RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO2-T07

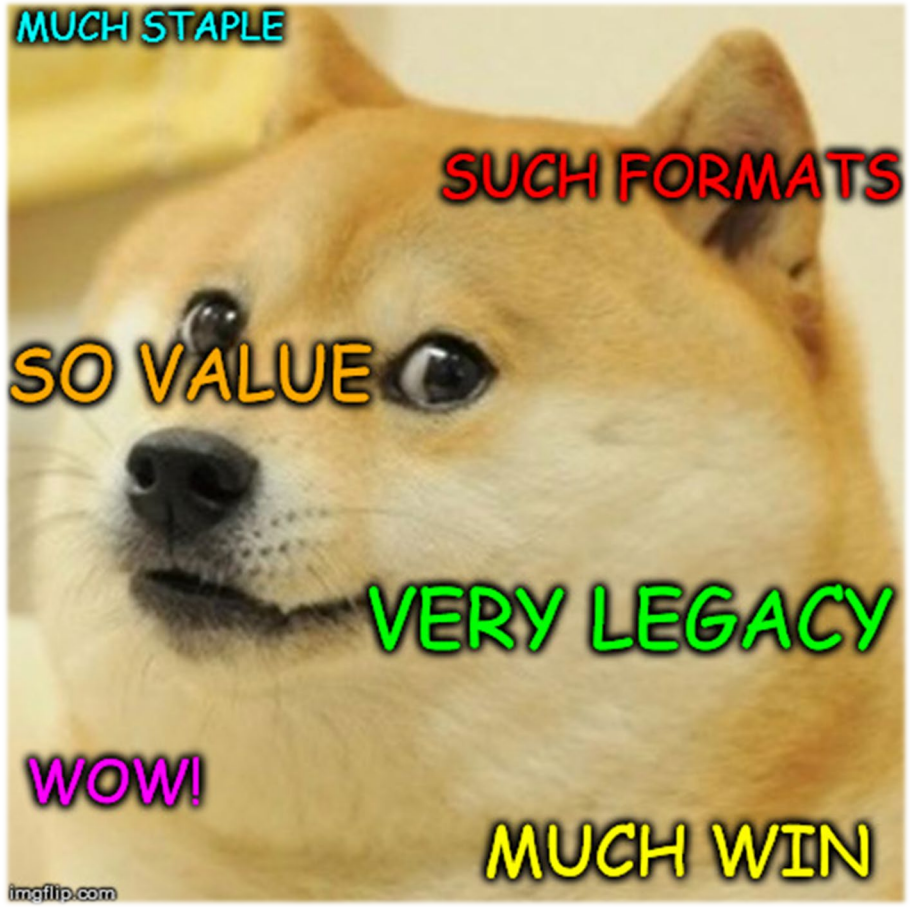
99 Security Tools and You Still Got Breached?

Matt Chiodi
Chief Security Officer, Public Cloud
Palo Alto Networks
@mattchiodi

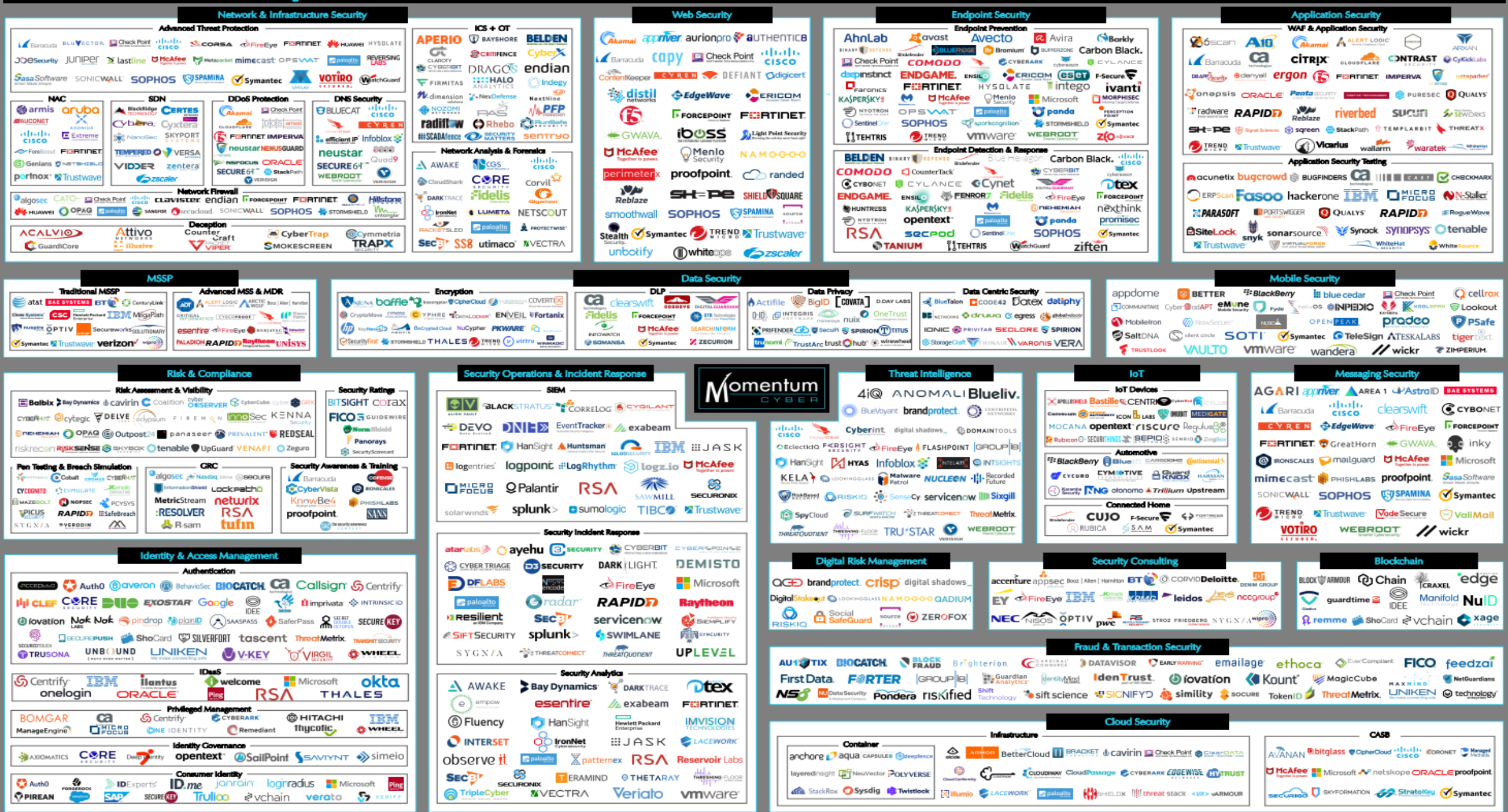
Sandy Wenzel
Consulting Engineer, SecOps
Palo Alto Networks
@malwaremama

