RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CSV-R11

The Advantage of Ignoring the Long Tail of Security: A Product View

James DeLuccia

Cybersecurity Cloud B2C & B2B, New Products, Honeywell

James DeLuccia

- Part of product engineering at Honeywell

- **Core mission**: Help create delightful customer experiences
- **Major project work**: Develop and introduce enhanced cybersecurity work patterns and technology on Azure
- **Scale**: Honeywell's customers make up roughly 25% of all buildings globally; operate 300+ subscriptions online, and 100s of products online
- **History**: 25+ years in technology; Writer, Researcher, Patents

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

RSAConference2019

Product considerations

Honeywell Buildings Technology

- We currently serve 25% of all buildings in the world
- 1,000s of products that depend on the cloud service providers
- 100s of cloud subscriptions and millions of resources
- Millions of hardware end-points (IOT), handheld devices, and more with orchestration between fixed locations and the cloud
- Ongoing Challenge
  - Deliver to market expectations, regulations, and a brand of trust
  - Heavy evolution in our space
  - Transformation of technology available in our space and utility
  - Churn in regulation and geo-political relations impact our supply chain

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

Global product footprint, team, and market

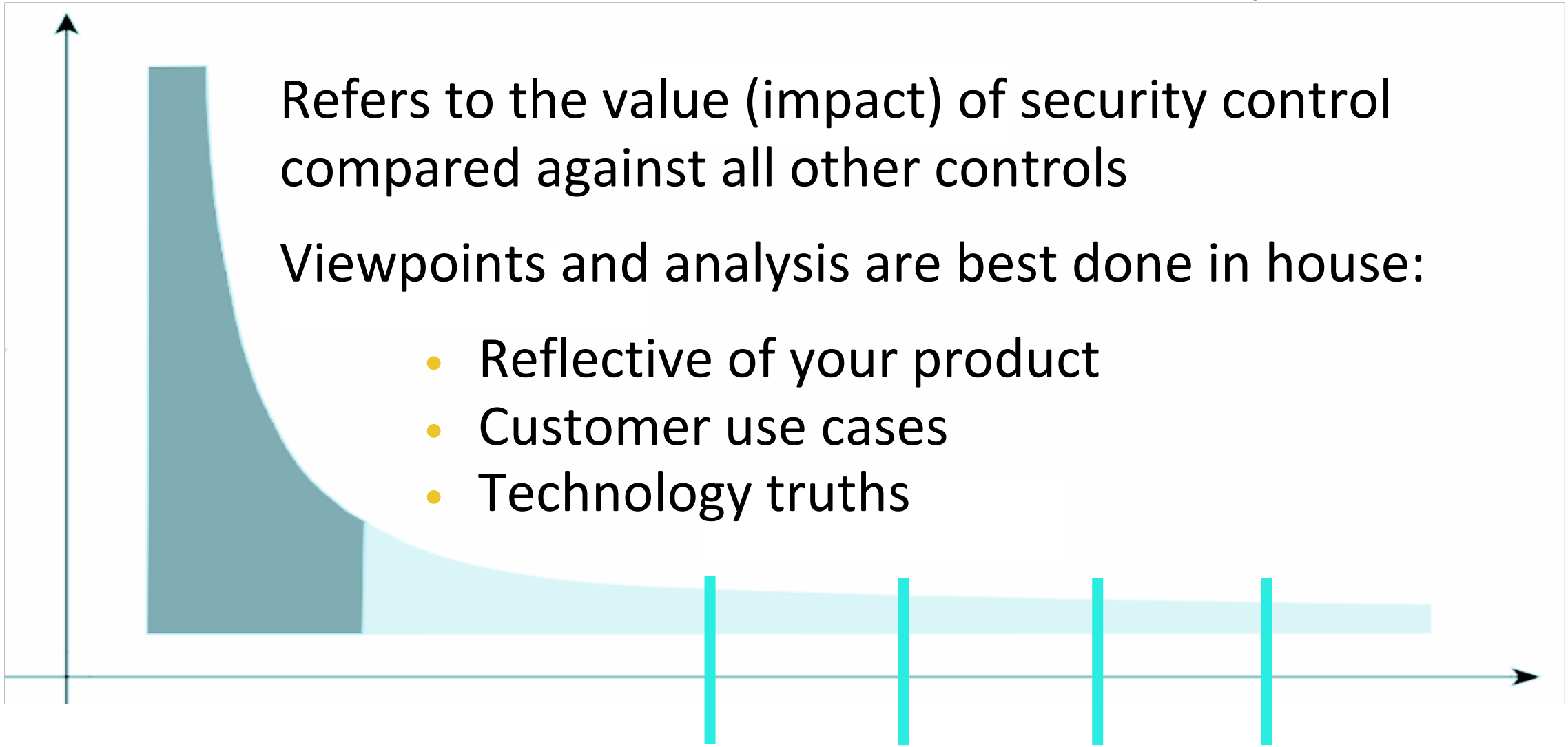
- We build and sell products globally
- Leverage the leading cloud service providers
- Have a globally deployed team that reflects our developers
- Serve global markets and thus coordinate closely with local authorities and local partners

