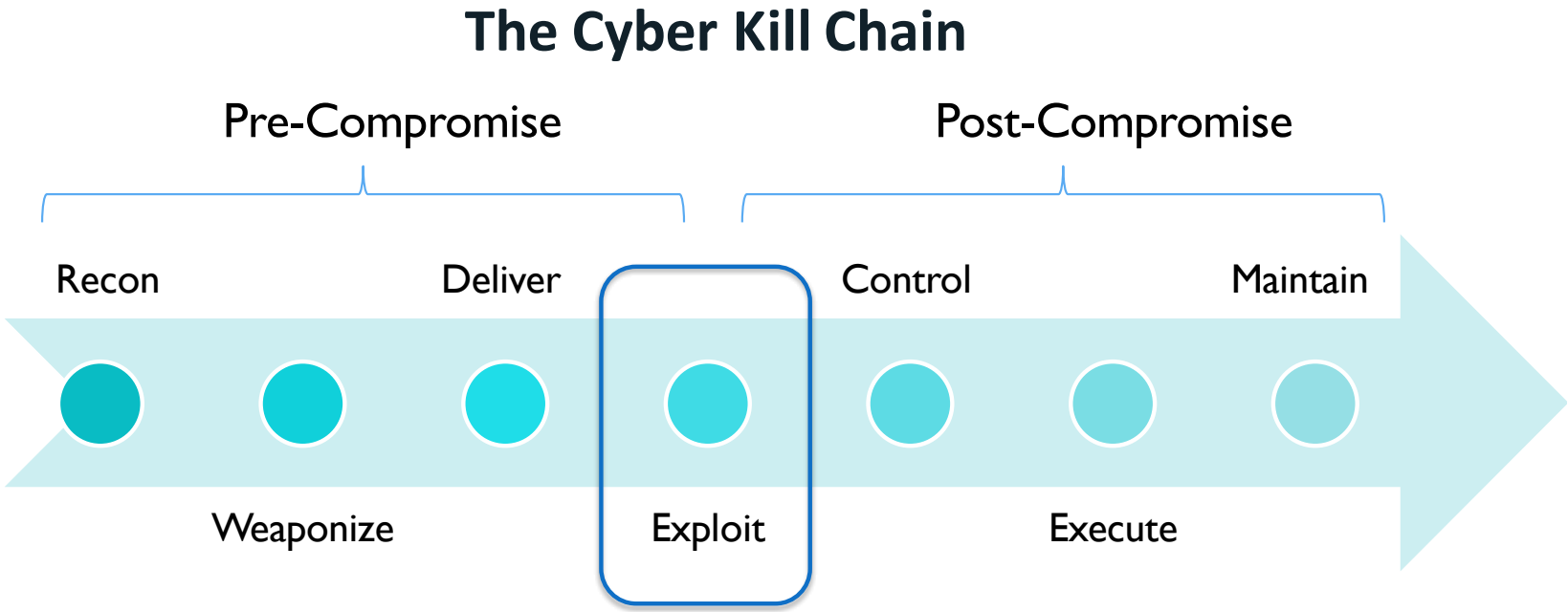
Zip file uploaded and unpacked for reuse

5)

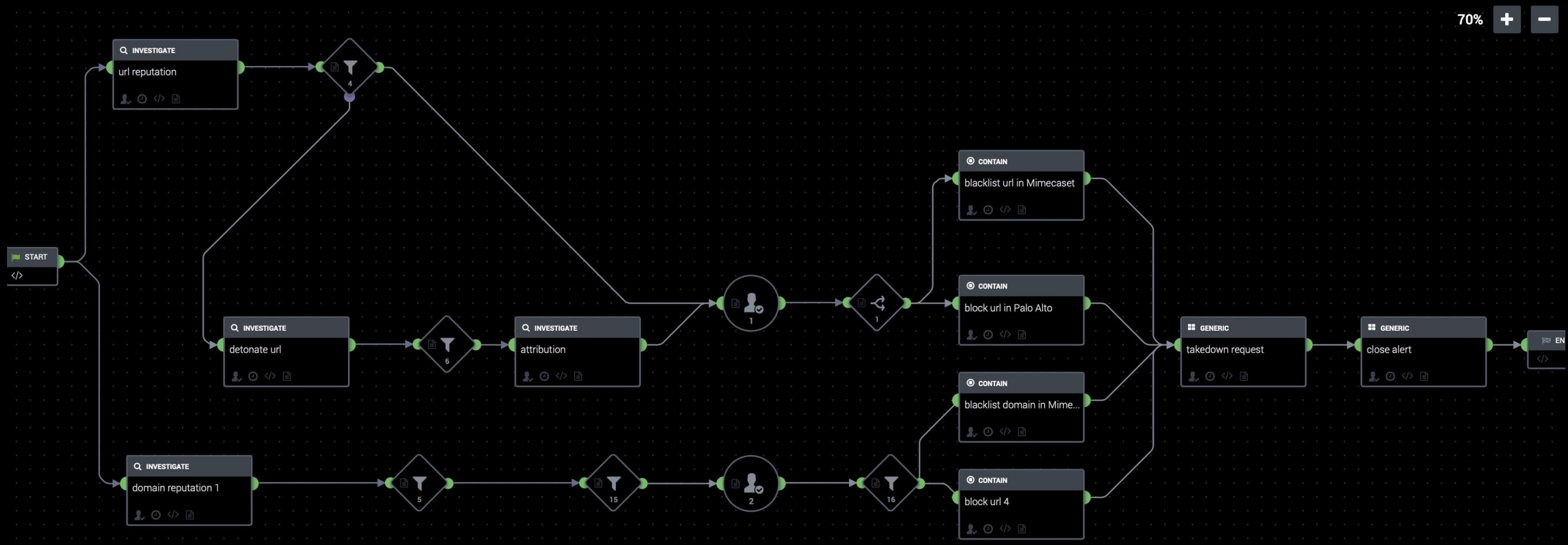
New phishing campaign w/ spoofed website