Outcome

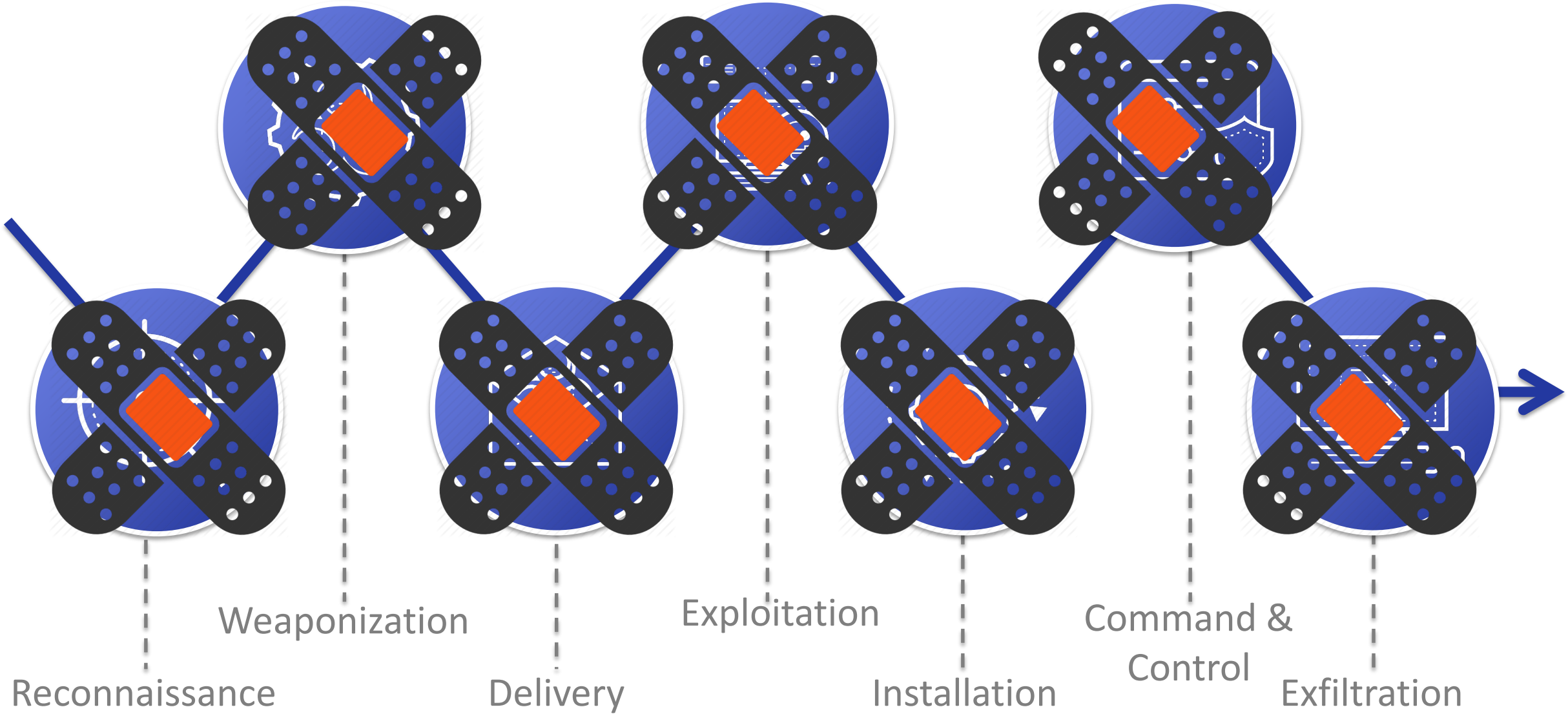
- Explain why “Best of Breed” ain’t workn’
  - Promise not to kill you with stats
- Apply the 80/20 rule to Cybersecurity
  - Impress your boss and colleagues
  - Actually reduce risk
- Demonstrate actionable steps to rationalize your security portfolio