RSAConference2019

What is the long tail of security controls

Practicality and focus

Long Tail of Security Controls



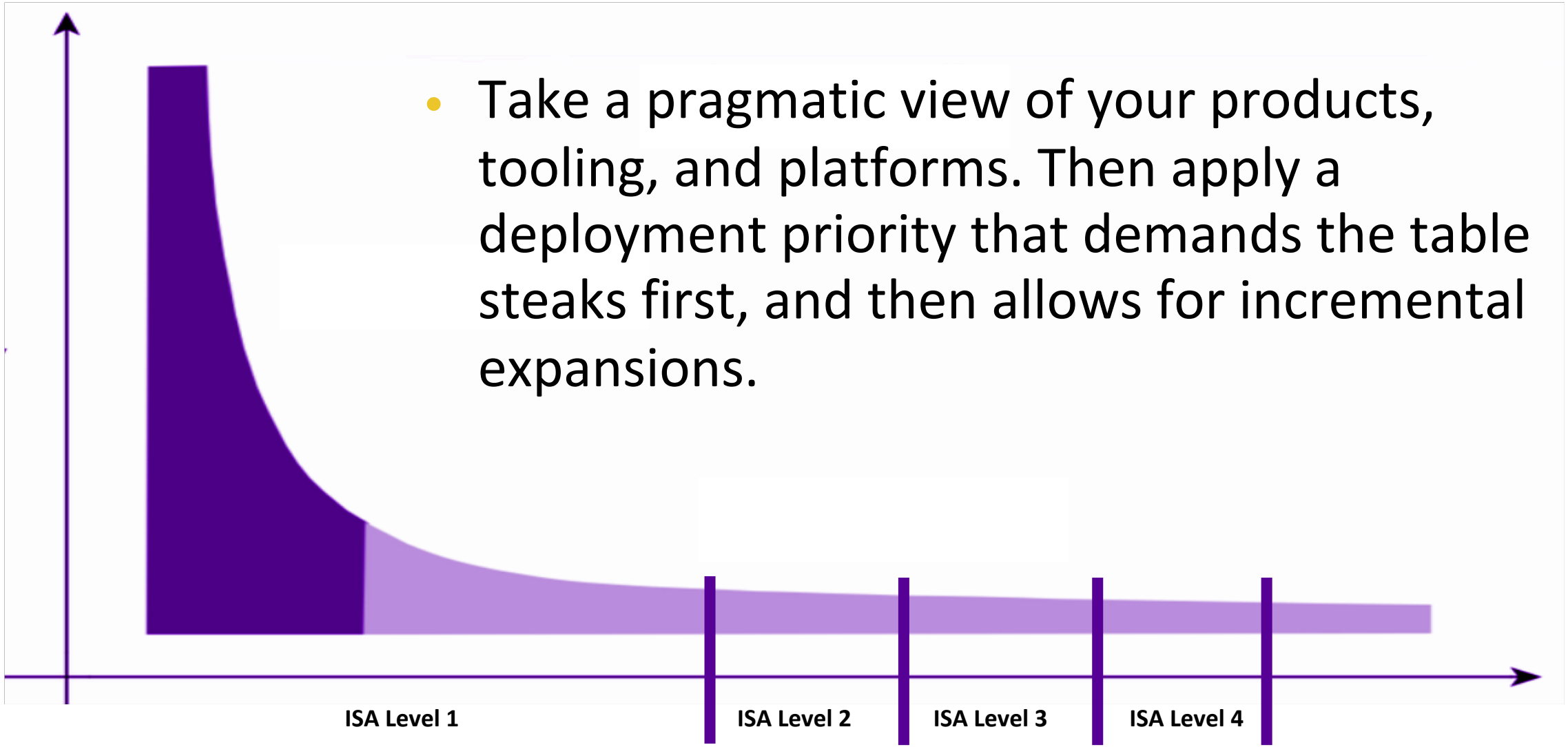
Refers to the value (impact) of security control compared against all other controls

Viewpoints and analysis are best done in house:

