RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CSV-F02

Hacking Your Security Culture for the Cloud

Brian Riley

Senior Director, Global Cyber Risk Management
Liberty Mutual Insurance

or: How an InfoSec Curmudgeon Learned to Stop Worrying and Love the Cloud

$ whoami

Brian Riley, Senior Director

- Global Cyber Risk Management
- 25 years of experience with cybersecurity in financial services

Liberty Mutual

At Liberty, we believe progress happens when people feel secure.

Liberty by the numbers

- Founded 1912, based in Boston
- Nearly 50,000 employees in 30 countries and economies worldwide
- 5th largest global P&C insurer*
- Ranked 75th on Fortune 100 list of largest companies*

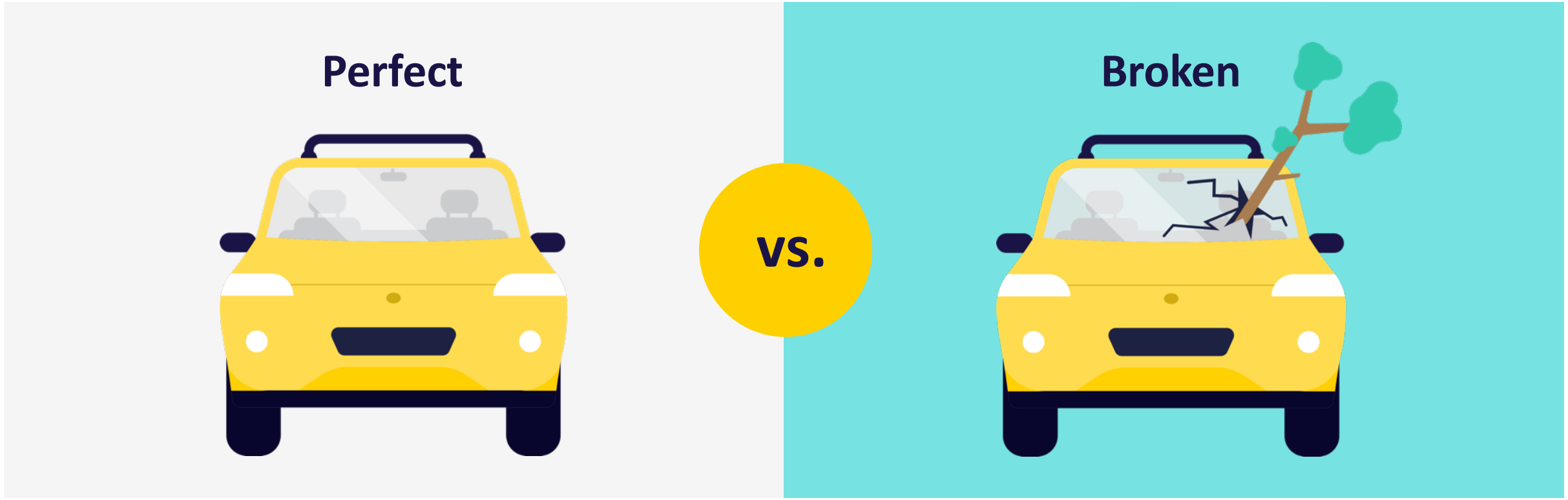
*Based 2018 gross written premium and revenue, respectively.

An early (mistaken) understanding of the Cloud

"I'll tell you exactly what Cloud Computing is… Cloud is nothing more than the current crop of **vacuous, meaningless marketing nonsense** that vendors use to try to open new markets. It really means nothing but is generally applied to **large-scale virtualization** (which we have been doing for years), **just with fewer controls and less oversight.**"

– B. Riley, 9/2013

The classic InfoSec mindset



Early steps: Drawing some wrong conclusions

The cloud is really just our 4th Data Center. So let's protect it with the same controls we use in the other three.

But we know how to do all of this. If the cloud is just another data center, why is it so hard to do what just works everywhere else?

Thinking differently

"We cannot **solve** our problems with the **same thinking** we used when we **created** them."

– Albert Einstein

Implications for security: Two paradigms shift

Cloud computing shifts the economics of security in ways that affect both attackers and enterprises.

Data Centers

Servers are fixed assets that depreciate over time, creating the incentive to keep systems around for as long as possible to maximize return on investment – creating many traditional security problems.

Cloud environments

We pay only for what we use, creating the incentive to destroy environments as quickly as possible and rebuild them only when they are needed. This reduces risk (a threat can only be persistent in an environment that is persistent).

Everything is software – which presents opportunities and creates new challenges

Opportunities

- Infrastructure and applications are built consistently through automation, simplifying disaster recovery
- Security and compliance controls can be automated, offering continuous compliance
- Automated deployments reduces the need for human interaction with systems, limiting insider threats and risk of misconfiguration
- Some security controls are much easier to implement in the cloud

Challenges

- Traditional handoffs and security checks no longer occur
- While automation eliminates many common risks, mistakes can have much bigger impact
- Some security controls are harder or more expensive to implement in the cloud

But the Cloud is more complicated!

How much should a developer need to think about the way BGP is configured in our network routing?

Is an understanding of how packets route relevant to making the right choices about firewall rules?

With developers defining AWS Security Groups in CFTs, do we give enough tools to help people code the right rules?