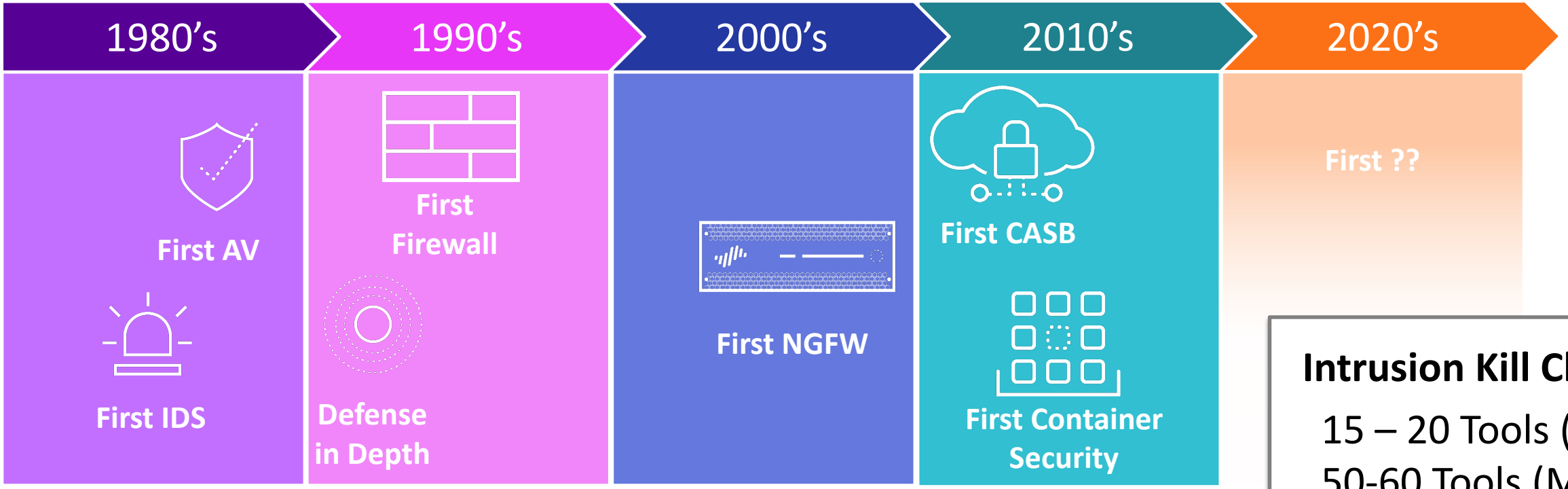
CYBERscape v2.5



Lockheed Martin Cyber Kill Chain



Point Products Are Killing Us



Intrusion Kill Chain

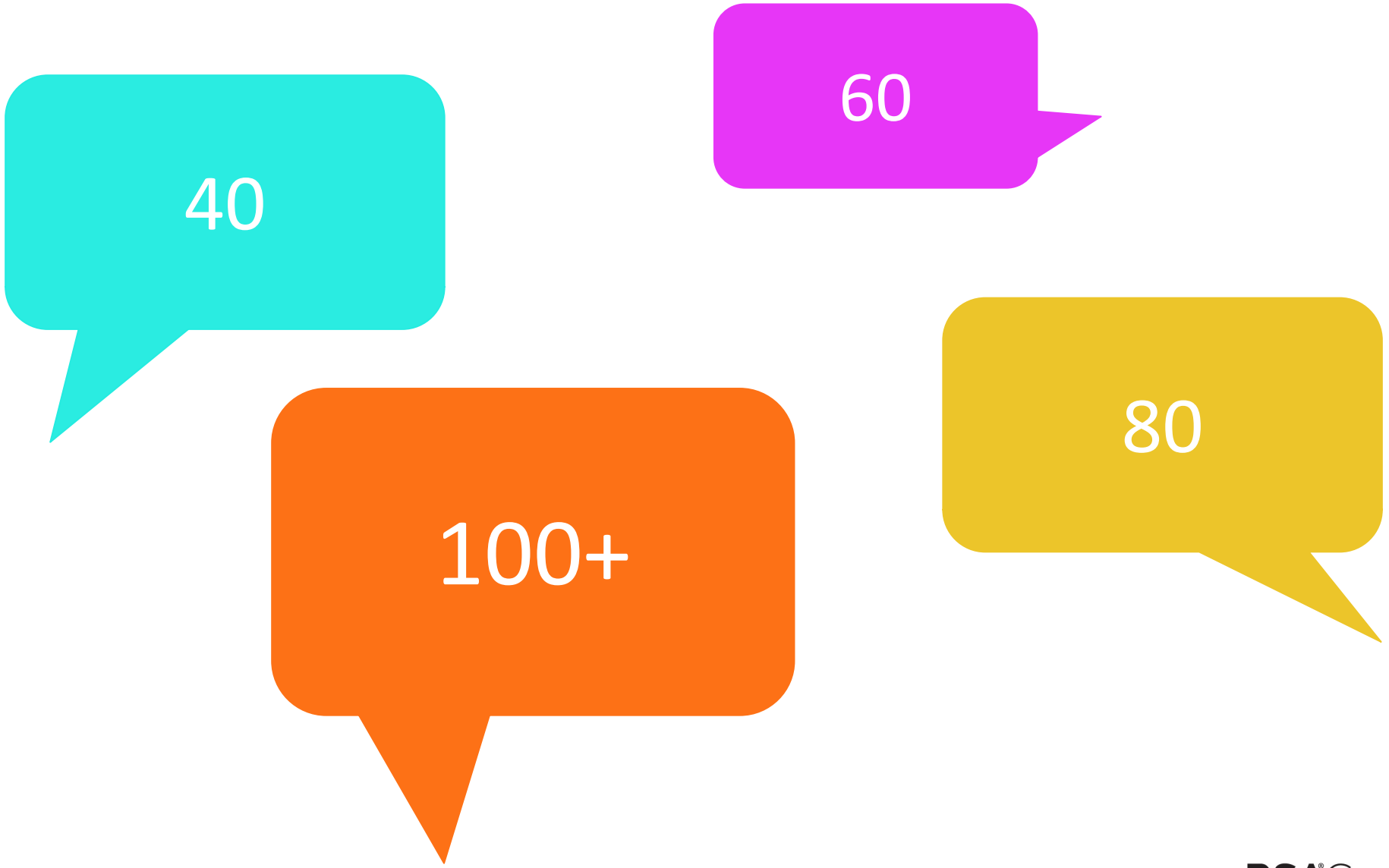
15 – 20 Tools (S)
50-60 Tools (M)
>130 Tools (L)

Layered Defense: Why It Worked

Pepperidge Farm Remembers…

The Hidden Costs of Point Products

Survey Time!



When people say:

“I liked your art/book/play. It was different.”