- Reflective of your product
- Customer use cases
- Technology truths

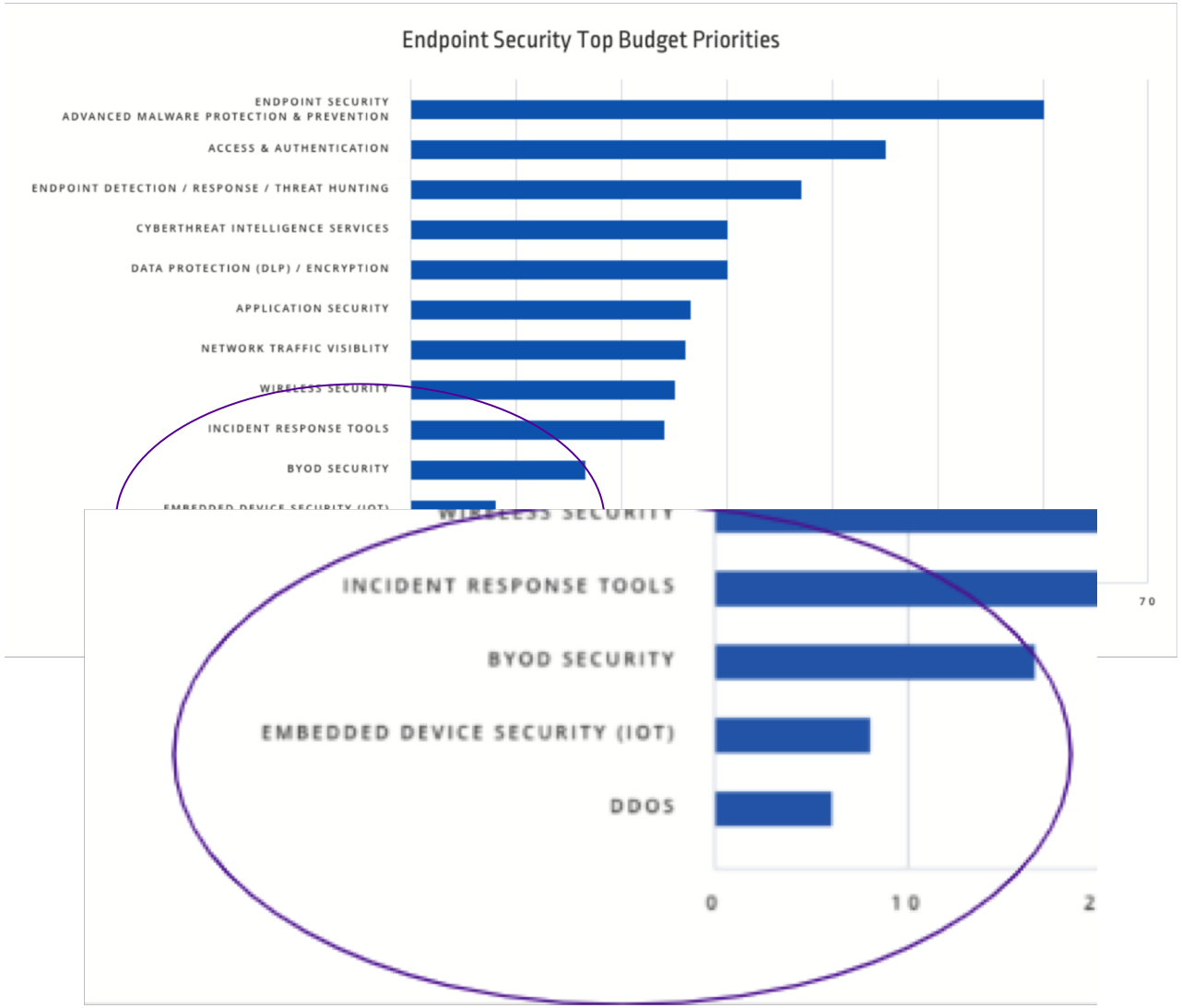
Long Tail of Security Controls

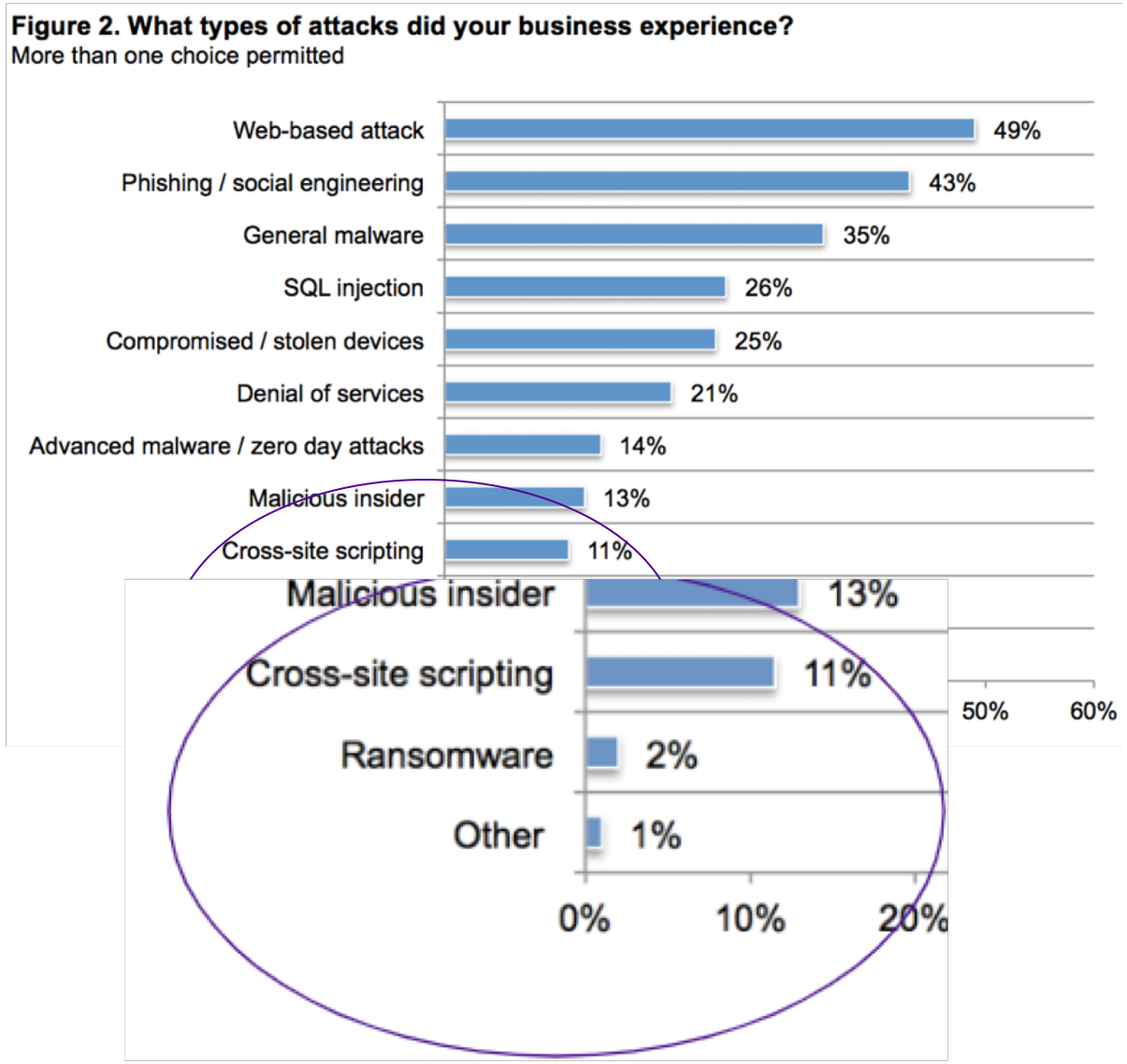
- Take a pragmatic view of your products, tooling, and platforms. Then apply a deployment priority that demands the table steaks first, and then allows for incremental expansions.



