RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

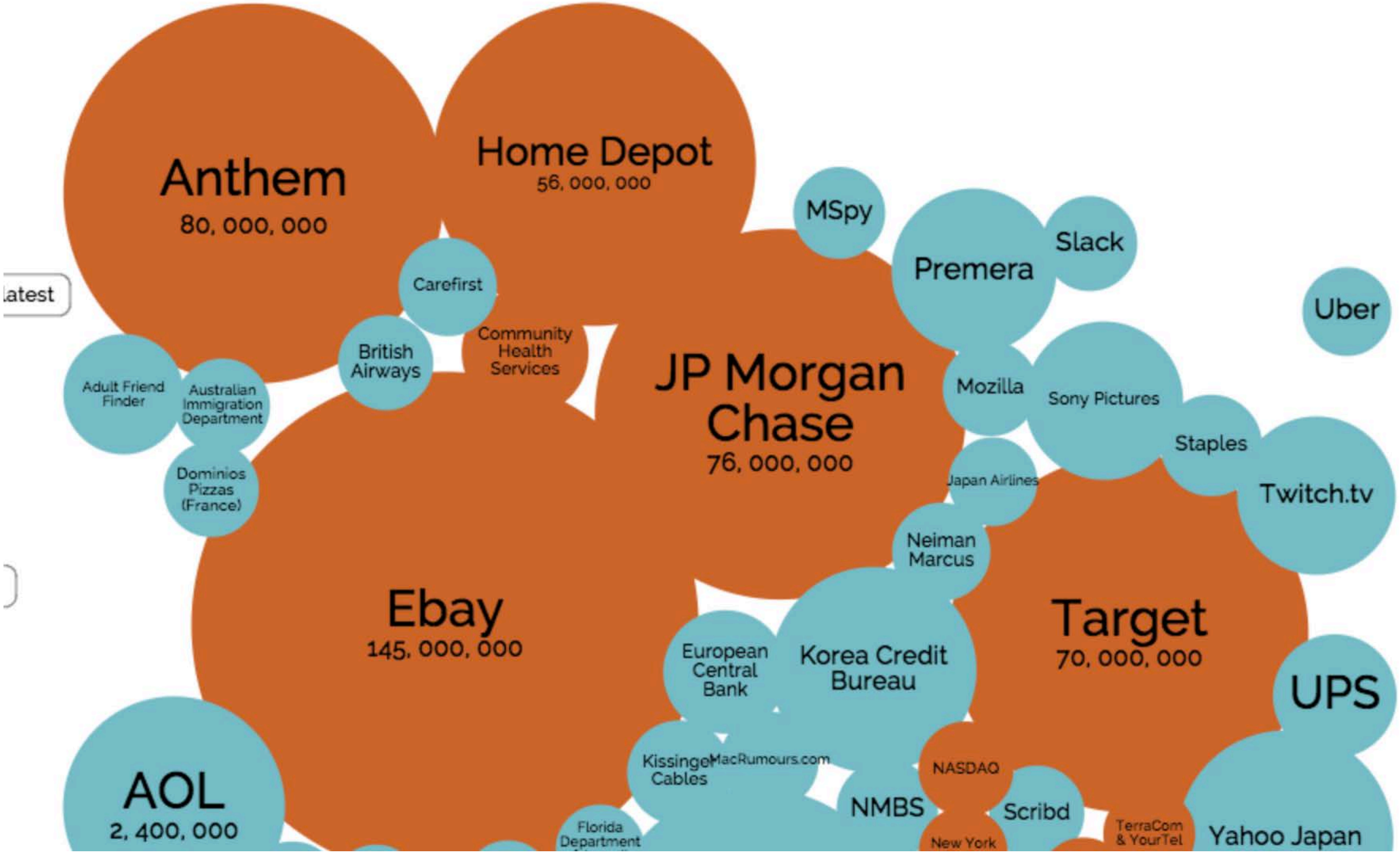
Challenge today's security thinking

SESSION ID: CLE-R01

You've Done Everything Right, and Still There's a Breach. Now What?

Zulfikar Ramzan

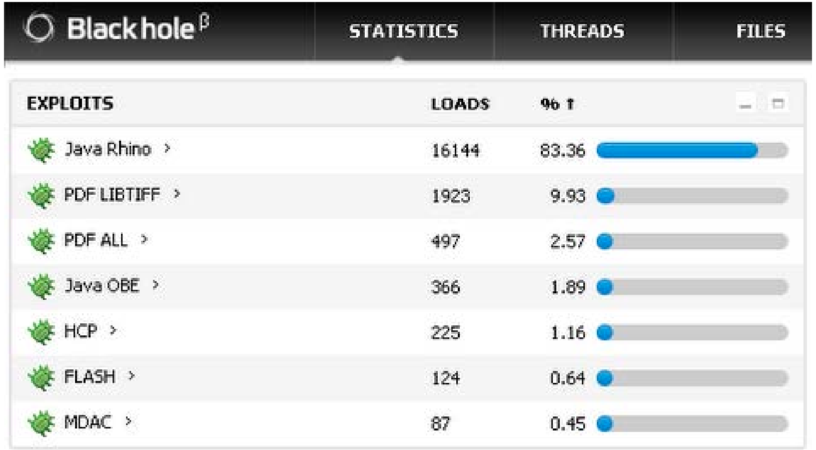
Chief Technology Officer
RSA
@zulfikar_ramzan



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Why Are Intrusions Successful?

Threats are targeted. macro-distribution supplanted by micro distribution (e.g., via packing, polymorphism)



EXPLOITS	LOADS	% ↑
Java Rhino ›	16144	83.36
PDF LIBTIFF ›	1923	9.93
PDF ALL ›	497	2.57
Java OBE ›	366	1.89
HCP ›	225	1.16
FLASH ›	124	0.64
MDAC ›	87	0.45

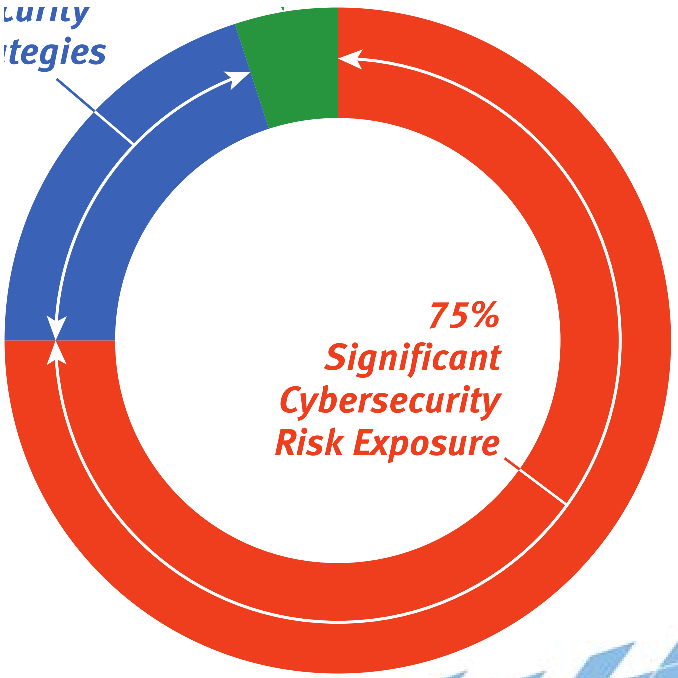
Powerful attack toolkits available w/ tiered pricing, 24x7 customer support

