RSAConference2019

San Francisco | March 4–8 | Moscone Center

SESSION ID: STR-T07

The Digital Risk Dilemma
How To Protect What You Don't Control

Nick Hayes

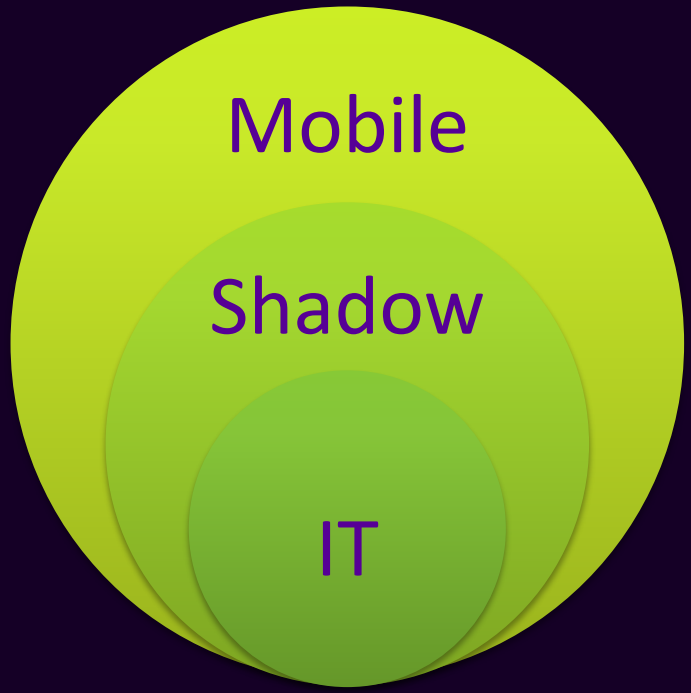
Vice President, Strategy
IntSights

@nickhayes10

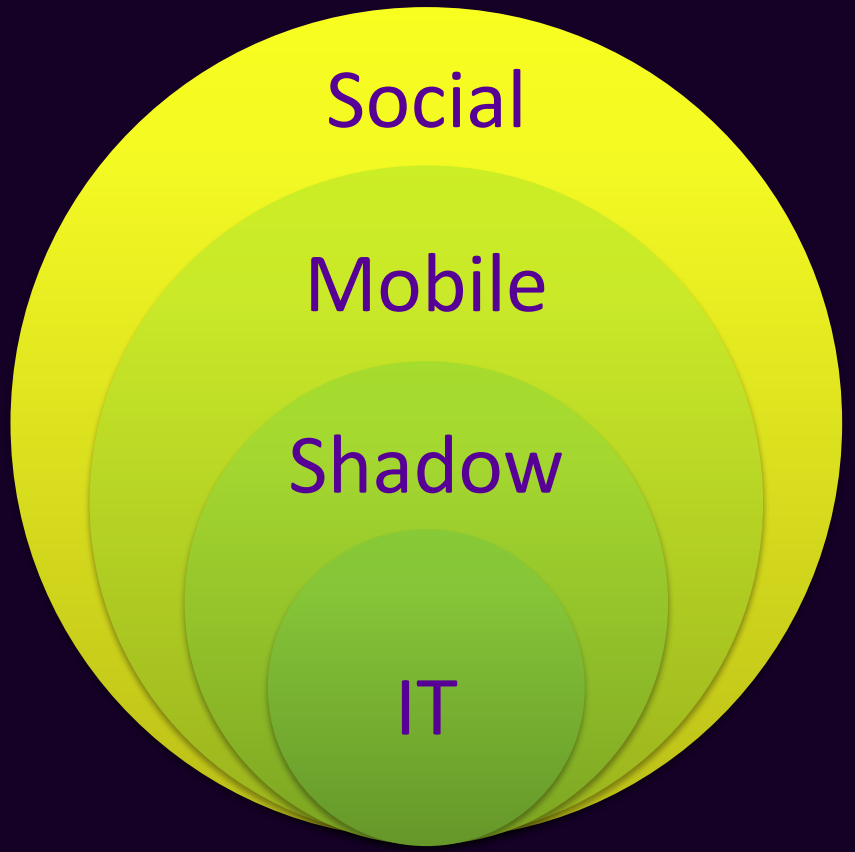
Our attack surface keeps growing

Our attack surface keeps growing