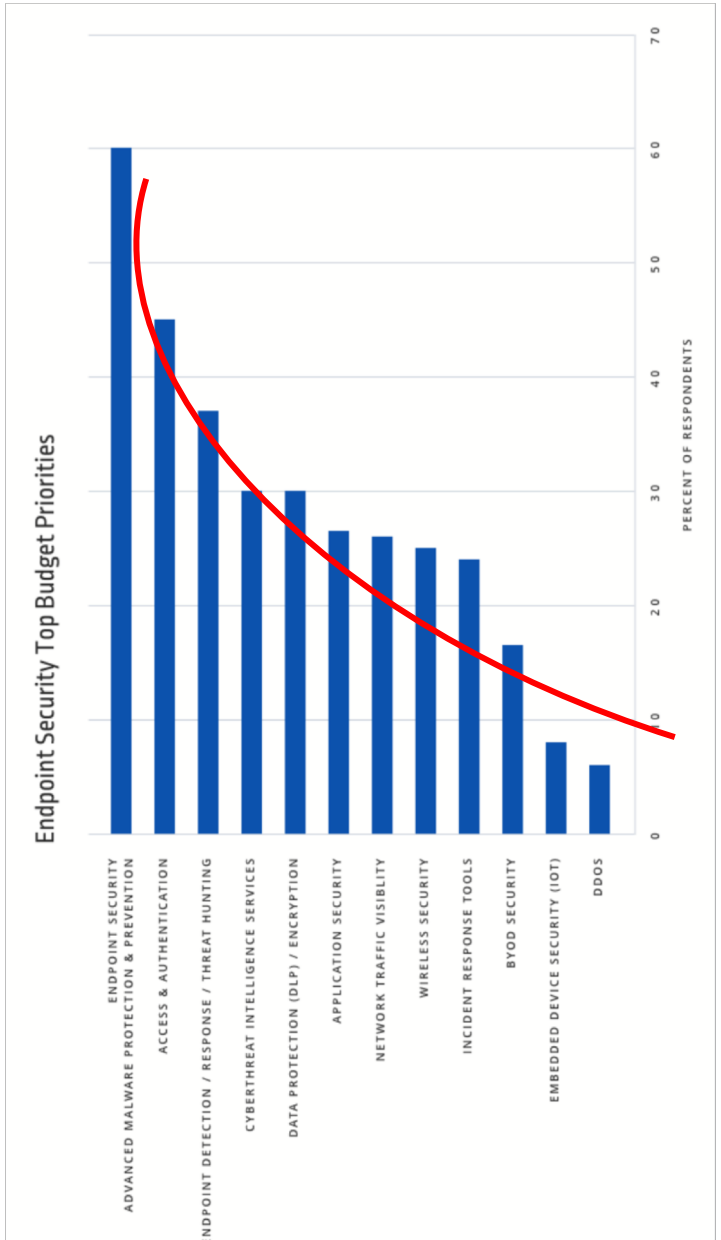
DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