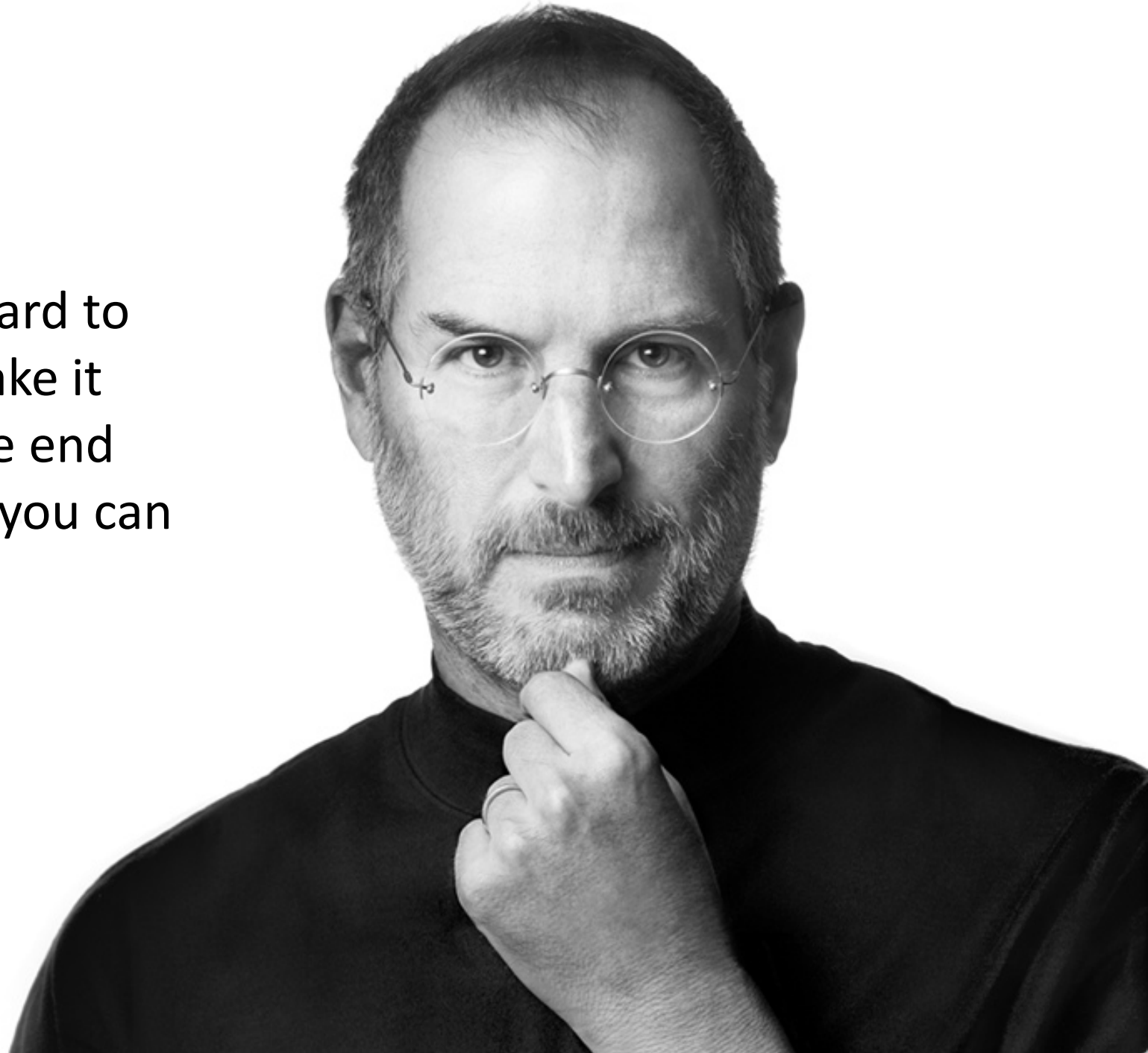
They really mean:

“It was weird and I didn’t like it.”

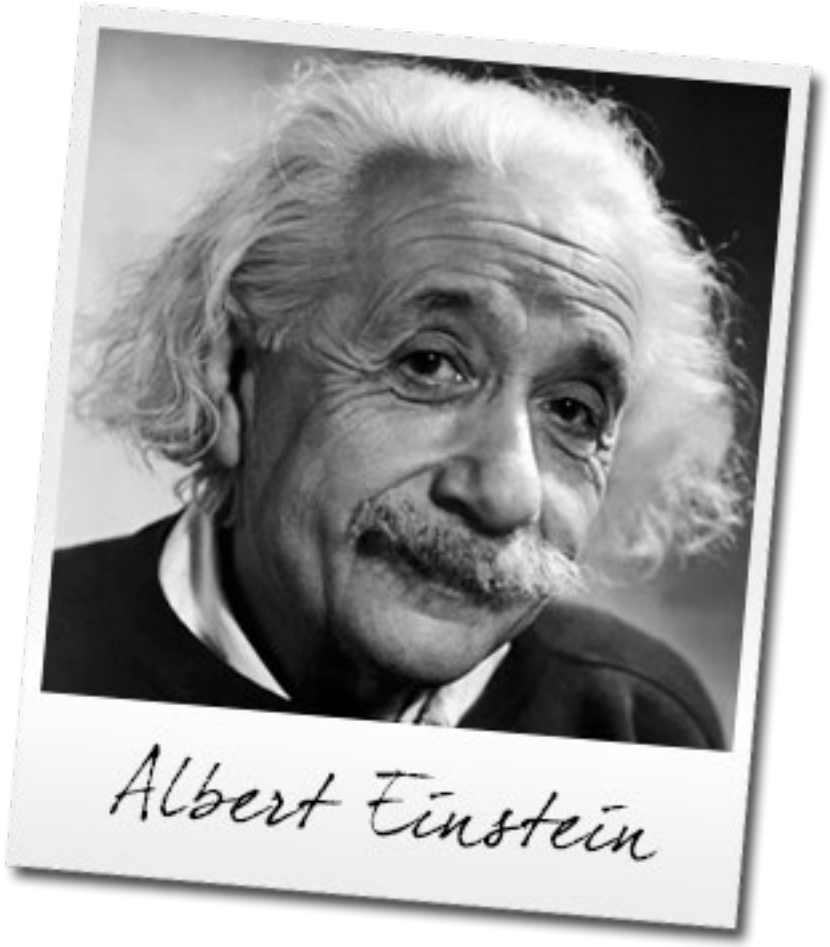
What we say:
46% consider effectiveness of a cybersecurity product the most important criteria

***What we actually do*:** Only 8% buy security products with integration and shared intelligence with other controls as their #1 priority

“Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple. But it’s worth it in the end because once you get there, you can move mountains.”
- Steve Jobs