Security Maturity Survey Results

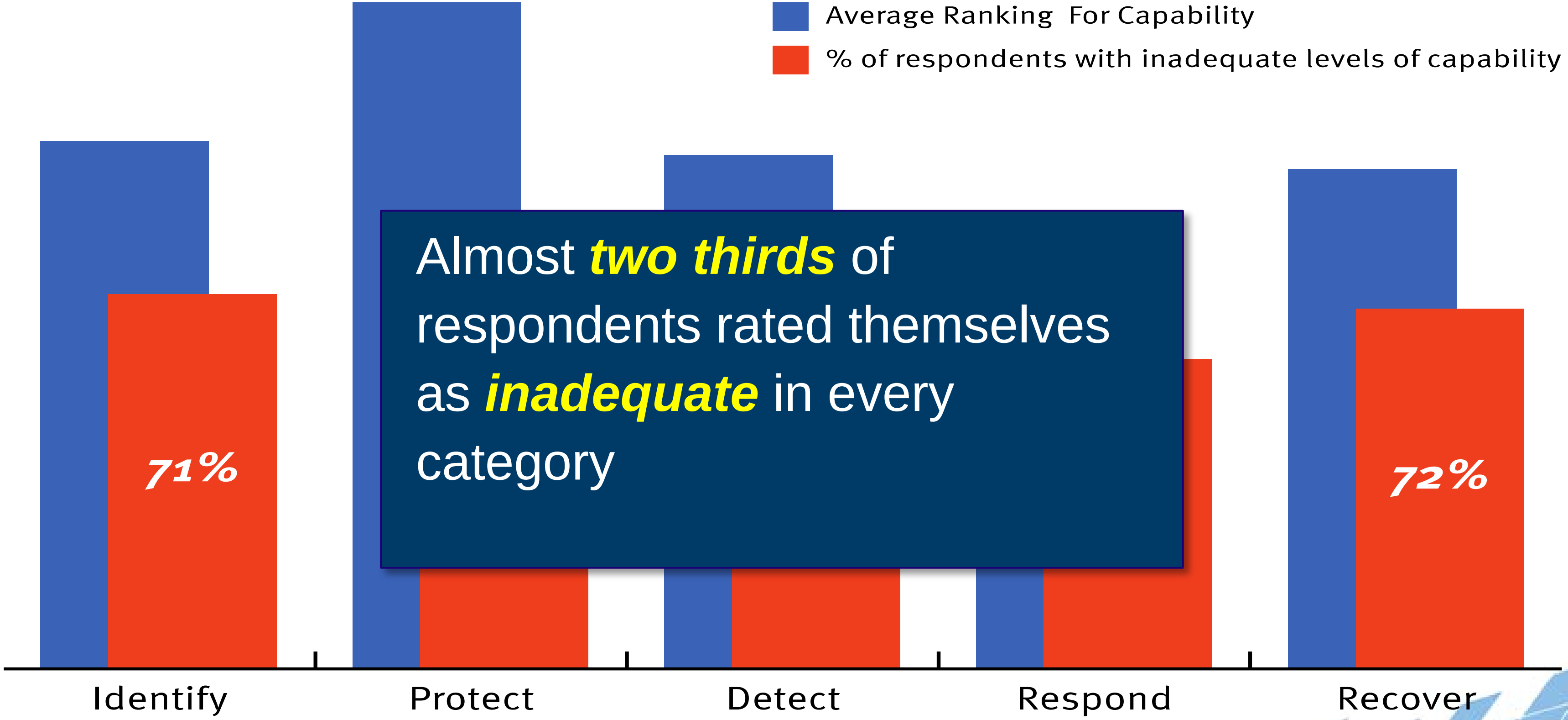
Surveyed ***400+*** Security professionals across ***60+*** countries.

75% of respondents have significant cybersecurity risk exposure

Only a quarter of respondents surveyed indicated that they have mature security strategies and just ***5%*** have Advantaged capabilities.