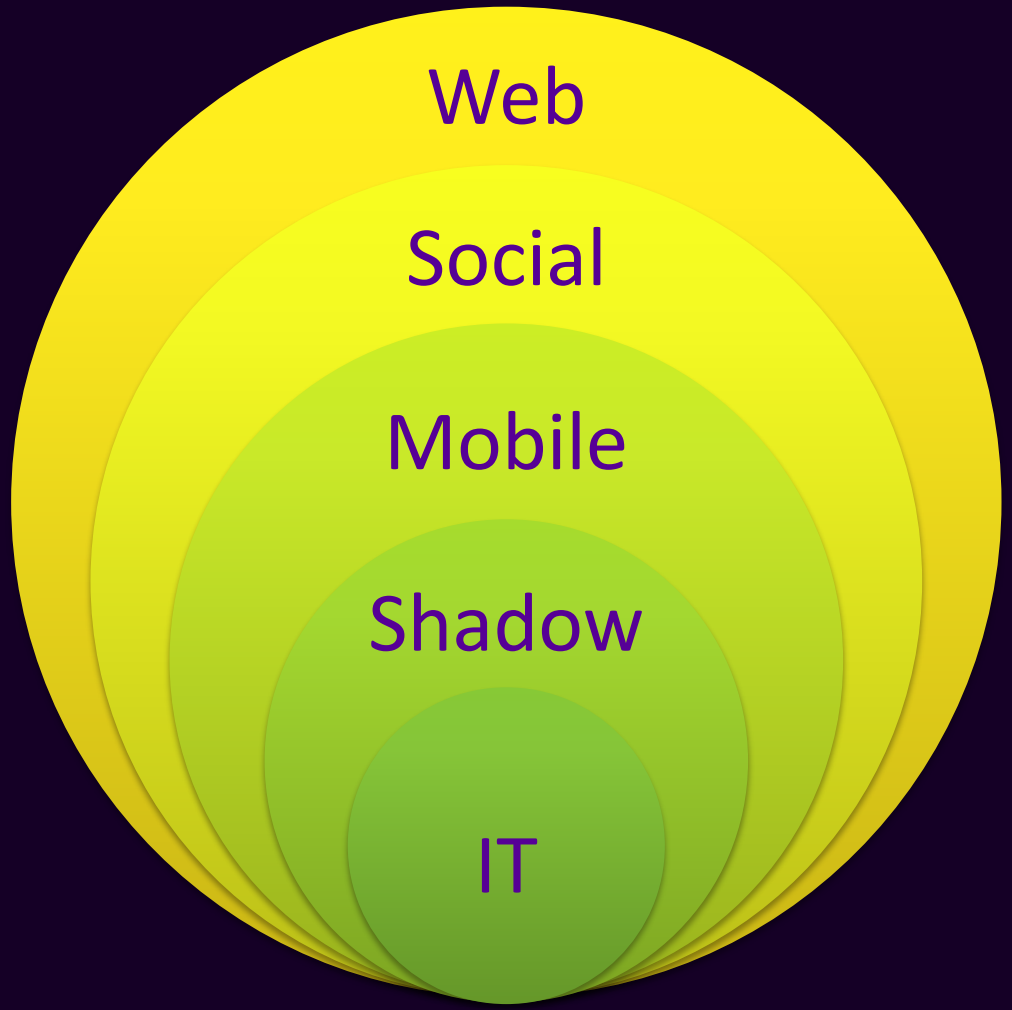
Our attack surface keeps growing



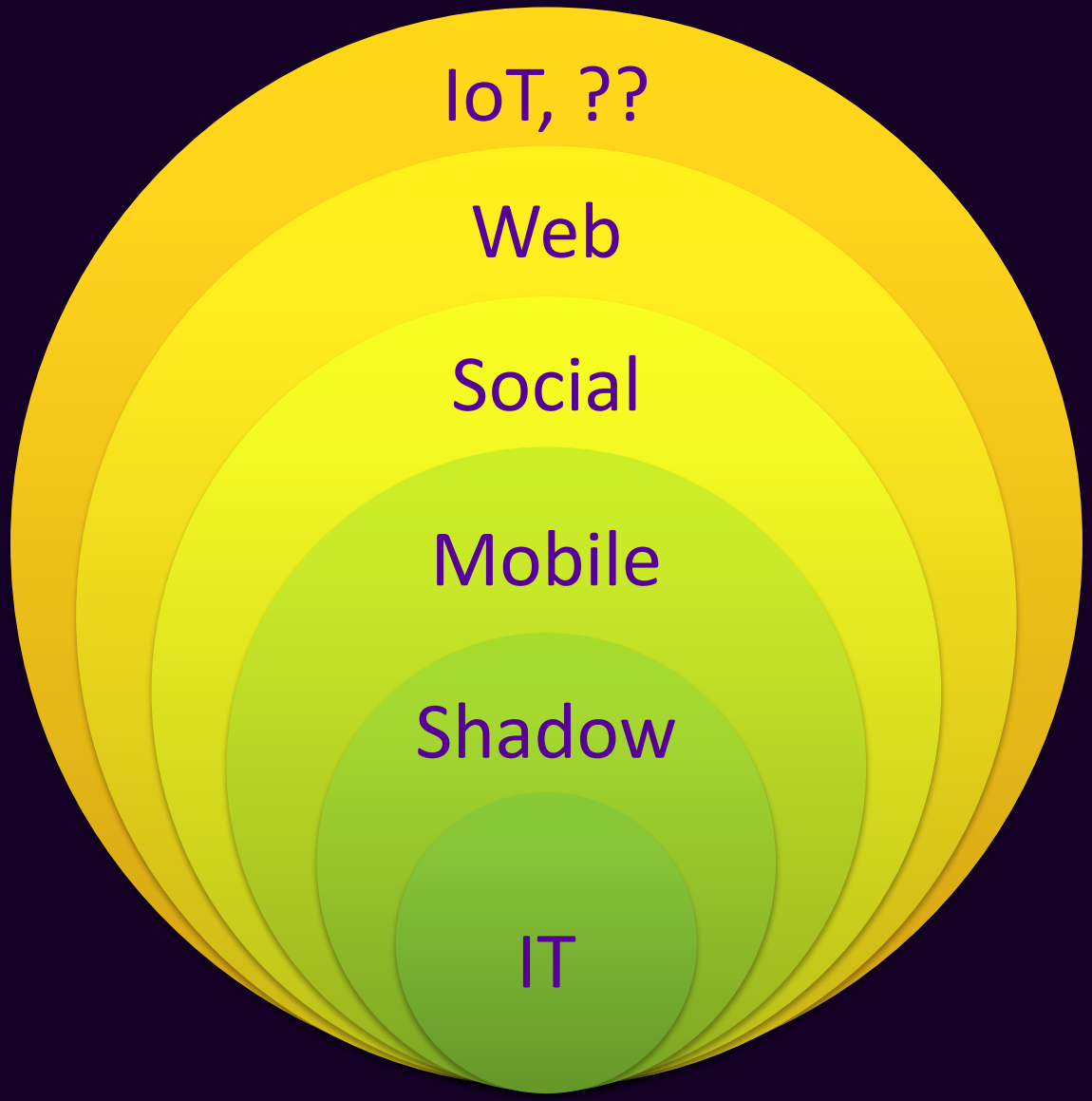
Our attack surface keeps growing



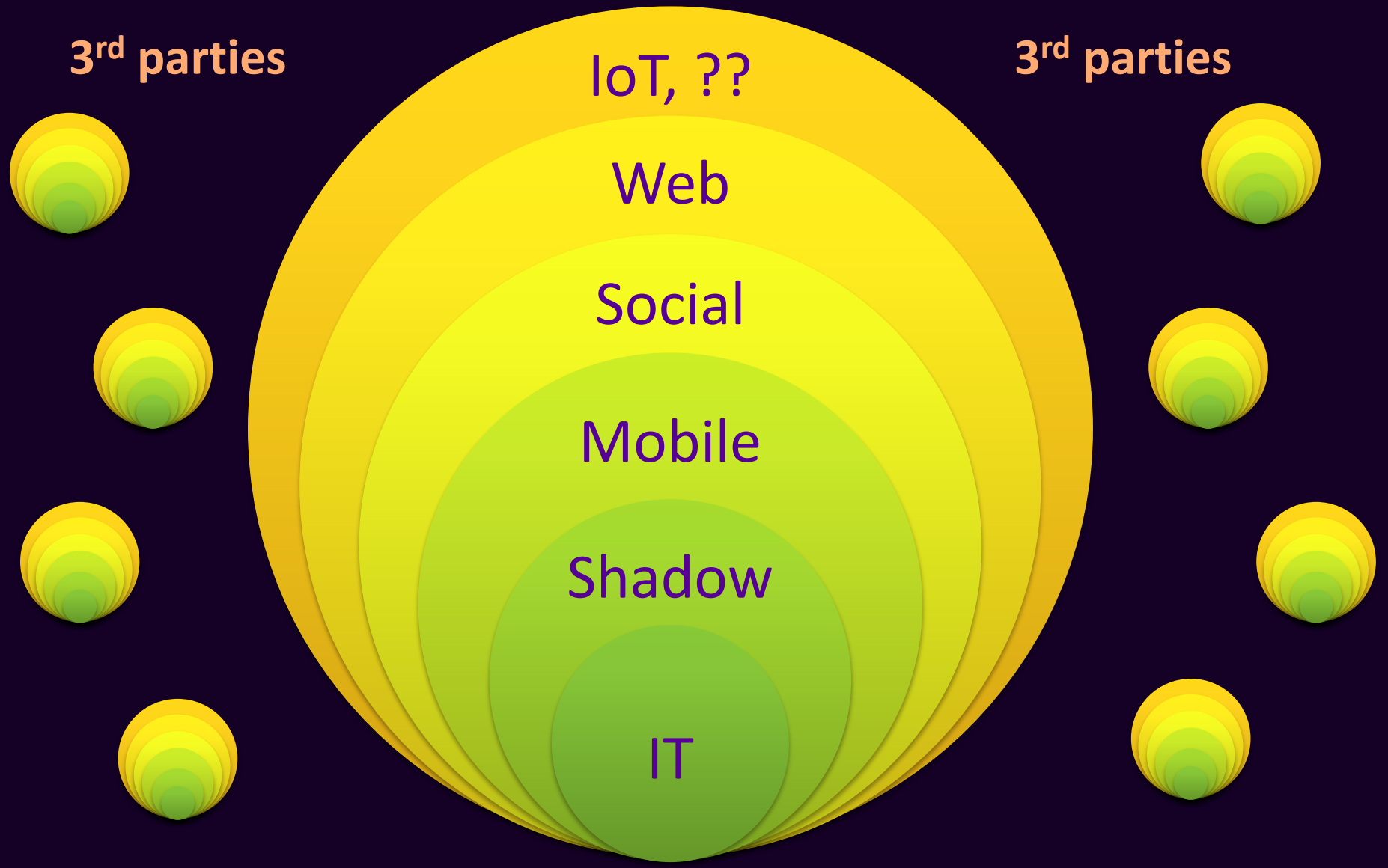
Our attack surface keeps growing



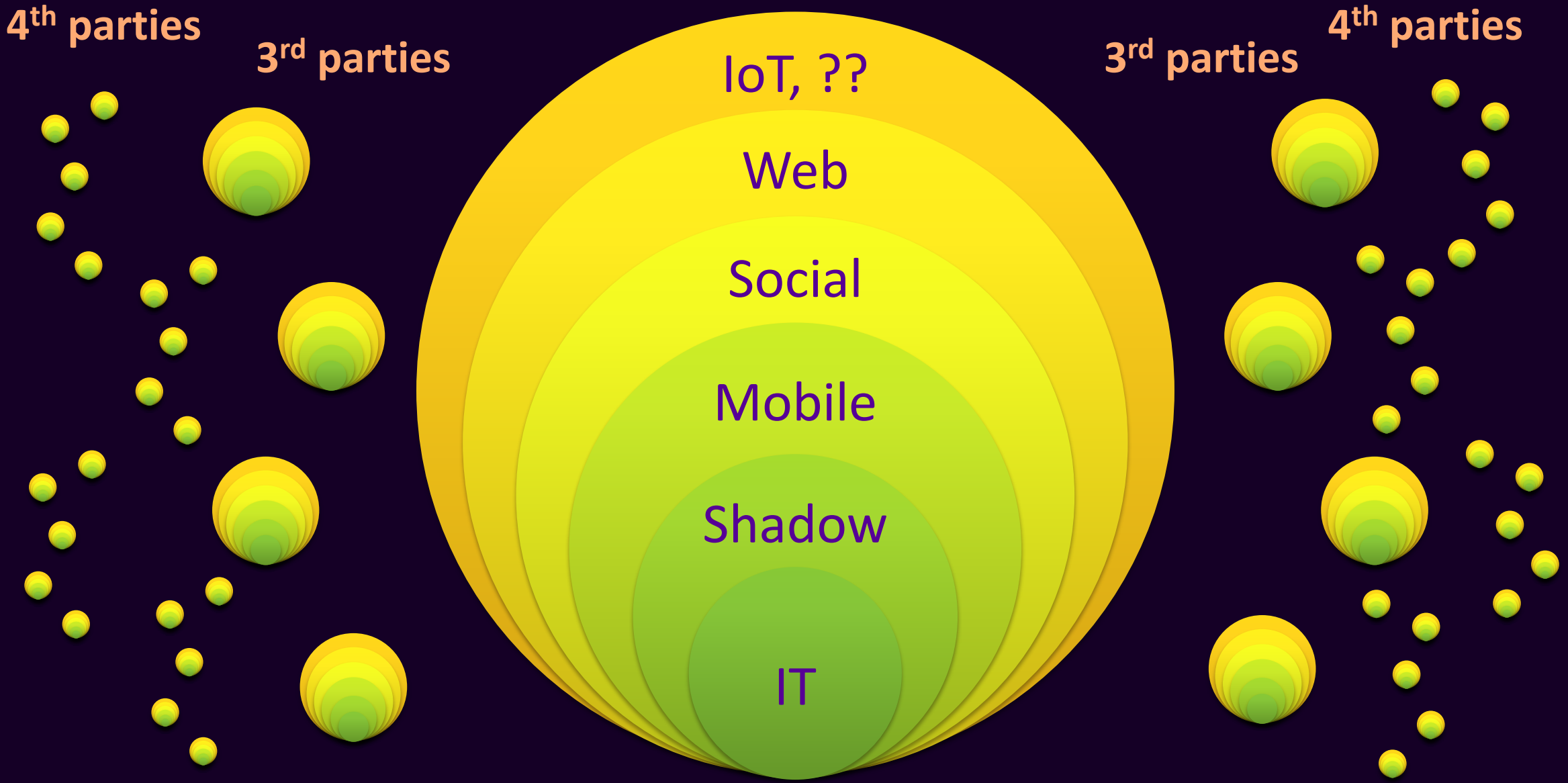
Our attack surface keeps growing



Our attack surface keeps growing