Shutdown Phishing Early In Attack Chain, Pre-Exploit

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



Phantom Playbook: Phishing Detect & Respond



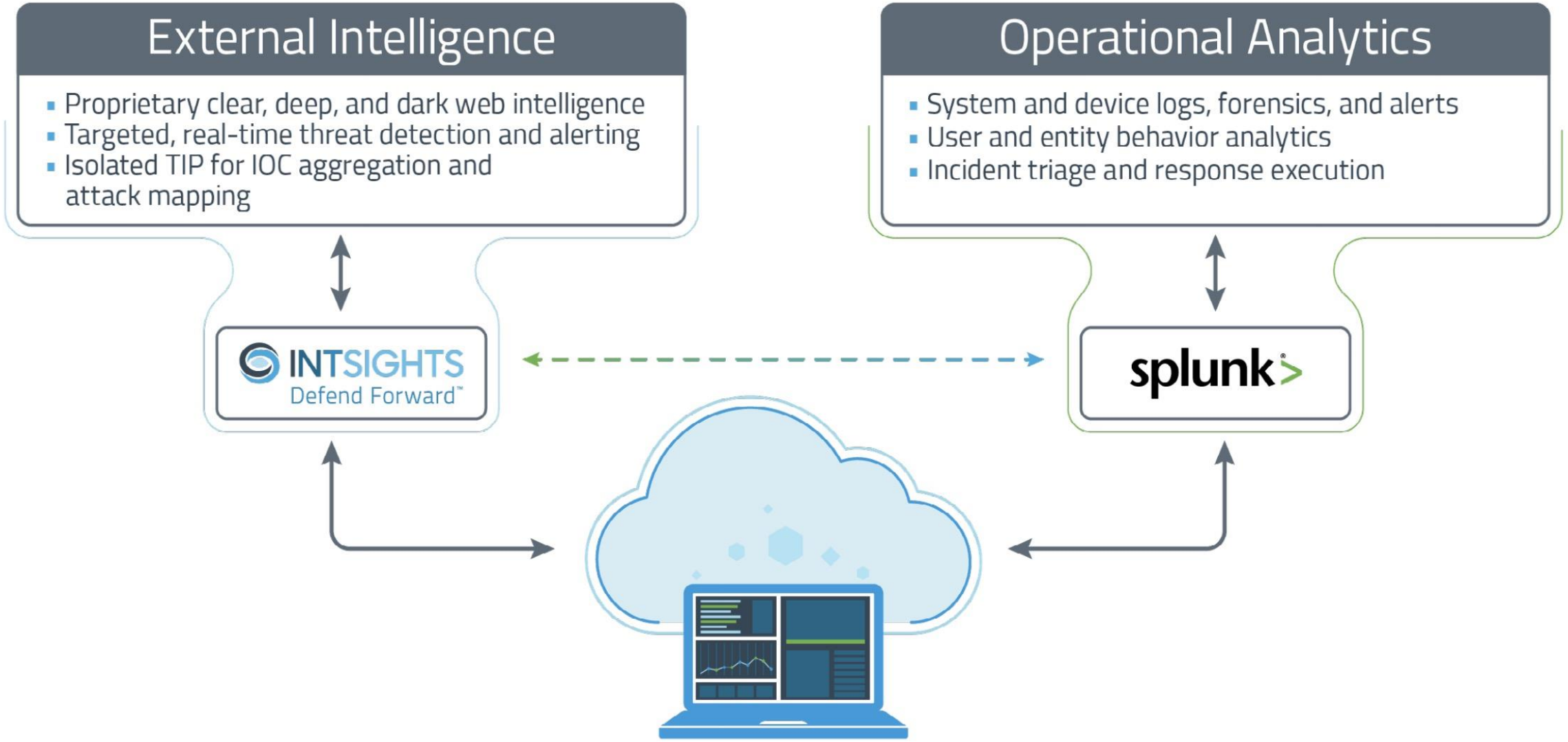
Splunk + IntSights For 360° Visibility

External Intelligence

- Proprietary clear, deep, and dark web intelligence
- Targeted, real-time threat detection and alerting
- Isolated TIP for IOC aggregation and attack mapping

Operational Analytics

- System and device logs, forensics, and alerts
- User and entity behavior analytics
- Incident triage and response execution



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.

INTSIGHTS
Defend Forward™

Thank You!

Nick Hayes
VP, Strategy

nick.hayes@intsights.com
@nickhayes10

Get a live demo at Booth #158!