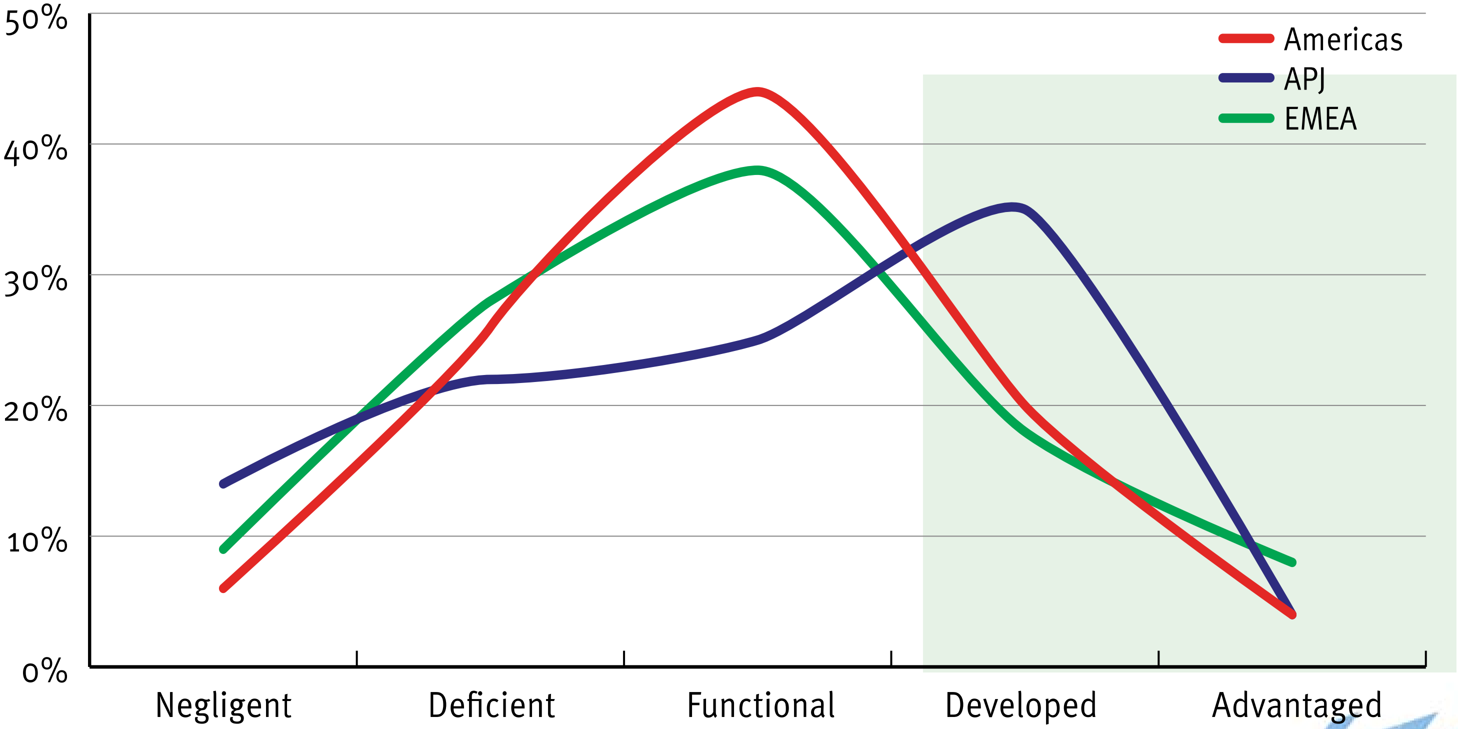
Capabilities Compared

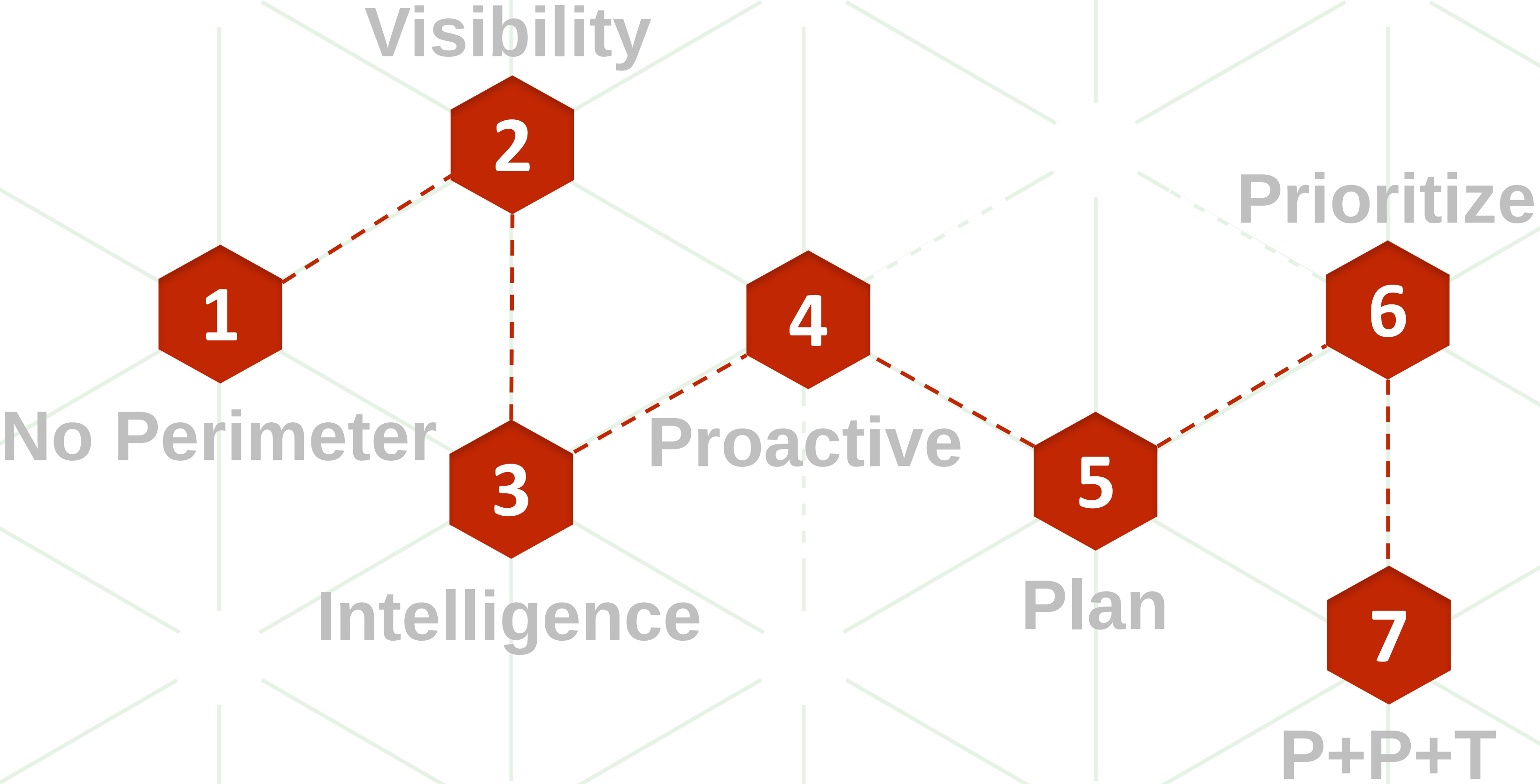


Almost ***two thirds*** of respondents rated themselves as ***inadequate*** in every category

Geography

ORGANIZATIONS IN APJ REPORTED THE MOST MATURE STRATEGIES




Visibility
2
1
No Perimeter
3
Intelligence
4
Proactive
5
Plan
Prioritize
6
7
P+P+T