Our attack surface keeps growing



What does this look like?

278% Retail goods for sale on black markets

297% Retail phishing websites

171% Compromised employee credentials

149% Stolen credit cards for sale on dark web

Your assets, your credentials, your customers

Buying and selling accounts

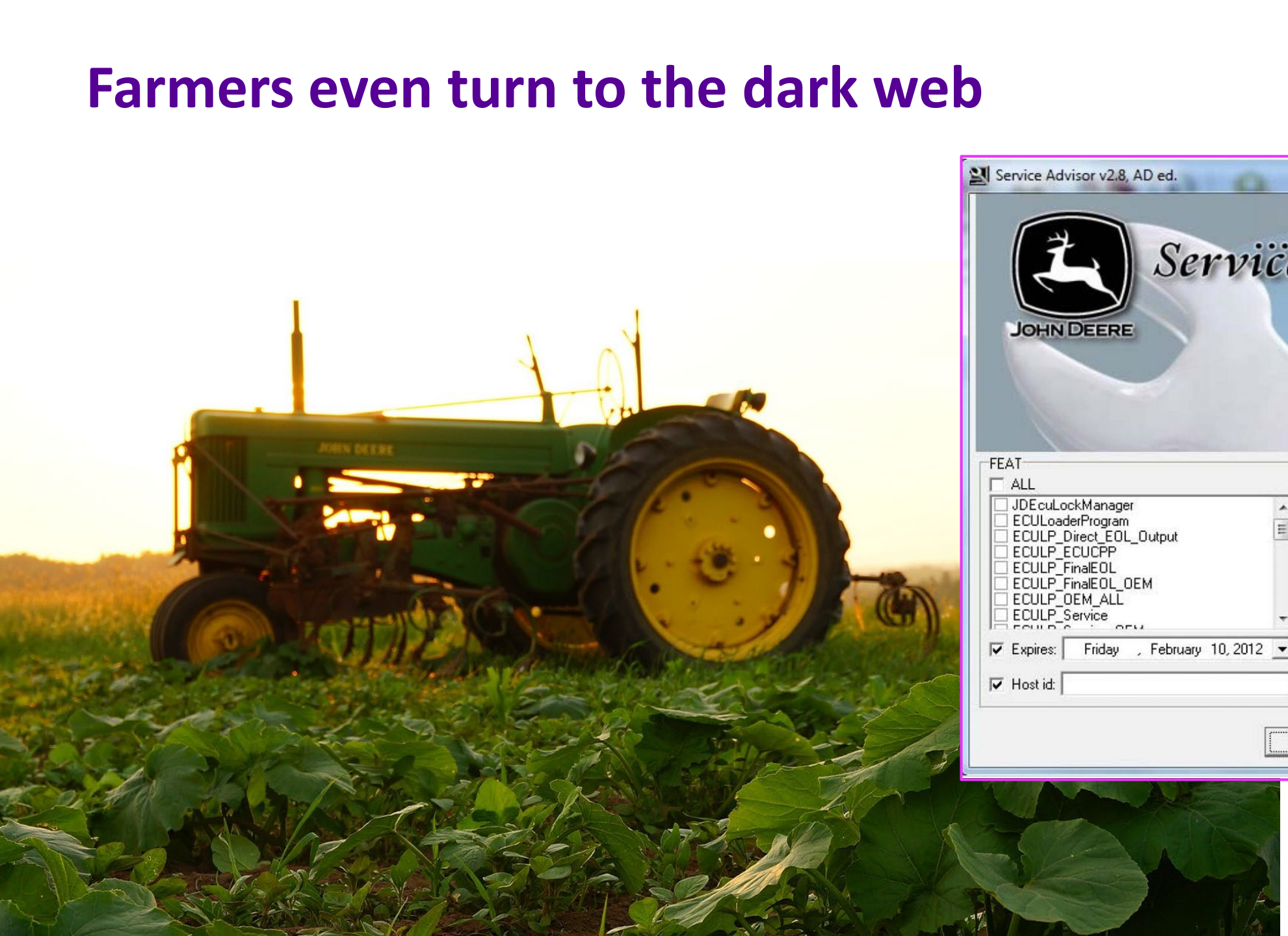
Shop	Balance	Points	Type	Country	CC	Bank	Info	Last order	Mail access	Seller	Price ($):	
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	☐
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	☐
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	☐
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A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