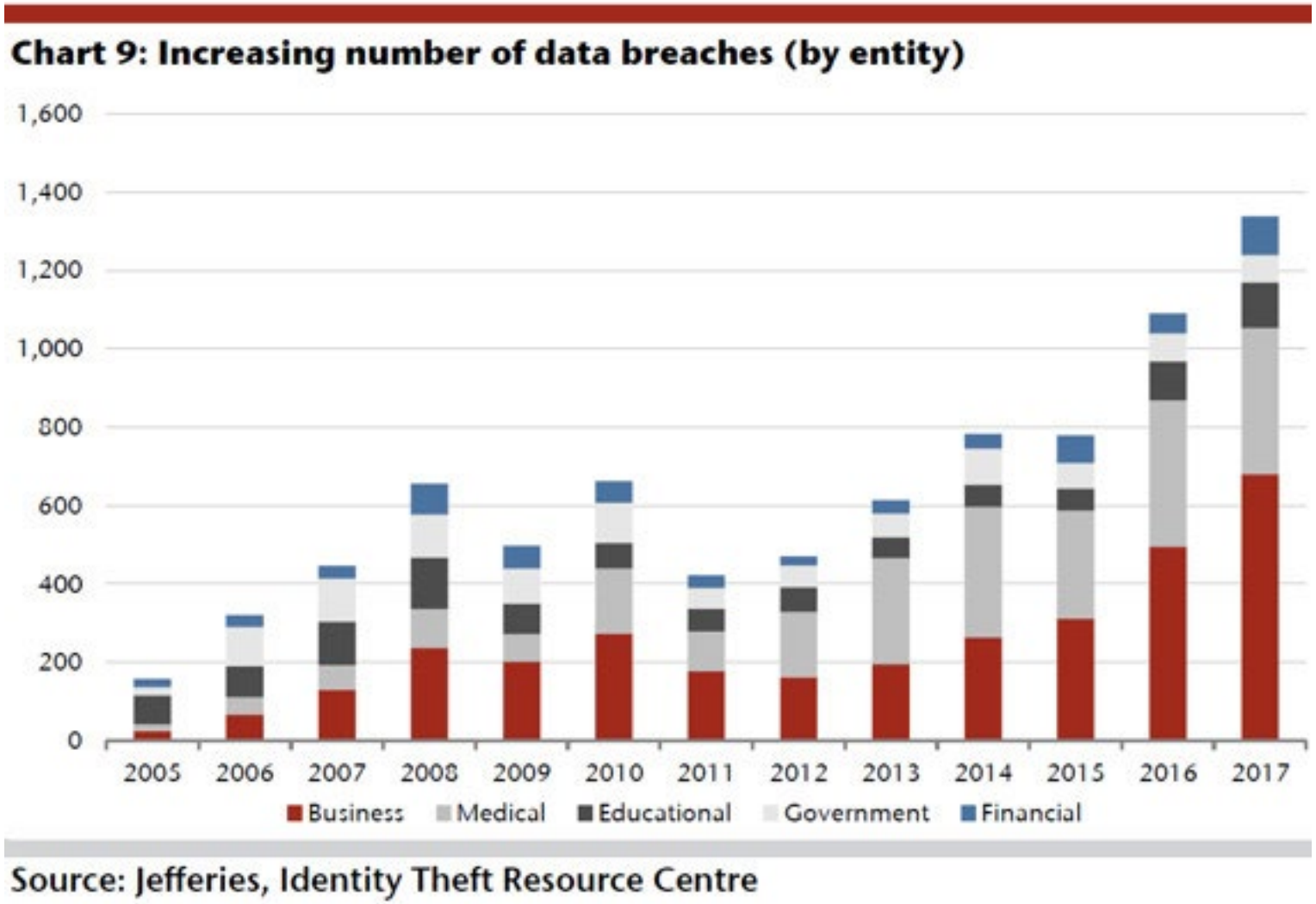
“EVERYTHING SHOULD BE MADE AS SIMPLE AS POSSIBLE, BUT NOT SIMPLER.”
—EINSTEIN



What we say:
54% only purchase best-of-breed <u>if they are designed for broader integration</u>

***What we actually do*:** 46% buy best-of-breed products regardless of the product's ability to integrate with other security technologies

Breach Stats: BoB Ain't Workn'



RSAConference2019

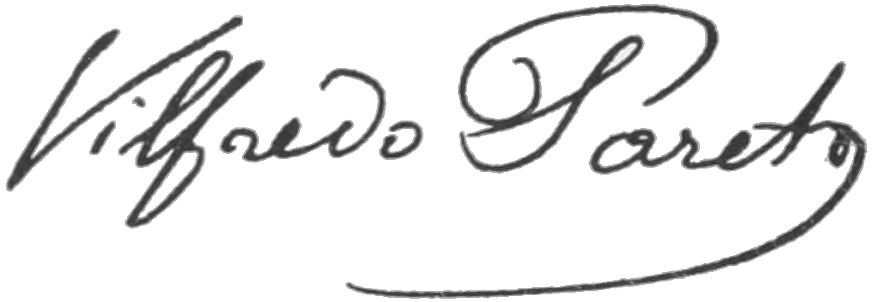
“We’re facing 21st century issues, discussing them in 20th century terms, and proposing 19th century solutions.”

- Tom Wheeler, former Chairman of the FCC

Who Was Vilfredo Pareto?