Eliminate the Perimeter / Prevention Mindset

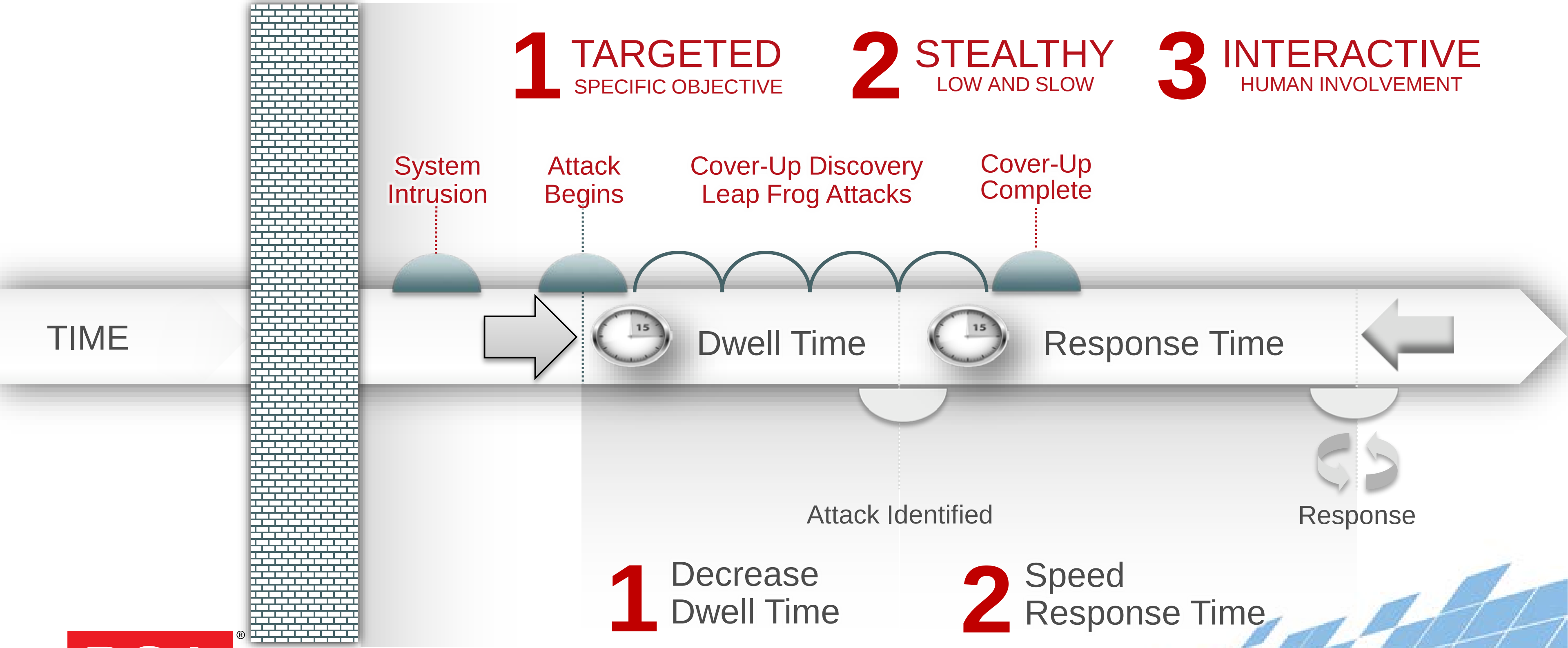
1

Advanced Threats Are Different

1 TARGETED SPECIFIC OBJECTIVE

2 STEALTHY LOW AND SLOW

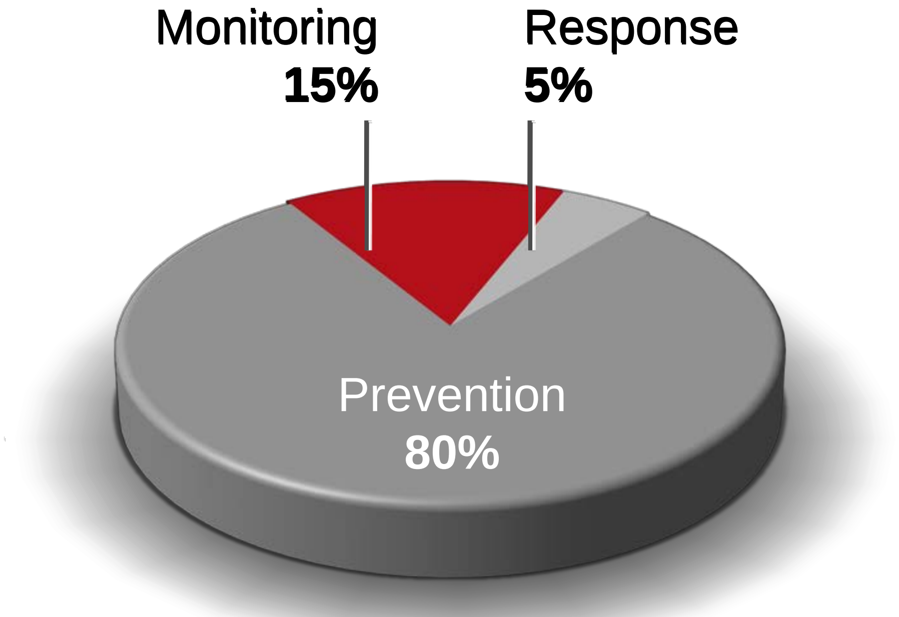
3 INTERACTIVE HUMAN INVOLVEMENT



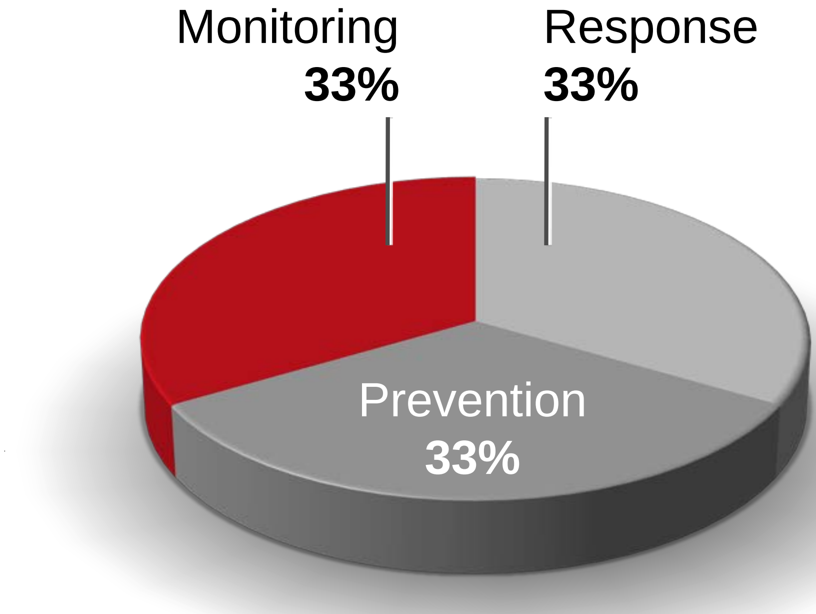
1 Decrease Dwell Time

2 Speed Response Time

Shift Priorities and Capabilities



How we spend



How we *should* spend

Strive for pervasive and reliable