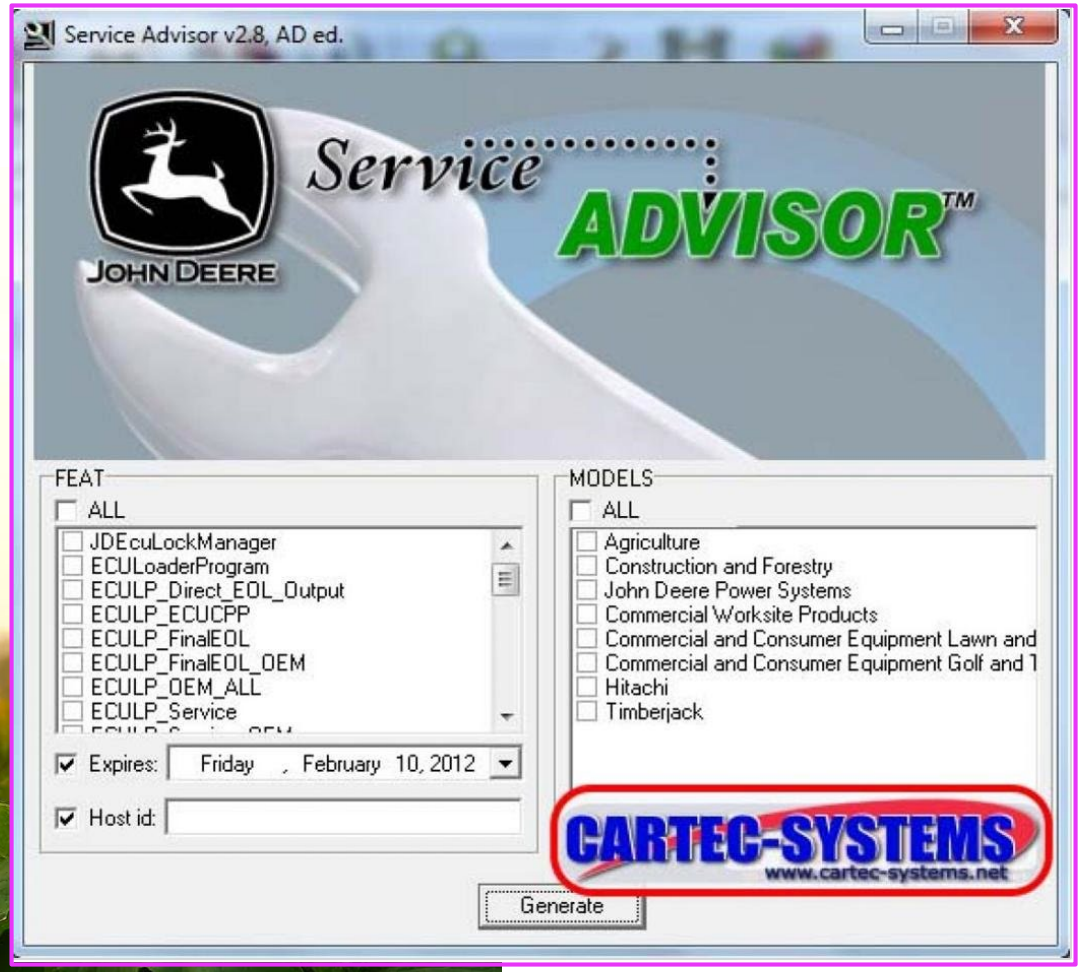
Customer logins

```
********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 if you want

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

Farmers even turn to the dark web



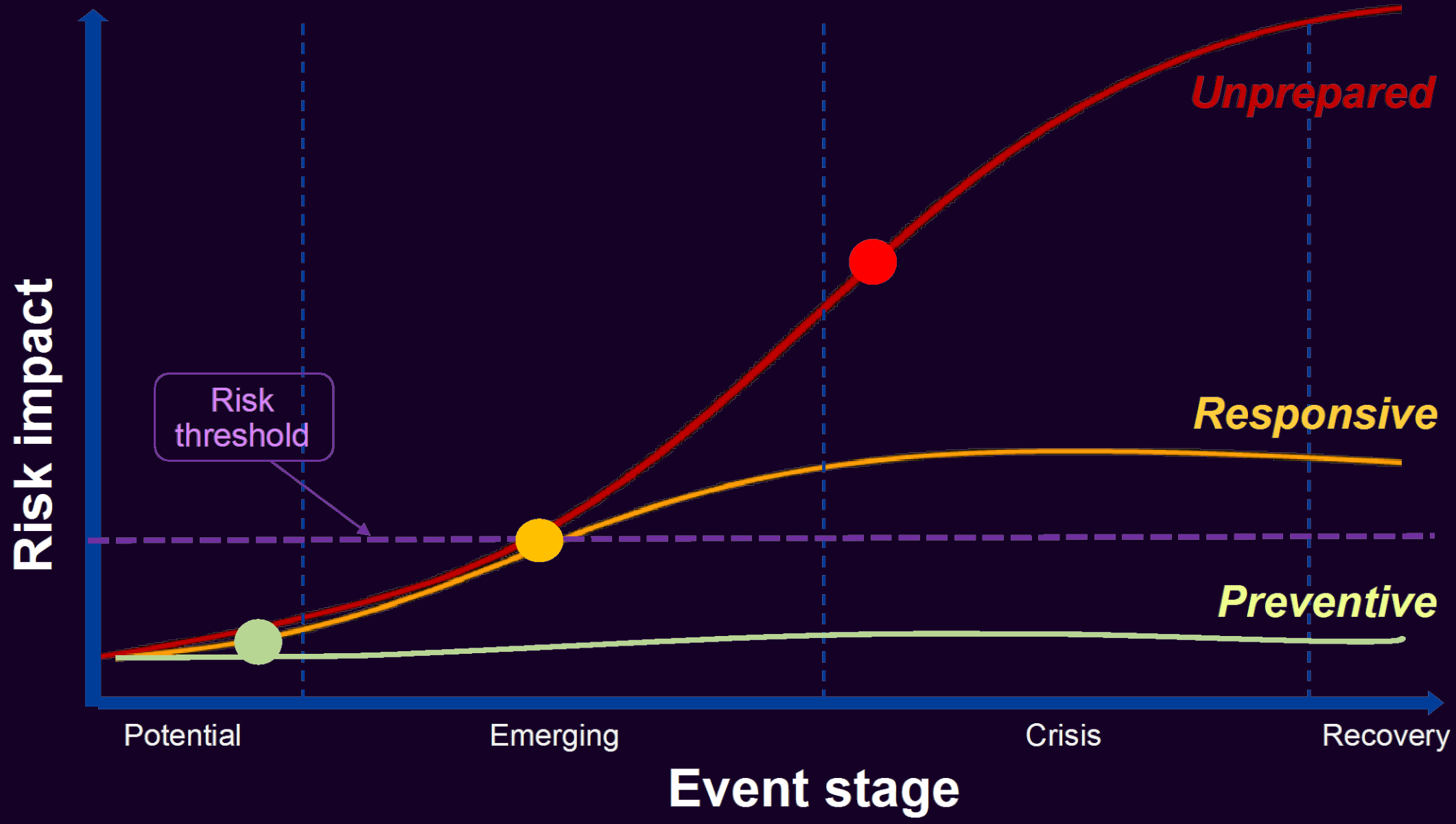


RSAConference2019

A Shift In Mindset

From Prevent… To Detect And Remediate

Minimize the *impact*



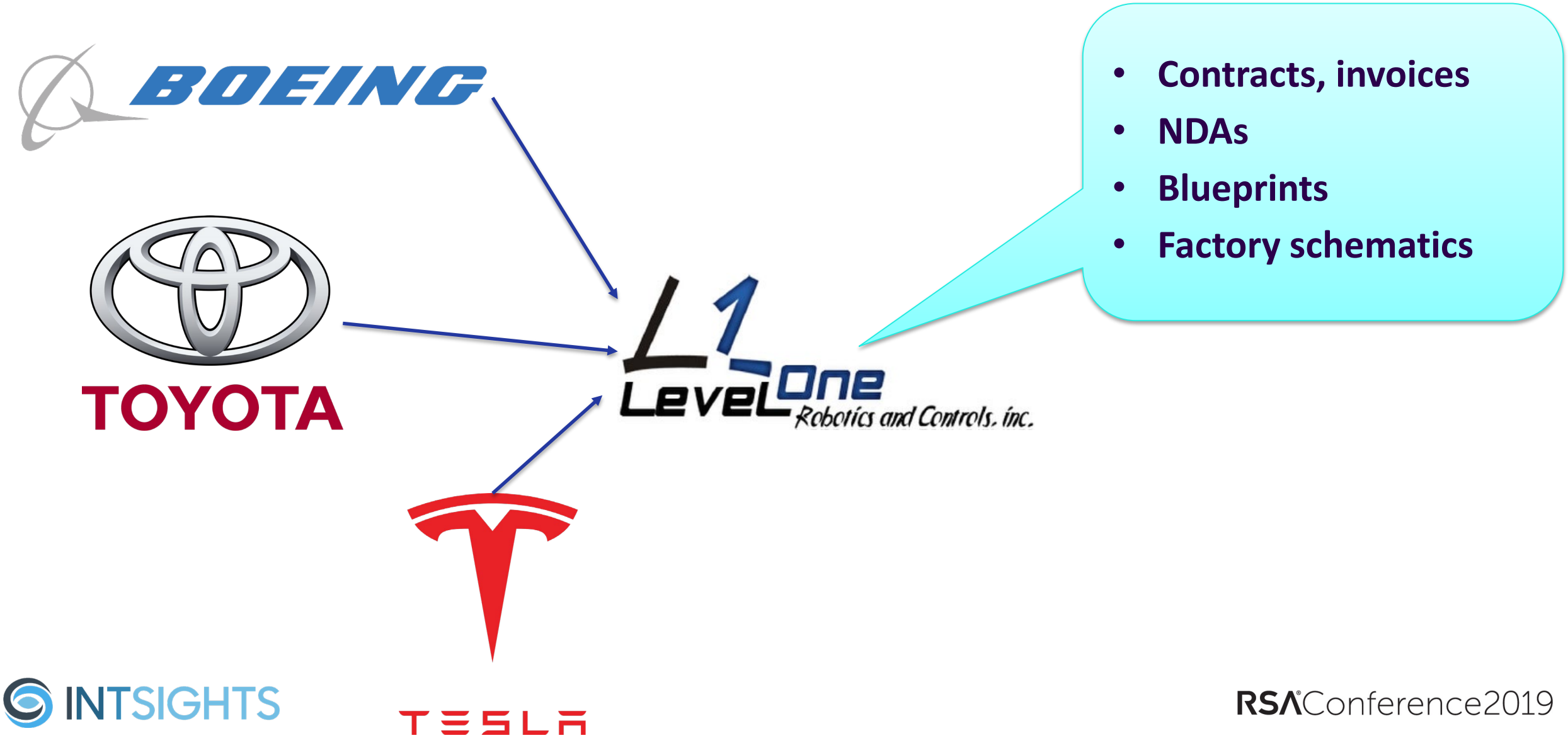
How quickly can you take action?

- Stolen intellectual property, exposed credentials
- Brand hijacking, ad scams, account takeovers
- Digital extortion, attack coordination
- Executive/VIP safety
- Third-party risks
- Phishing

WHAT ARE
YOU
LOOKING AT?

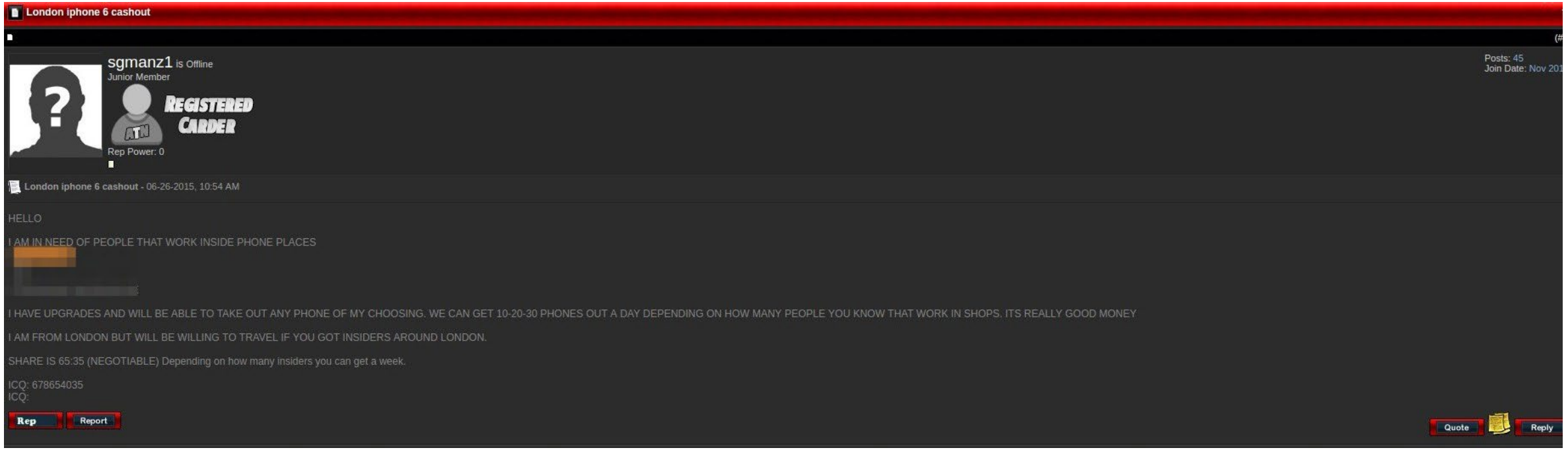