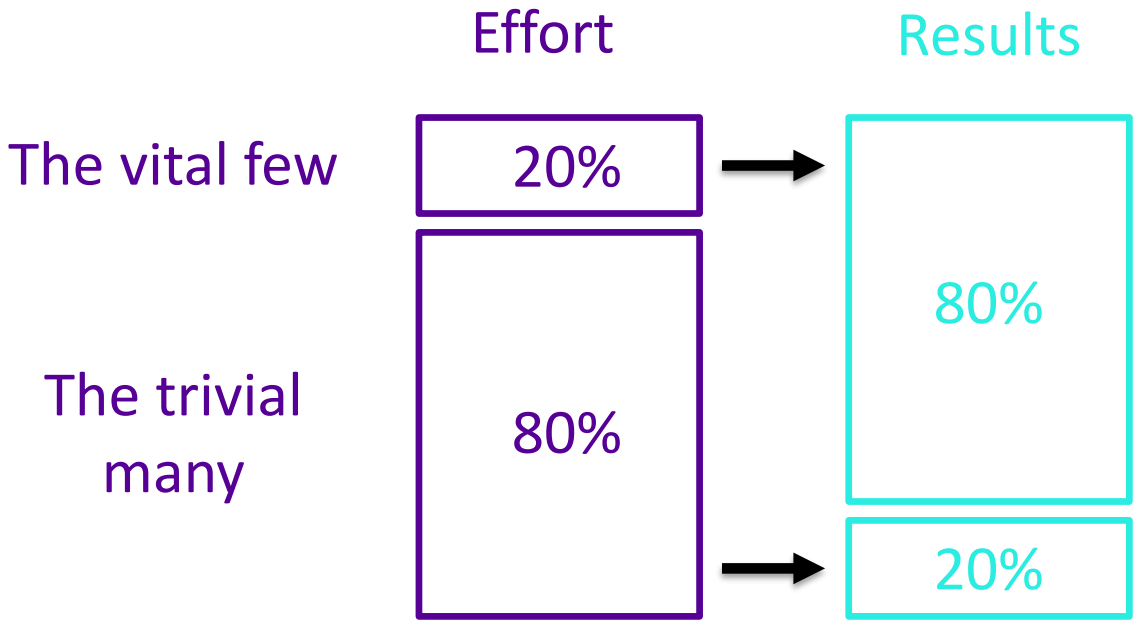
- Italian engineer, sociologist, economist, political scientist, and philosopher.
- Found 85% of wealth in Milan was owned by 15% of citizens.
- Observed 80% of Italy's land was owned by 20% of the people.

1848 - 1923



What Does the Pareto Principle Actually Say?

Investopedia: “[the Pareto Principle] specifies an unequal relationship between inputs and outputs. The principle states that 20% of the invested input is responsible for 80% of the results obtained. Put another way, 80% of consequences stem from 20 percent of the causes.”



80/20 Cybersecurity

- Australian Cyber Security Centre (ACSC) claims that when implemented effectively, the Essential Eight mitigates 85% of targeted cyber-attacks.
- Center for Internet Security (CIS) claims CIS-20 defeat 80% of common attacks.

80/20 Driveway Shoveling

- Could have taken 30+ minutes
- Spent 10
- Driveway 100% accessible

Applying the 80/20 Rule: NIST vs. ACSC

NIST 800-53r4

- 965 controls
- 20% of 965 = 193
- 80% of 965 = 772

NIST

ACSC Australian Cyber Security Centre

8 controls

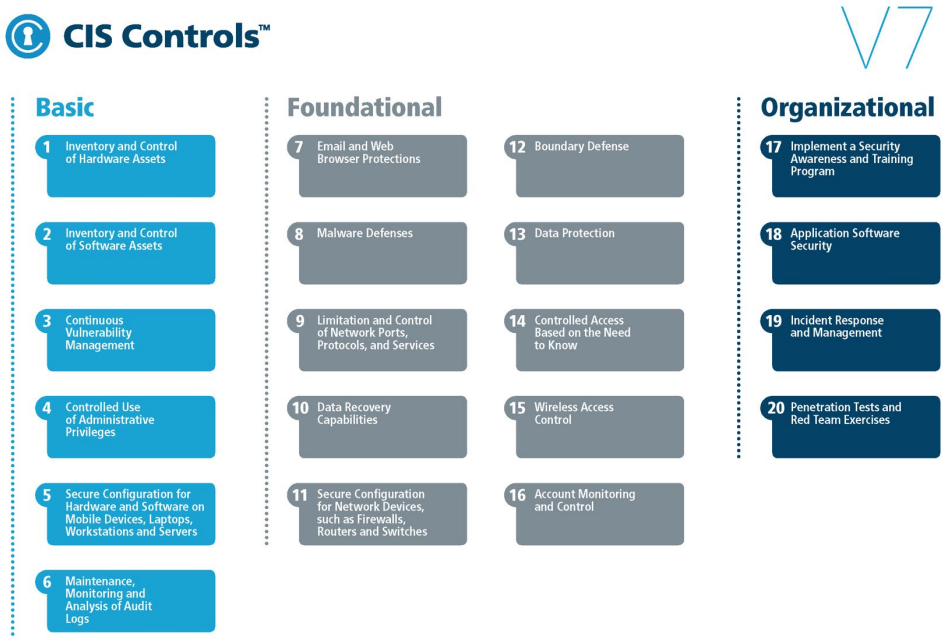
Applying the 80/20 Rule: NIST vs. CIS-20

NIST 800-53r4

- 965 controls
- 20% of 965 = 193
- 80% of 965 = 772

CIS-20

149 sub-controls



mindset

"Security is a ~~process~~, not a product."

– Bruce Schneier (April, 2000)

Step 1: Inventory Existing Security Tools

- Create a spreadsheet that lists out all tools
- Why was it originally purchased? (find the RFP)
- Quantify investments with major vendors
- Document features *actively* used vs. available
- How does it share threat intelligence?

What Your Tools Inventory Might Look Like…

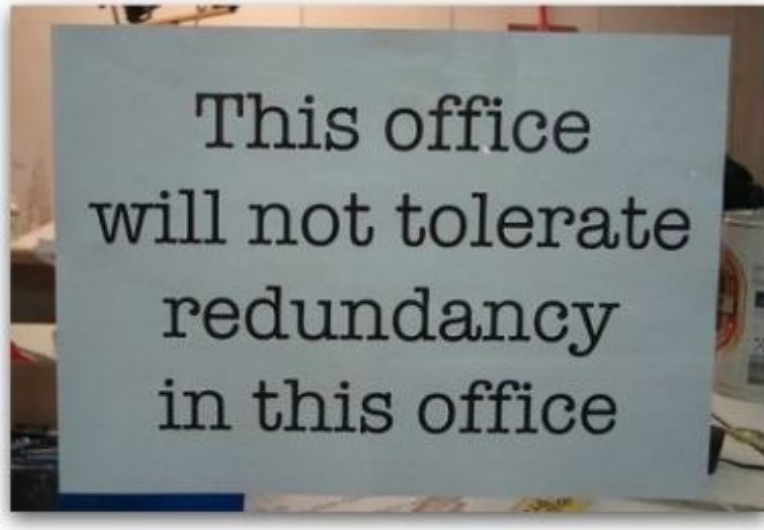
Product Name	Vendor	Risk Target	CIS Control Mapping	Features in use	Integration Capabilities	Stand-alone or platform
SuperUltimateSecurity	Acme	Public cloud infra compliance and security	Inventory and Control of Assets, Security configurations of servers,Secure Configuration for NW devices, firewalls, Boundary Defense	Inventory; IR; secure config	Open API	Platform
BigBadSecurity	Big Security 123	Network security	Limitation and control of network ports, protocols and services; boundary defense; IR and management	Basic firewall	Partial	Stand-alone
Hacker9	Networking Big Company	Endpoint security	Continuous vulnerability management, Secure configs of workstations and servers, malware defenses, Data protection, Application Security, IR and management	IR, vuln management, asset inventory	Open API	Platform