visibility

2

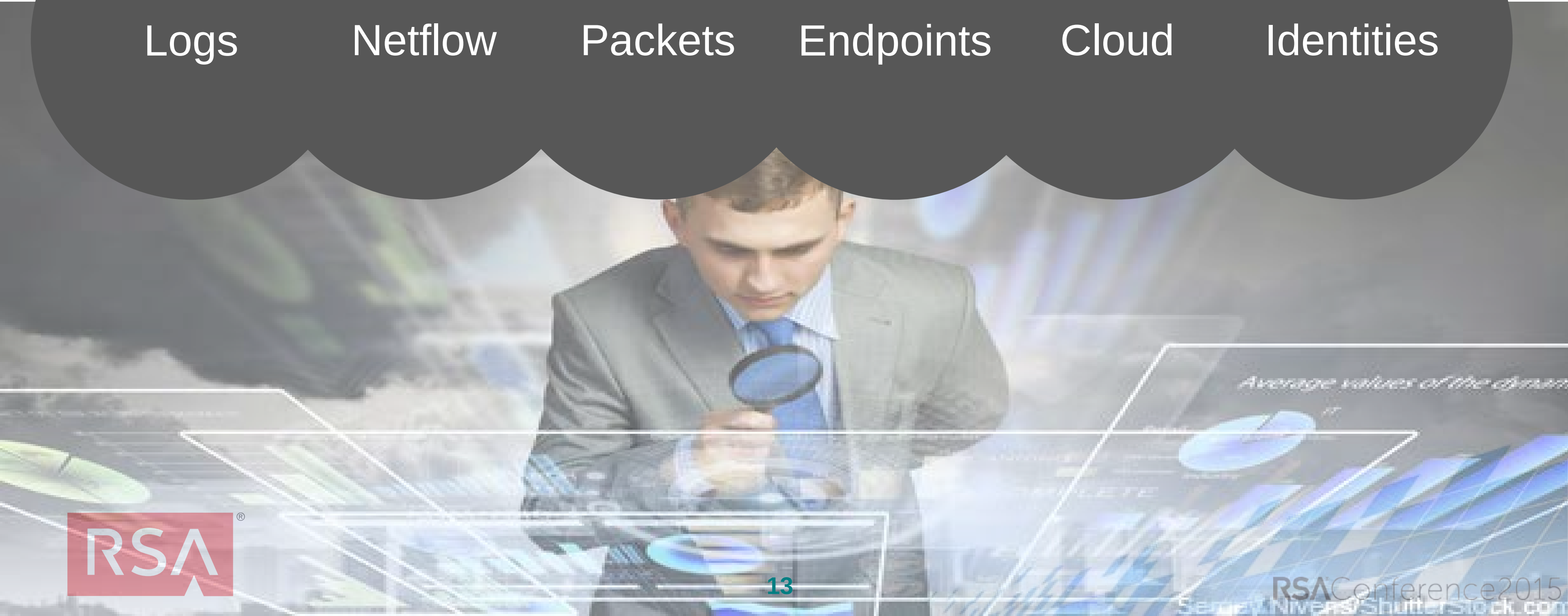
Strive for pervasive and reliable

visibility

2

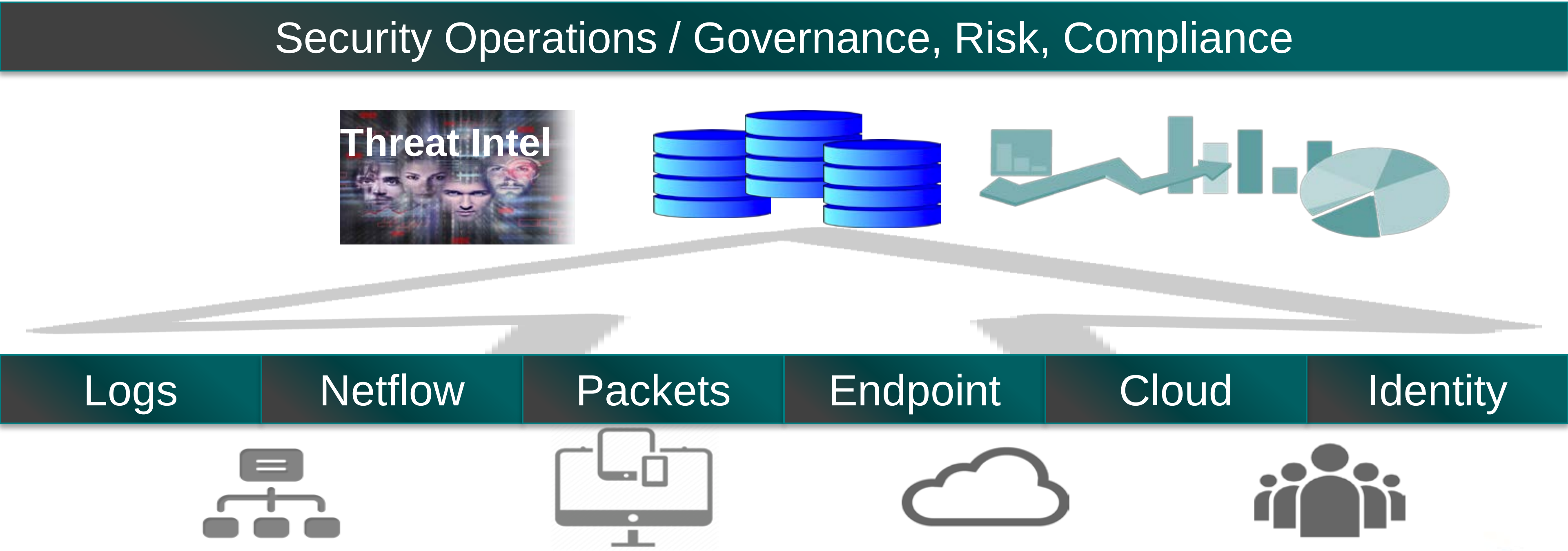
Key Visibility Points

Logs Netflow Packets Endpoints Cloud Identities



Sergey Nivens/Shutterstock.com

The “Revised” Map



Security Operations / Governance, Risk, Compliance

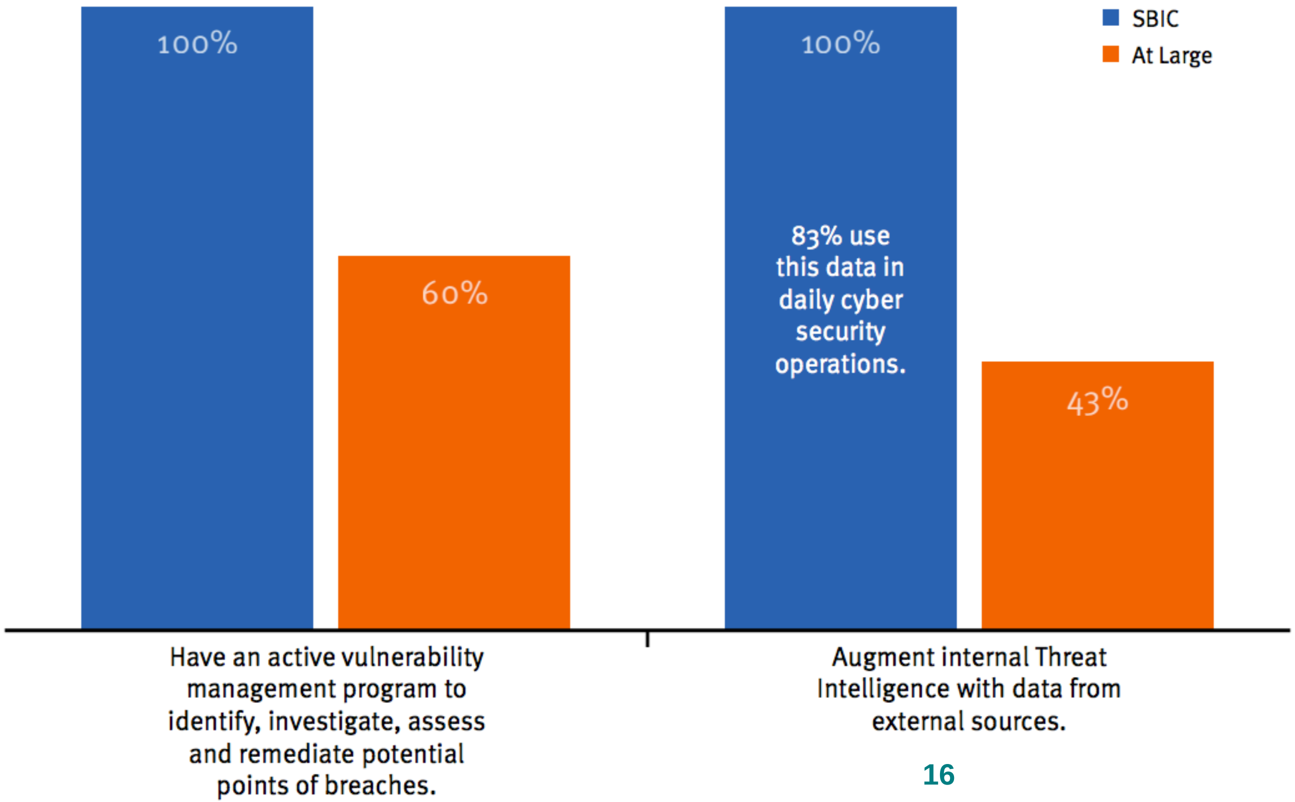
Logs | Netflow | Packets | Endpoint | Cloud | Identity