Tailor your threat intel to *your business*.

Limit your exposure, track your third-parties at scale



Make sure your intellectual property *stays yours*

Insider threats recruited on the dark web



RSAConference2019

Digital Risk Protection (DRP) In Three Steps

Three-step process for continuous digital risk protection

Map

Catalog your entire digital footprint.

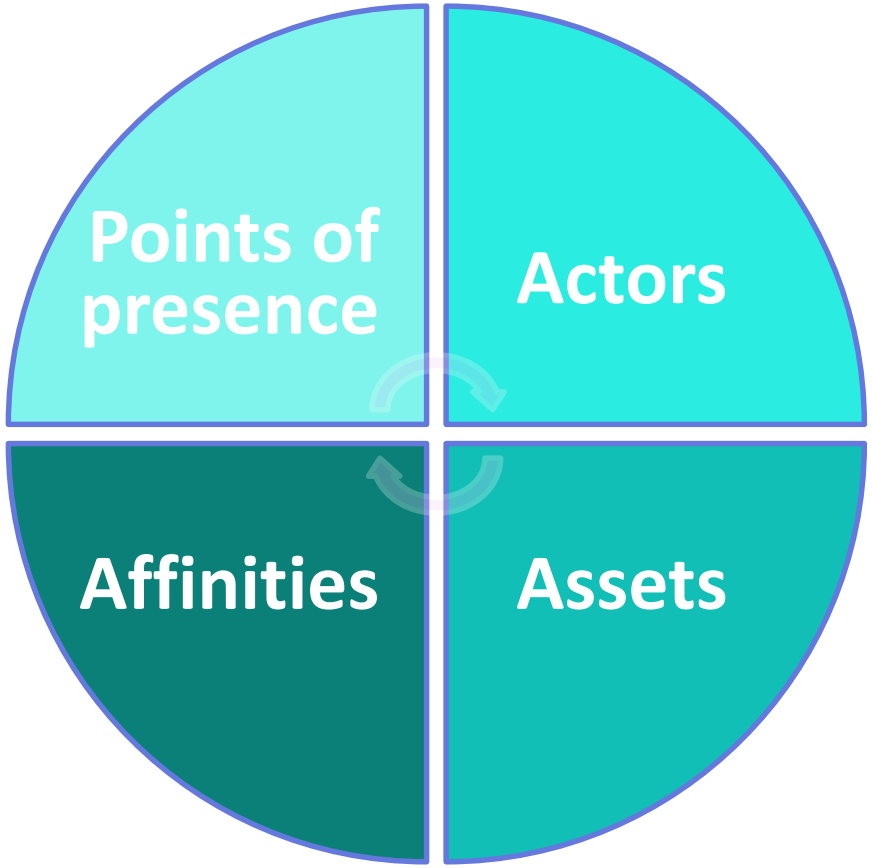
Monitor

Actively scan for new instances or modifications of your digital assets.

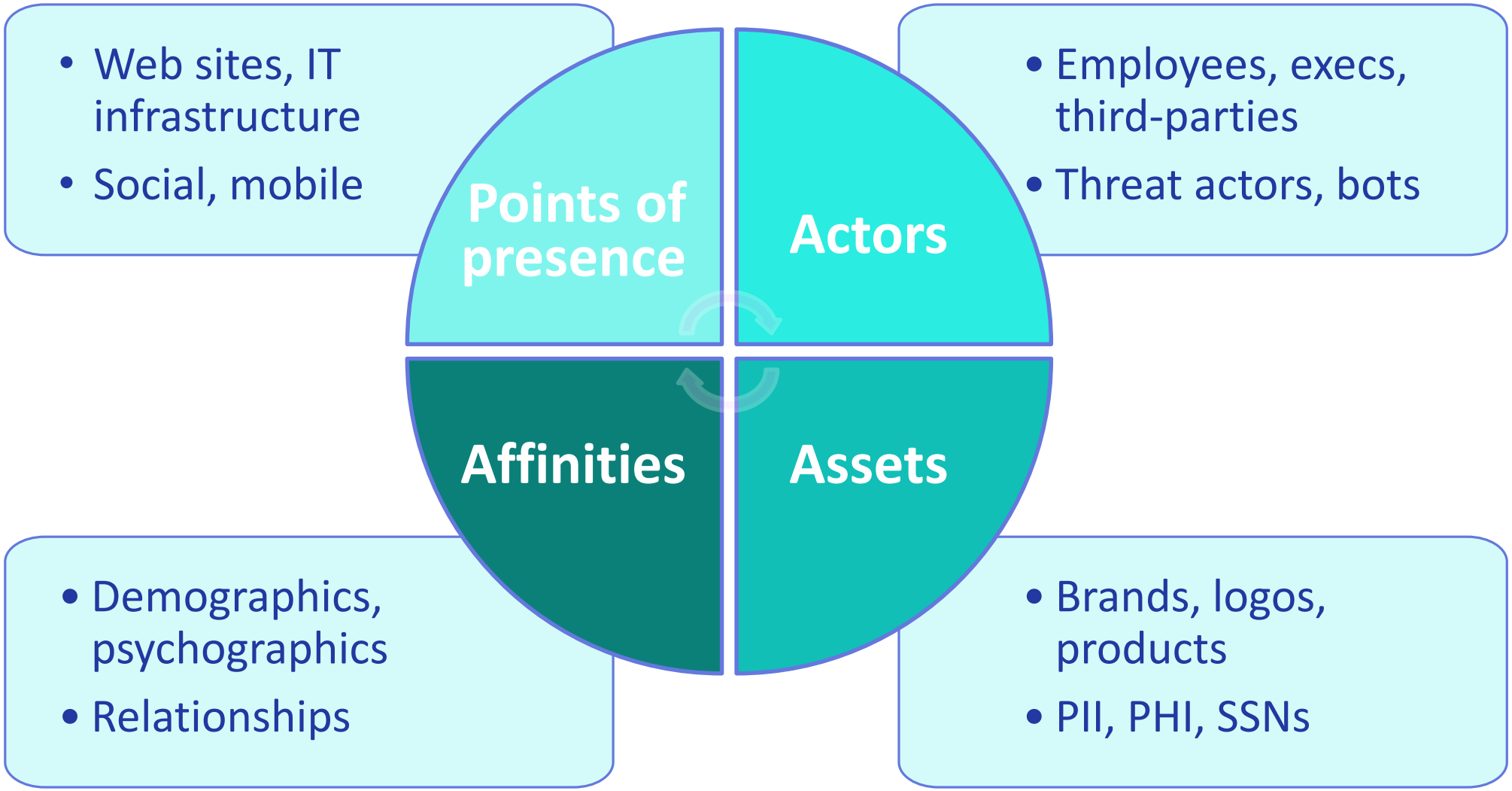
Mitigate

Streamline controls and remediation plans to curb risk impact.

Map your footprint



Map your footprint, in context



Establish consistent visibility

- Data collection techniques