Step 2: Create a Tools Coverage Map

- Determine your critical coverage categories (CIS-20, Essential 8, etc.)
- Analyze how well each tool covers the category
- Be amazed with how much overlap you have

Tools Coverage Map Might Look Like This…

	Vendor X Product Y	Vendor X Product YY	Vendor X Product YYZ	Vendor X Product XYZ	Vendor A Product Y	Vendor B Product C	Vendor C Product X	Vendor N Product K
Privilege Management	●							
Whitelisting	●	●						
Client-Based Proxy			●			●		
Traditional AV					●	●		
Firewall				●		●		
Memory Protection				●	●	●	●	●
Cloud Sec				●		●	●	●
Next-Gen Antimalware						●	●	●
Real-time Endpoint Query								◑



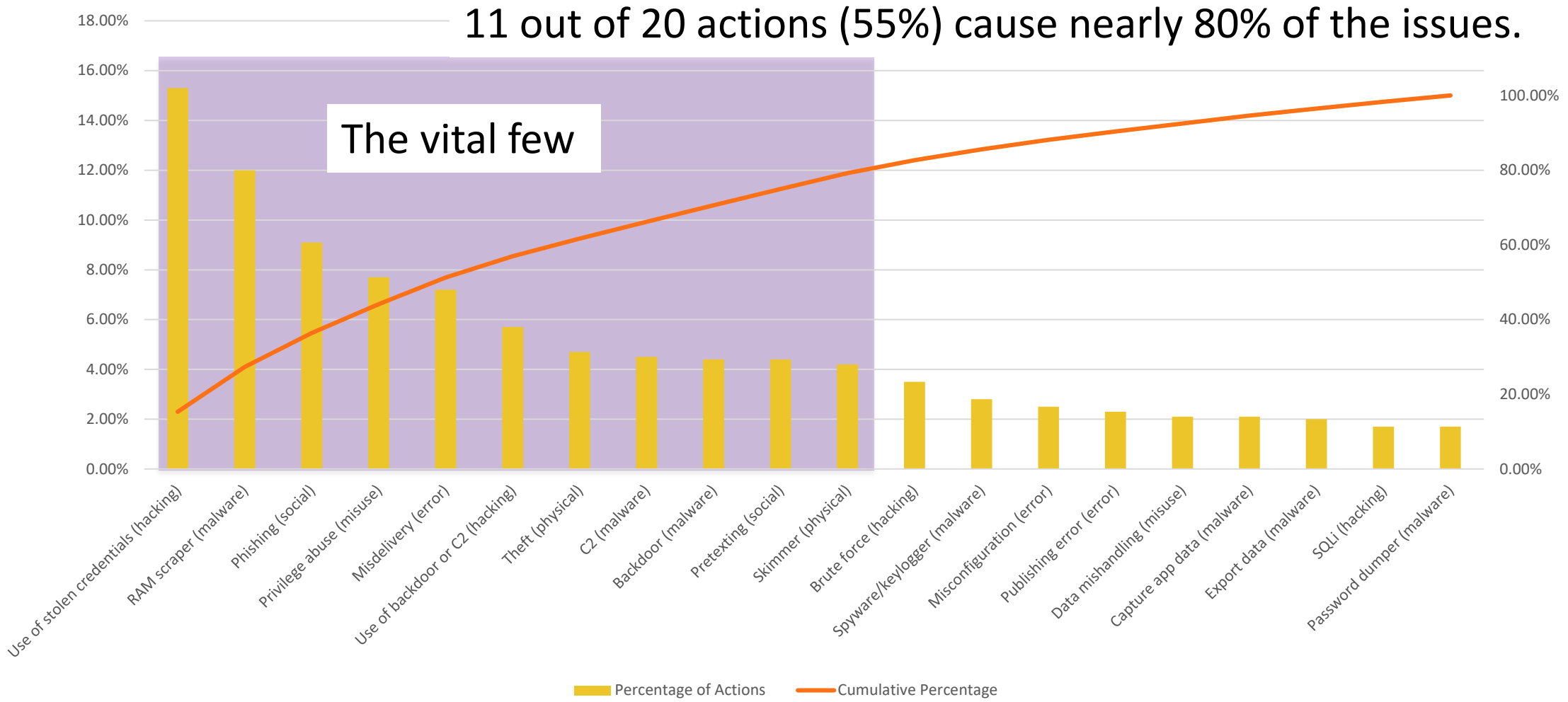
Step 3: Compile and Categorize Your List of Incidents

- Work with your SOC/IR team
- Create or utilize existing set of actions (or use DBIR's)
- Track the following for each action:
  - Number of occurrences
  - Percentage of total
  - Cumulative percentage