Leverage and Operationalize Threat Intelligence

3

Threat Intelligence:

collecting and synthesizing internal and external threat data to implement effective detection, investigation, and response to security events



Security operations must maintain a certain level of flexibility. With zero-day events and other types of attacks that are less understood, security operations teams must be nimble and adaptive. Subscription-based services are good for additional help if your team is resource constrained.

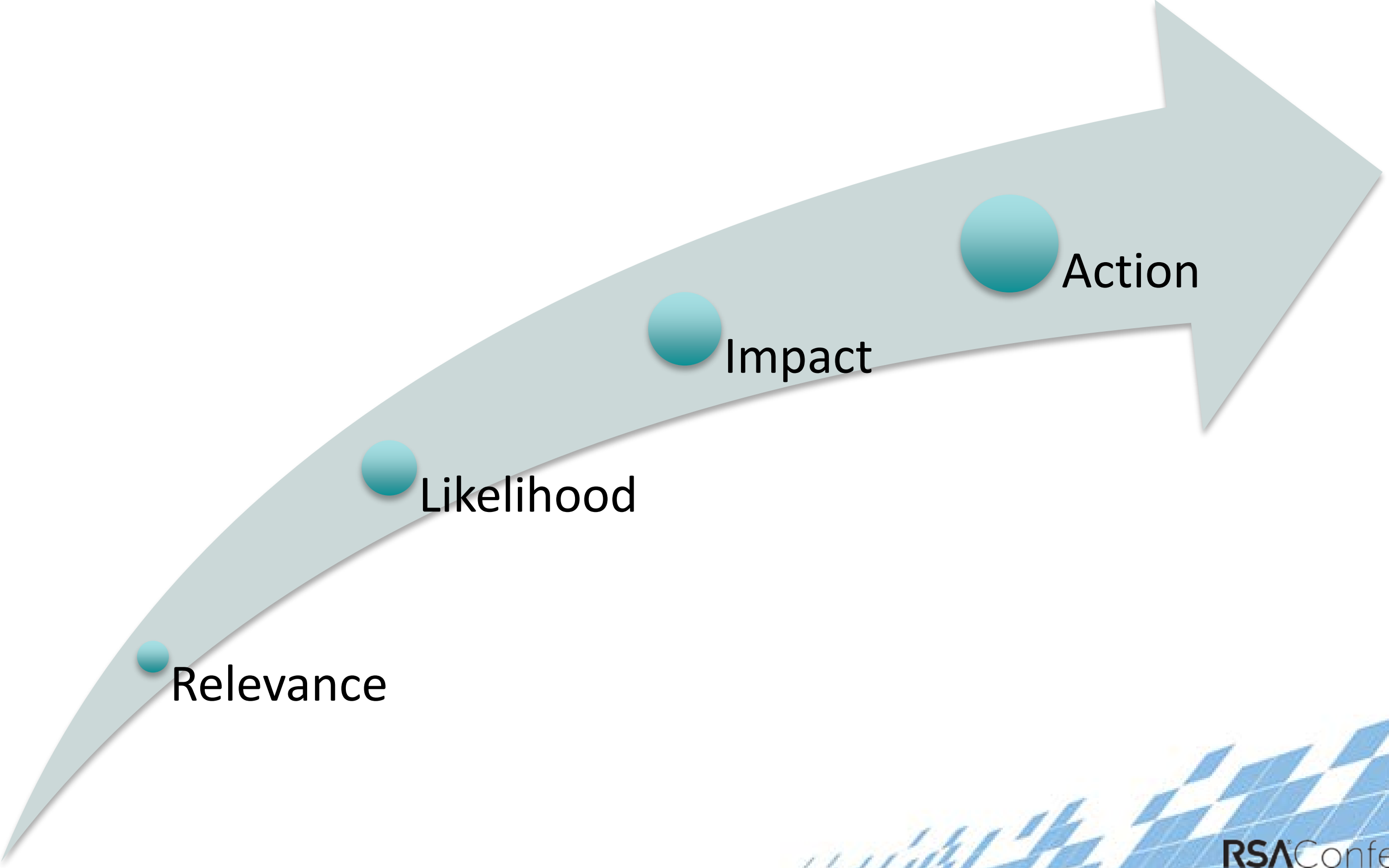
-Jerry Geisler, Sr. Director, Information Systems Security Ops, Office of the CISO, Walmart.