  - Access: APIs, pay-for-access data, other security intel feeds
  - Harvesting: Data crawlers, bots, sensors, etc.
  - HUMINT: analyst-curated, in-depth investigations
- Breadth and depth of risk analytics
  - Scope: number of assets, entities, regions, data types
  - Frequency: rate of scans – weekly, daily, real-time
  - Sophistication: risk scoring, alert options, data visualization

Prepare your response

- Digital risk scenario analysis
- Technical controls and contingencies
  - External: Takedowns and event remediation
  - Internal: Integration w/ security tools: firewalls, ESGs, etc.
- Response teams and plans
  - Decision trees, crisis communications
  - Key external stakeholders, regional support

RSAConference2019

What next?

Threat alerts are only
useful in context.

Preparing your approach

- What immediate challenges do we want to solve?
- Where are our assets and 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 our expected outcomes in 6 months, 1 year, 3 years?

Key takeaways

1. Assume you lost -- detect and remediate supersede prevent.
2. Threat intel improves your SecOps – when it's *contextualized* and *actionable.*
3. Define your use-cases; start with one or two.
4. Get comfortable with grey; strive for risk-based decisions.

RSAConference2019

San Francisco | March 4–8 | Moscone Center

SESSION ID: STR-T07

Thank you!

Nick Hayes

Vice President, Strategy
IntSights

@nickhayes10