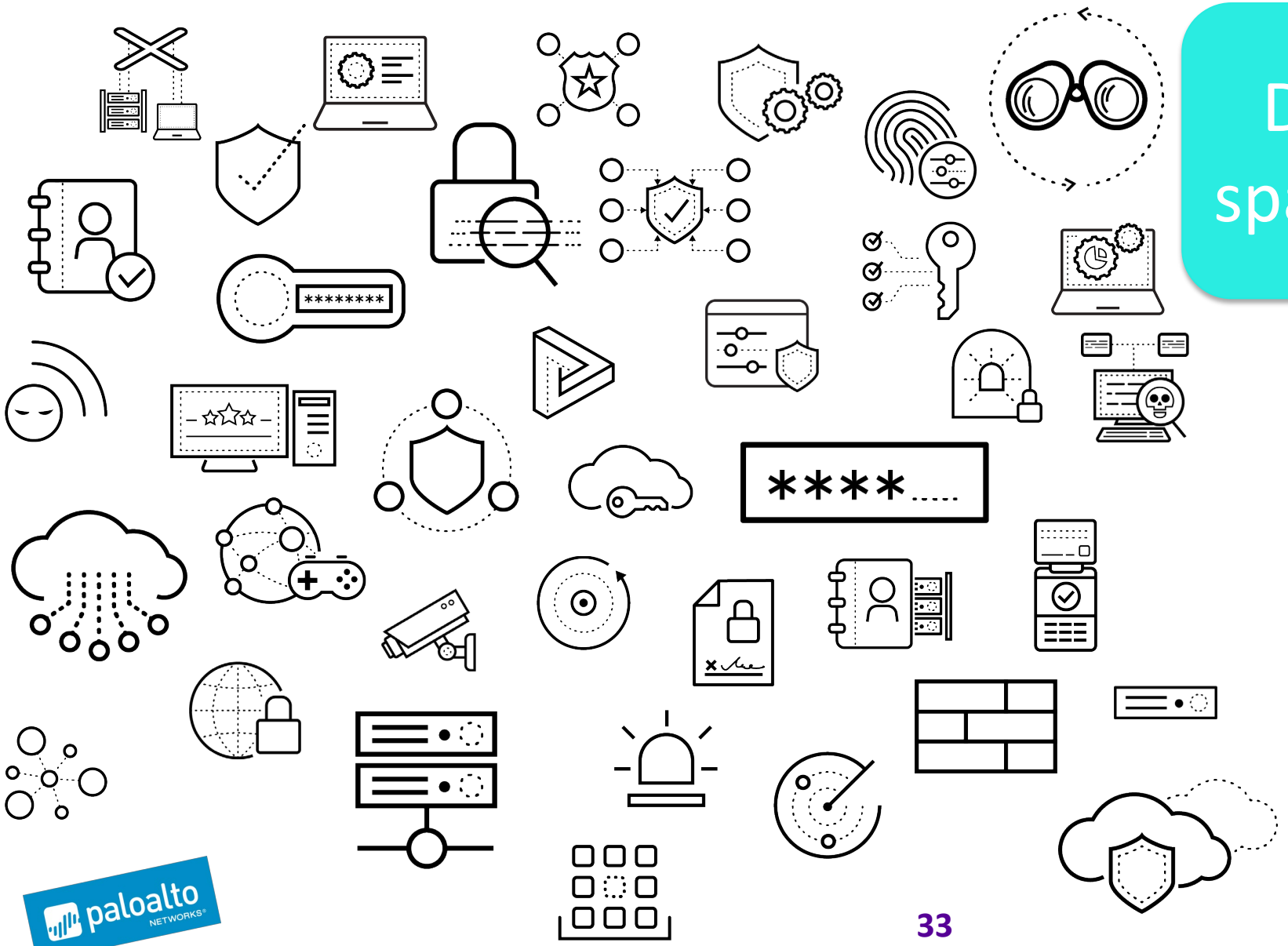
Your Actions Might Look Like…2018 DBIR Top 20

#	Action	Number	Percentage of Actions	Cumulative Percentage
1	Use of stolen credentials (hacking)	399	15.30%	15.30%
2	RAM scraper (malware)	312	12.00%	27.30%
3	Phishing (social)	236	9.10%	36.40%
4	Privilege abuse (misuse)	201	7.70%	44.10%
5	Misdelivery (error)	187	7.20%	51.30%
6	Use of backdoor or C2 (hacking)	148	5.70%	57.00%
7	Theft (physical)	123	4.70%	61.70%
8	C2 (malware)	117	4.50%	66.20%
9	Backdoor (malware)	115	4.40%	70.60%
10	Pretexting (social)	114	4.40%	75.00%
11	Skimmer (physical)	109	4.20%	79.20%
12	Brute force (hacking)	92	3.50%	82.70%
13	Spyware/keylogger (malware)	74	2.80%	85.60%
14	Misconfiguration (error)	66	2.50%	88.10%
15	Publishing error (error)	59	2.30%	90.40%
16	Data mishandling (misuse)	55	2.10%	92.50%
17	Capture app data (malware)	54	2.10%	94.60%
18	Export data (malware)	51	2.00%	96.50%
19	SQLi (hacking)	45	1.70%	98.30%
20	Password dumper (malware)	45	1.70%	100.00%
	Total	**2602**		

Pareto Analysis of the 2018 DBIR Top 20



Step 4: Map Security Portfolio to Your Vital Few



Does it spark joy?

Your Vital Few Mapping Might Look Like…

	Vendor X Product X	Vendor X Product Y	Vendor X Product Z	Vendor X Product ZZ	Vendor X Product ZZZ	Vendor X Product ZZZZ	Vendor Y Product X	Vendor G Product C	Vendor L Product N
Use of stolen credentials (hacking)	●								
RAM scraper (malware)	●	●							
Phishing (social)			●					◑	
Privilege abuse (misuse)									
Misdelivery (error)				●					
Use of backdoor or C2 (hacking)		◑					●		◑
Theft (physical)									
C2 (malware)	●					●	●	●	
Backdoor (malware)	◑		●	●	●			◑	
Pretexting (social)		◑							
Skimmer (physical)									◑

RSAConference2019

Make Your Move

Leveraging the Power of the Platform

- First ~30 Days
  - Read *The 80/20 Principle* by Richard Koch, take a ton of notes
  - Meet with all cyber team leads and *begin* inventory of tools in use (buy list too)
- Within ~60 days
  - Expand tools inventory with risk statements and incident #'s
  - Get really clear on how your tools are integrated—or not
- Within ~90 days
  - Map to your vital few and present to your major vendors
  - Create plan moving to ~80% single vendor
  - Develop game plan qualifying your ~20% best-of-breed