Is threat intelligence about looking backwards…

… when we should be looking *forward?*

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. --Sun Tzu

Relevance + Likelihood + Impact = Action



Relevance

Likelihood

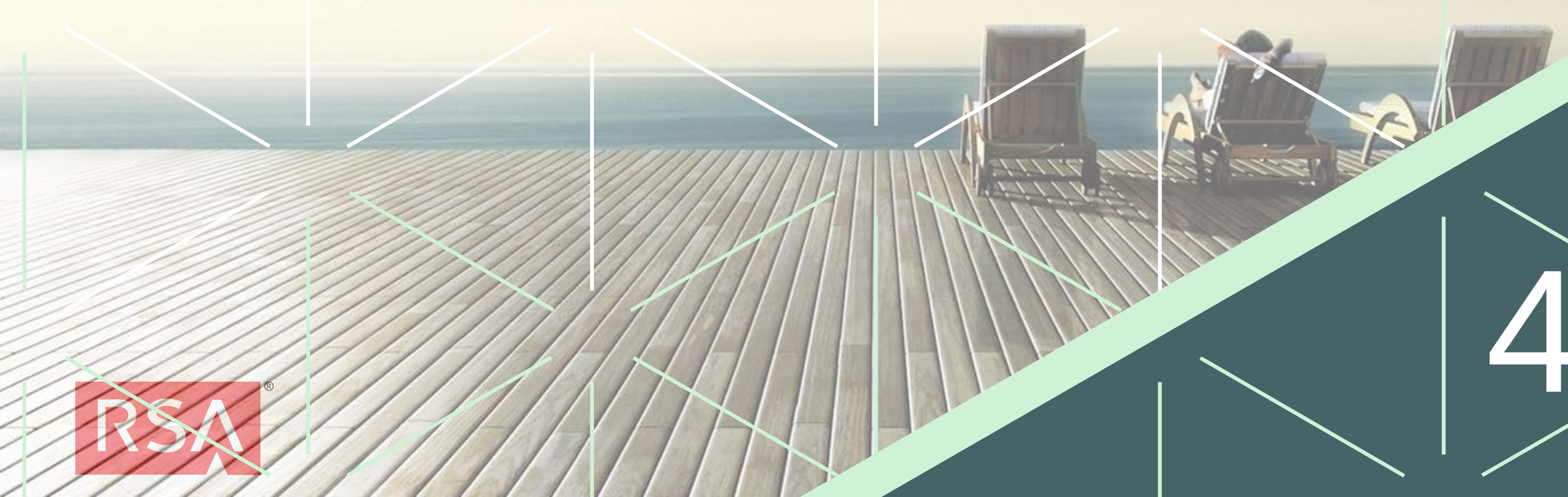
Impact

Action

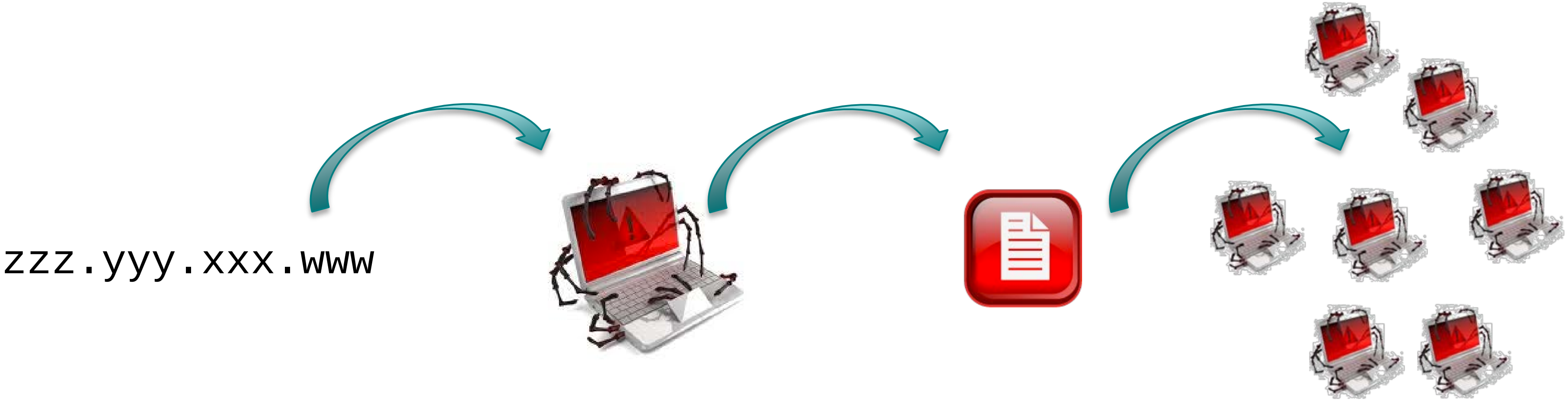
Don’t Sit Back…

Be Proactive

4



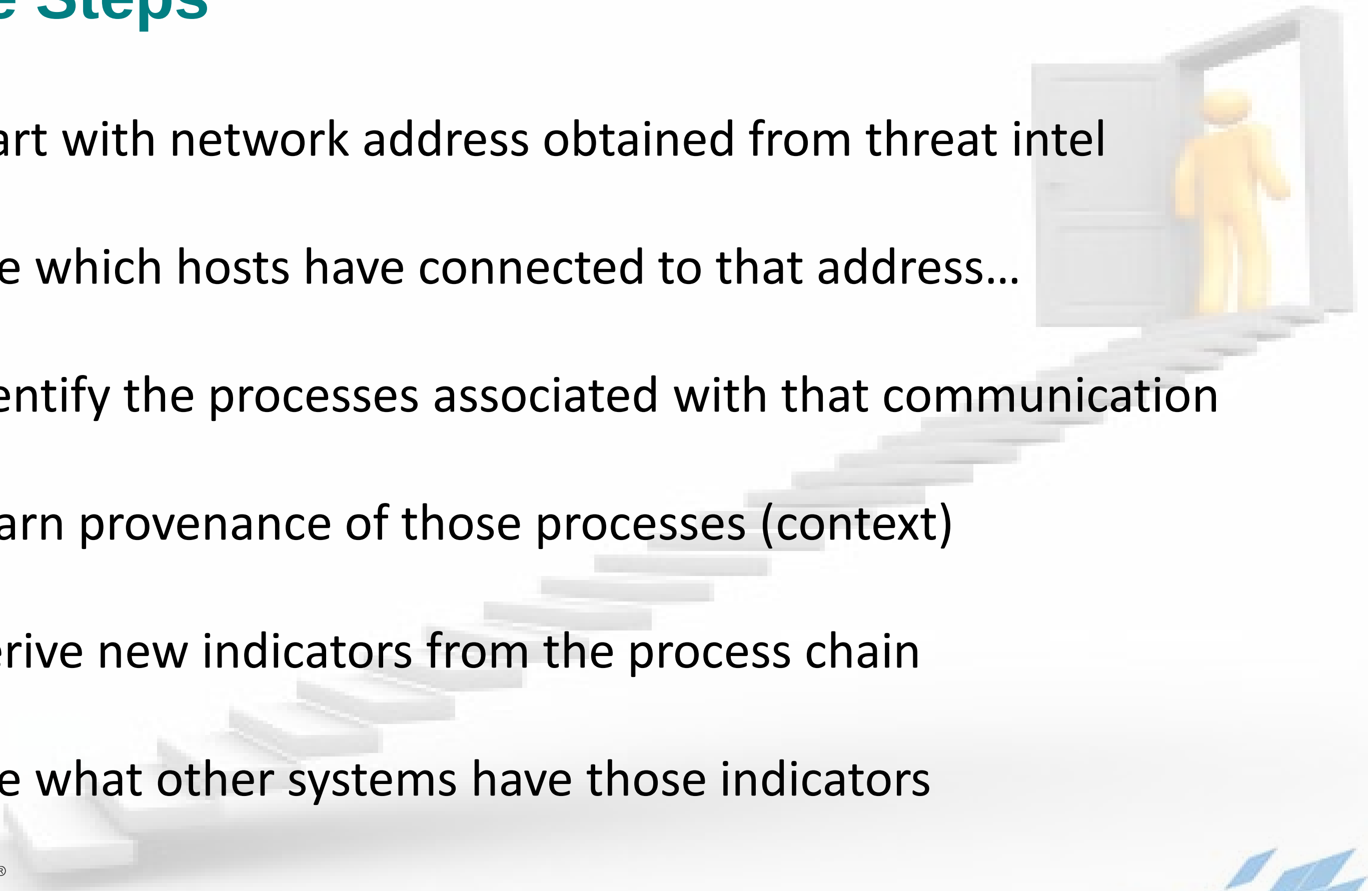
Peel Back the Layers



zzz.yyy.xxx.www

Starting with a single artifact or threat indicator, you can find broader attacks.