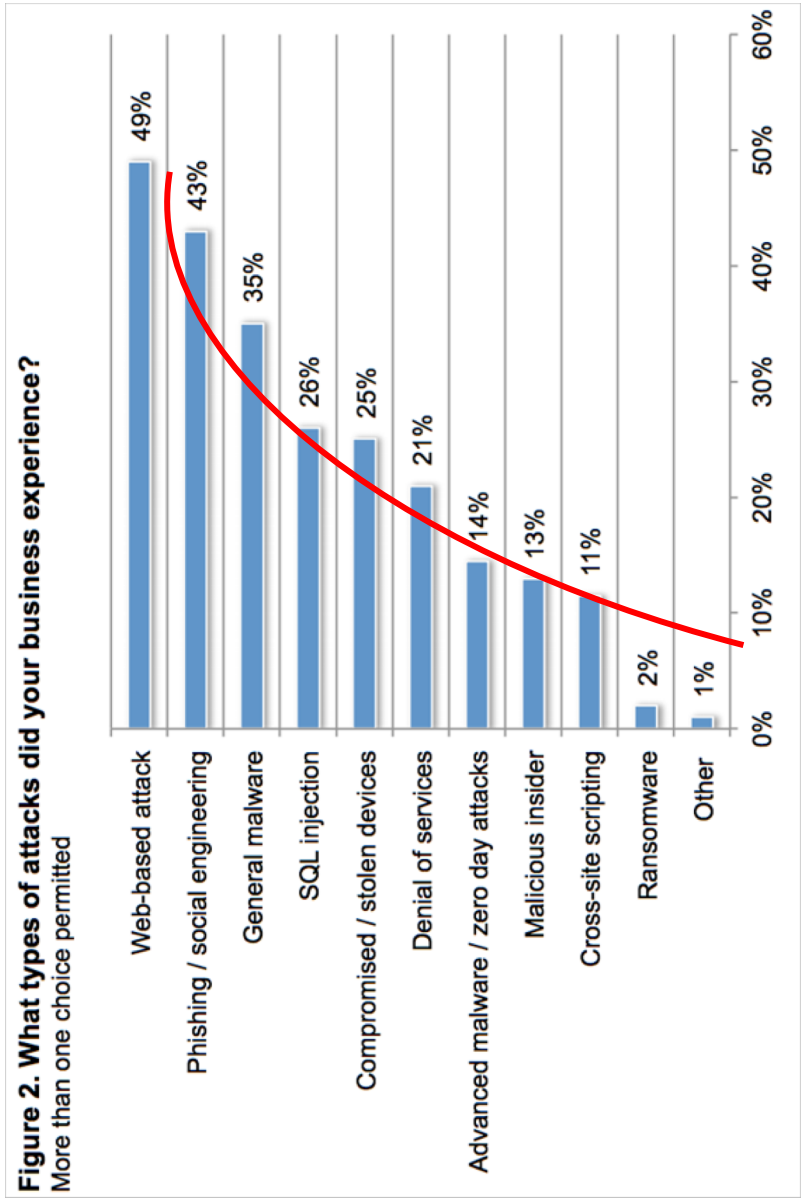
Context matters, examples



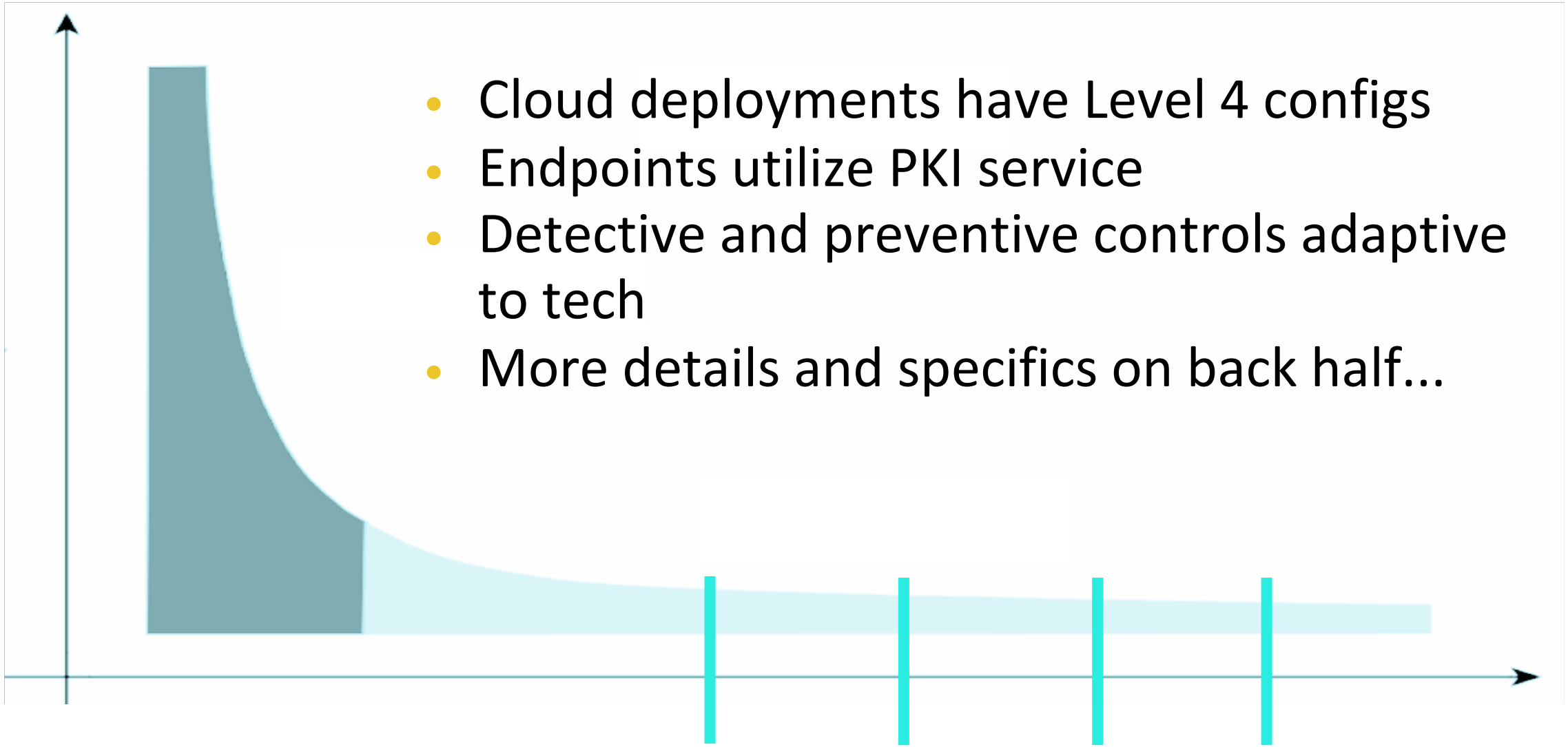


Relevance Matters More





Based on this lens, we prioritize controls



- Cloud deployments have Level 4 configs
- Endpoints utilize PKI service
- Detective and preventive controls adaptive to tech
- More details and specifics on back half…

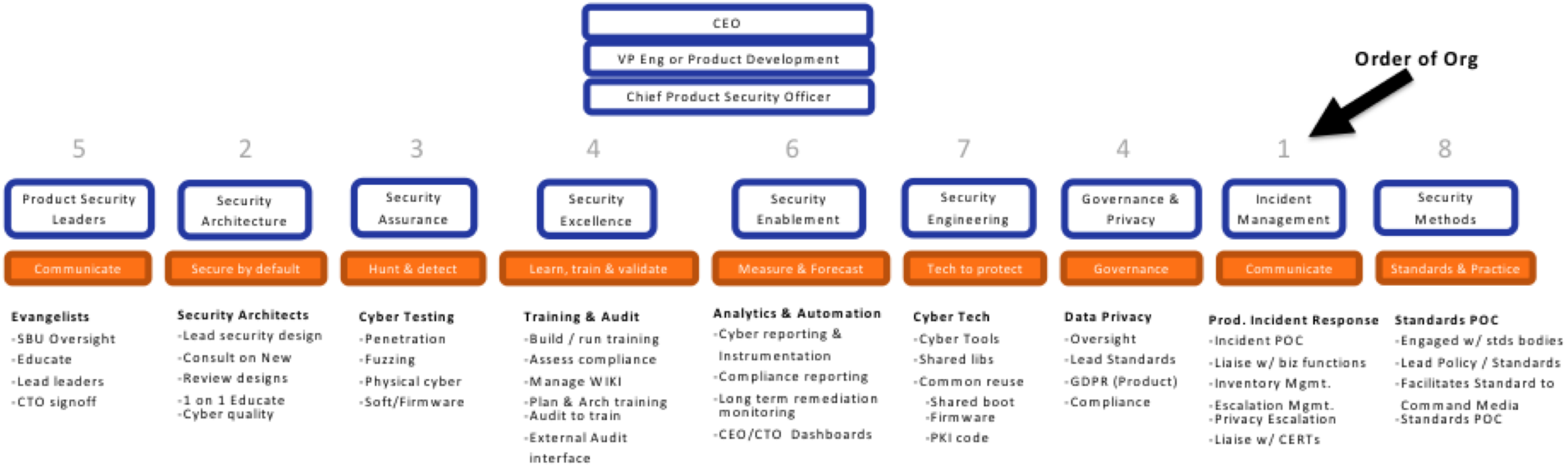
DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

RSAConference2019

Demonstrative Product Security Model

Practical and based on multi-organizational practices to deliver global digital and physical products w/ the cloud