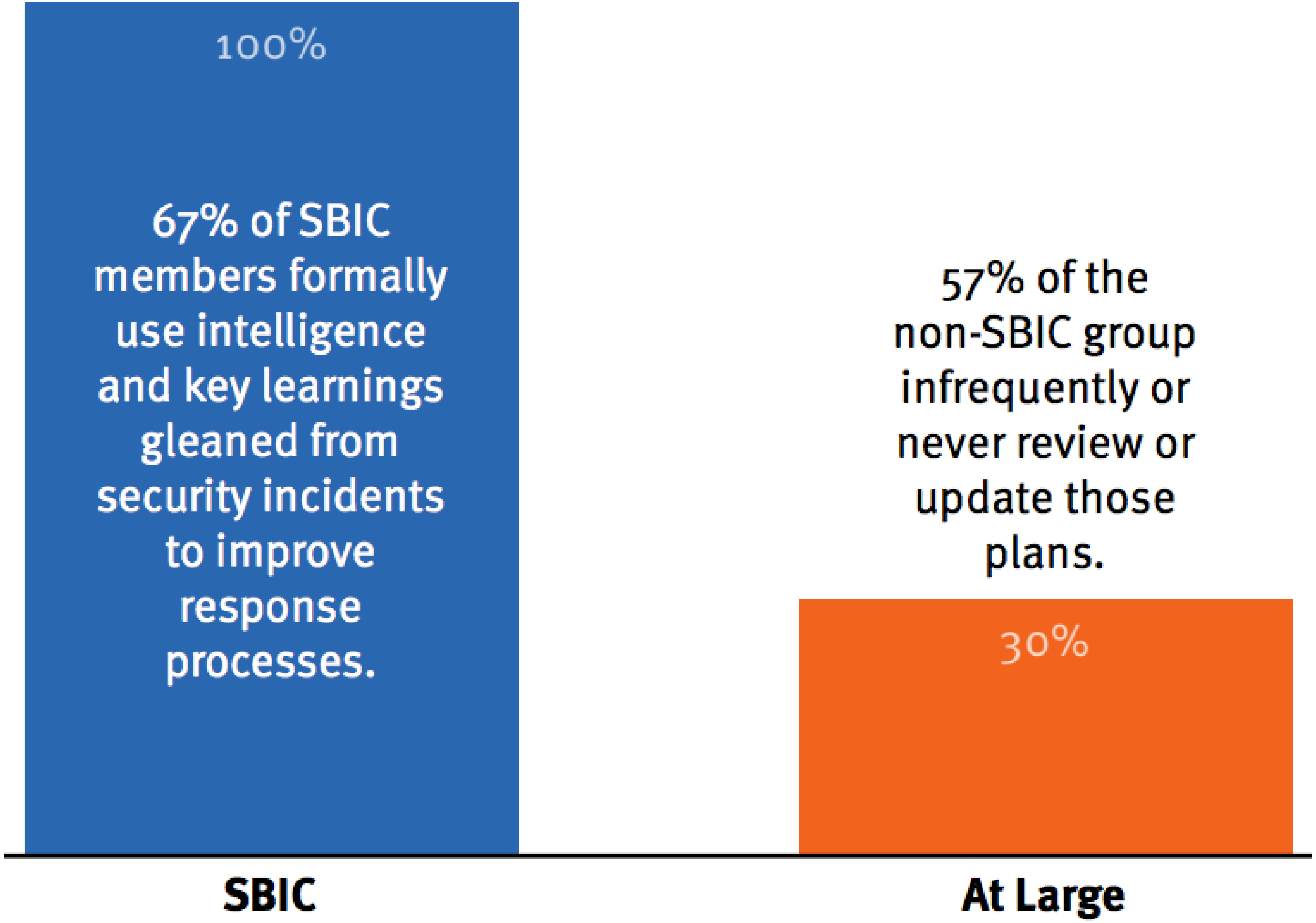
Example Steps



1. Start with network address obtained from threat intel
2. See which hosts have connected to that address…
3. Identify the processes associated with that communication
4. Learn provenance of those processes (context)
5. Derive new indicators from the process chain
6. See what other systems have those indicators

Don’t just have a plan… Review your plan and make sure it works

5



67% of SBIC members formally use intelligence and key learnings gleaned from security incidents to improve response processes.

57% of the non-SBIC group infrequently or never review or update those plans.

Have formal Incident Response plans in place.

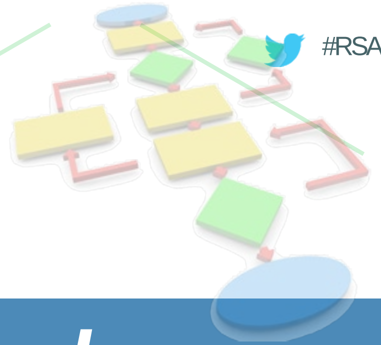
Incident Response planning has to be dynamic.

Organizations that fail to evaluate Incident Response plans against new threats expose their systems, data and infrastructure to attack.

prioritize

And use ***business context***

6



Balance between people, process, and technology

7

In Field Example

1. Identify initial malware (e.g., via traditional means or threat intel)

2. Has the malware been executed? How critical is the system?

3. Collect artifacts associated with that malware (e.g., parent files, domains collected, etc).

4. Find other endpoints/processes associated with those artifacts…

Seven Key Steps: Summary

1 Eliminate Perimeter / Prevention Mindset

2 Strive for pervasive visibility

3 Leverage and operationalize threat intelligence

4 Don’t sit back, be proactive

5 Don’t just have a plan, review your plan to make sure it works

6 Prioritize and use business context

7 Balance between people, process, and technology

Applying What You Have Learned…

Immediate:

- Review budget to see if it’s too prevention/perimeter focused
- Set-up regular review cadence for incident response plans

Intermediate term:

- Inventory your assets to identify what’s critical
- Identify your blind spots