Demonstrative Organizational Roles & Priority



Don't have to report into one – some can matrix

PROGRAM Backbone - Standards

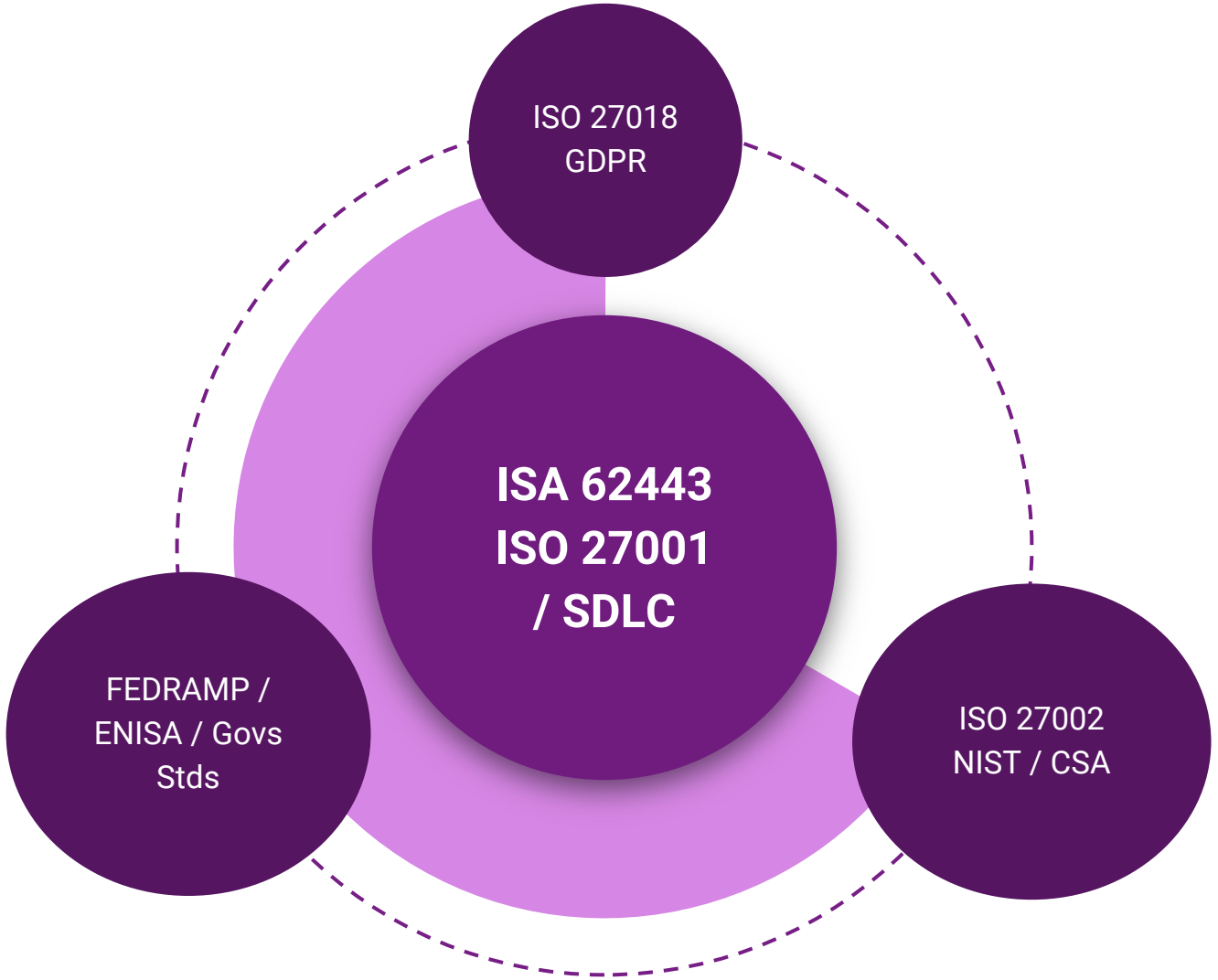
Demonstrative Examples:

- **IOT/IIOT** = ISA/IEC 62443 , (DRAFT) NIST IOT Baseline
- **Cloud** = CSA STAR, SOC 2 Type 2.
- **Product or Process Certifications** = ISASecure, UL 29001
- **People** = CSSLP, Ethical Hacker, CCSK, CCSP, CISSP
  + ISA/IEC 62443 Cybersecurity certificates
- **SSDL** = Microsoft Security Development Lifecycle

Together these guide our core controls
Architects define our product controls

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

Set your management system and then layer in controls



DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

RSAConference2019

How to focus your cybersecurity resources

Demonstrative method and tactics for product teams

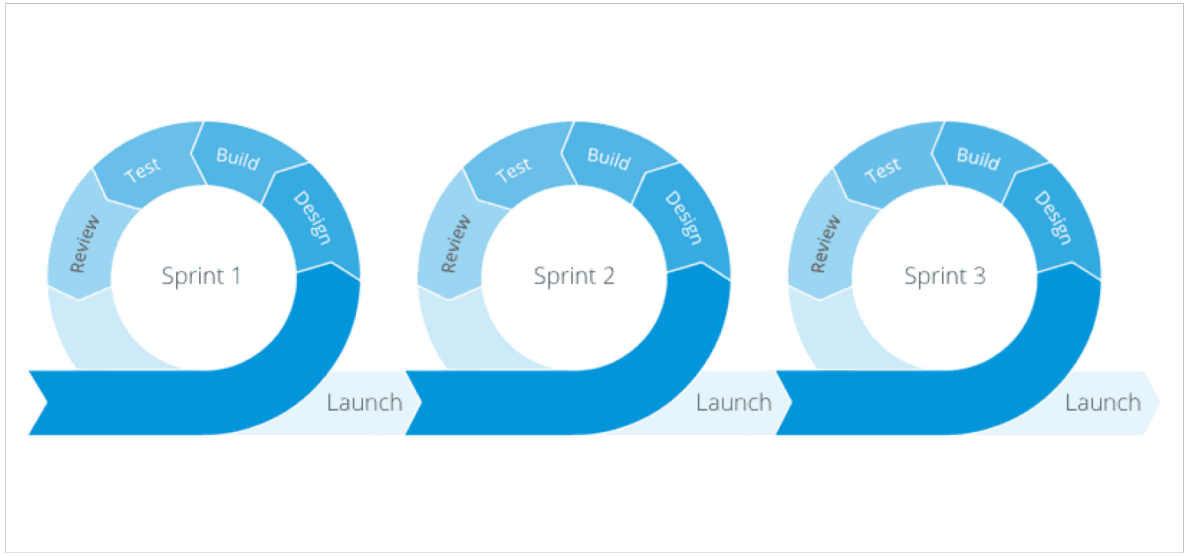
6. Embed and own the SDLC process

Start	Requirements	Design	Development	Testing	Deployment	Maintenance & EOL
Involve Security Architect	Security / Privacy Requirements	Threat Model	Threat Model	Security Tests	Security Review Checklist	"Wash/Repeat" SSDL
	Security Review Checklist	Security Tests	Security /Privacy Requirements	Security Risks	Security Risks	Revise PIA/DPIA
		Security Review Checklist	Security Manual		PIA/DPIA Review	Revise Threat Model
	Security Risks	Security/Privacy Requirements	PIA/DPIA		SIGN OFF	Cust Comms & PSIRT
		Security Risks				

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

5. Live with your developers, residents vs. guests

- Be a part of the Product Planning and design discussions
- JOIN daily stand-ups and sprints
- Embrace their development cycles
- Deploy Architects to development teams to build together
- Mutually accountable for product delivery and success



DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

4. Invent and create alternatives

- You are not a robot, yet …
- *Adapt cybersecurity requirements to the actual world*
- *Set infrastructure; intent & guidance*
  - *Limit cognitive dissonance with choices (NetFlix)*
  - *Platforms and shared components ← Cyber security helps source*

Encryption Guidance	Public Network	Private Network
Sensitive Data	HIGHEST	HIGHEST
Non Sensitive Data	LOWEST	LOWEST

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

3. Track, Log exceptions, and escalate

- Code **evolves** and gets **reused**, thus our tickets allow us to keep practicality match to new truths.
  - Assumptions evolve
  - Client environments change
  - Scope of product impact shifts
- All impact risk management and mitigation considerations
- All exceptions go beyond the security architect on the project:
  - Product Security Leaders
  - Chief Technology Officers (monthly)

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

2. Build and scale your knowledge with broader engineering

- Create the Passionate Few across the engineering organization
  - Individuals not owned by Cyber or matrixed into cyber
  - Give them training and free resources to develop their skill sets
  - Support and over deliver on growing their careers
- We are not creating cybersecurity professionals, we are making the engineering teams better

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

1. We must evolve too

- Our programs must also constantly evolve
  - Weekly track our security metrics across all phases, programs, and work with escalations directly
  - Monthly review over entire governance, documentation (training, and operational wikis), and make updates broadly
  - Sit with our engineers, participate in planning at the business and product level (early identify skill sets and tools we need)
  - Report up to the CTO and CEO level; risks to act on, and customer impact
  - Annually we globally get together for deep dives & program updates

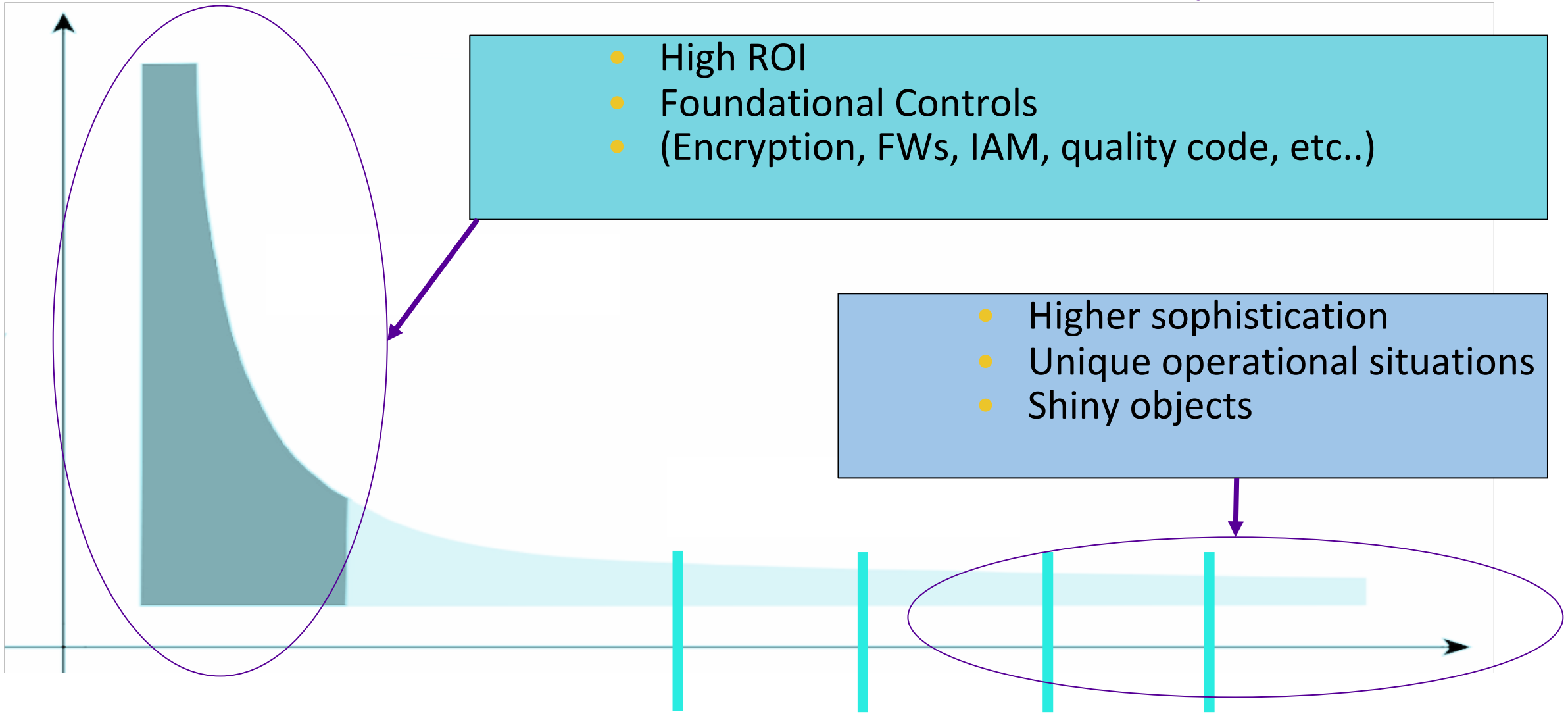
DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

RSAConference2019

Shiny Objects - resist

Long Tail - Foundational vs Shiny Controls

Send feedback to
@jdeluccia on twitter



DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

History supports that core elemental focus is critical

NOTHING has changed in the past 10 years -

- OWASP Top 10,
- SANS Top 20,
- Verizon Data Breach

…..top causes of breach **remain fairly constant**

The right thing is still the right thing

The only variable is are you having to edge more and less practical controls given the platform and customer nuances

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

Why IGNORING the shiny objects benefits you…

- Allows you to improve on strengths
- Resources spent on where we gain the biggest impact
- Are we really stopping an APT
- Prevents fatigue of cybersecurity in engineering teams
- Prevents burn out from cybersecurity team
- Brain matter can focus on the organization's custom needs …… I have found these to disproportionately impactful at Google, Microsoft, and now Honeywell

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

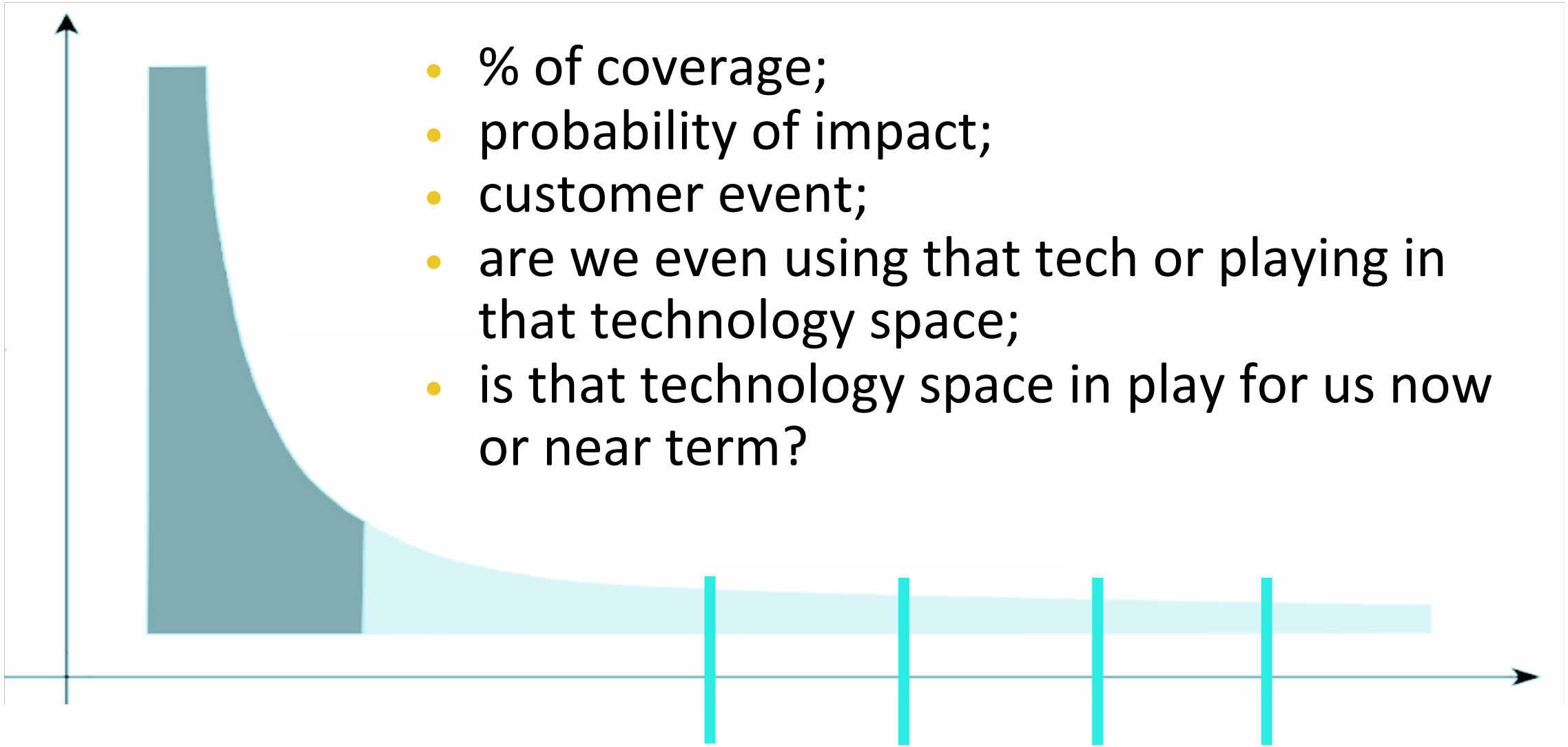
A few of my favorite ‘Shiny Objects’

Don’t buy these or be distracted by them…

- Quantum Computing mood rings
- Diamond studded Blockchain charms
- Deception based security
- Cyber warfare tools
- Cryptojacking Attacks
- Coinminers

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

How can you measure shiny impact needs for your org?



- % of coverage;
- probability of impact;
- customer event;
- are we even using that tech or playing in that technology space;
- is that technology space in play for us now or near term?

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

RSAConference2019

Our focus for tomorrow

What should be our focus over the next few years?

- Supply chain - hardware, software, and partnerships in the market (less isolation and more collaboration)
- Abstraction of services - continued refactoring of code and product stack
- Growth of cybersecurity standards and practices across our sectors
- Elemental security - further expanded

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

Actions, the most important

- Audit your coverage of security programs with the development of new products (are you involved cradle to grave?)
- Create clarity of security objectives against product types and your own control reference standard
- Connected products establish core basics - 100% vision of resources; automation of scripts that trigger; empower
- Conduct root cause analysis against engineer behaviors to discover cultural manifestations of policy

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD

Please grab the expanded list of my cloud security control recommendations for businesses in 2019 now on slideshare.

All available for free on Slideshare, 50+ articles posted on LinkedIN:

LI: James DeLuccia
Twitter: @jdeluccia

My greatest thanks

DO GOOD
GIVE YOUR TIME
HELP OUR WORLD