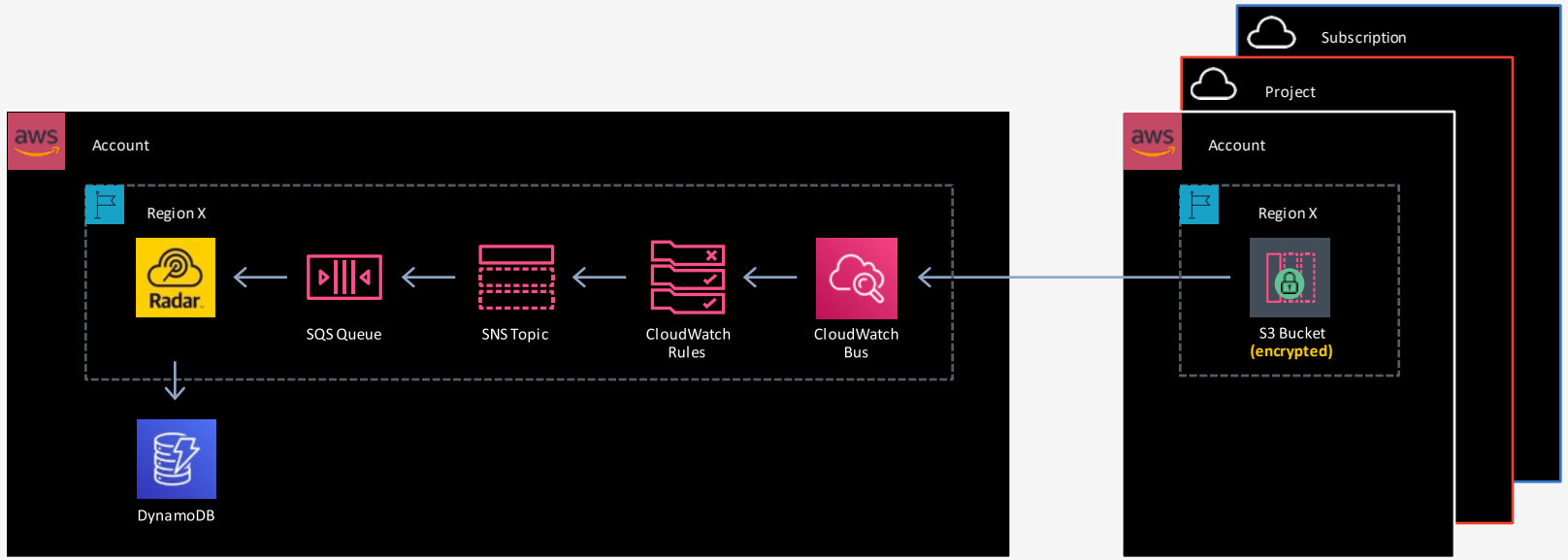
RSAConference2020

Tools to hack your culture

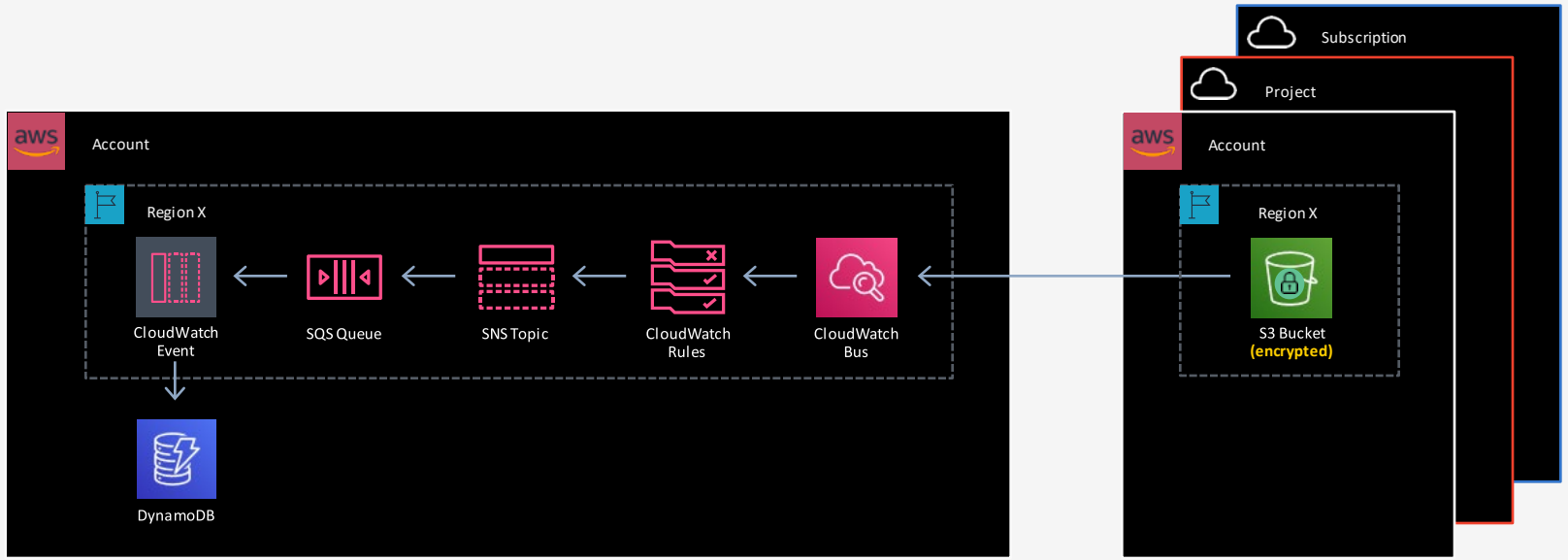
Infrastructure as code *requires* security as code


Radar
TM

Radar architecture

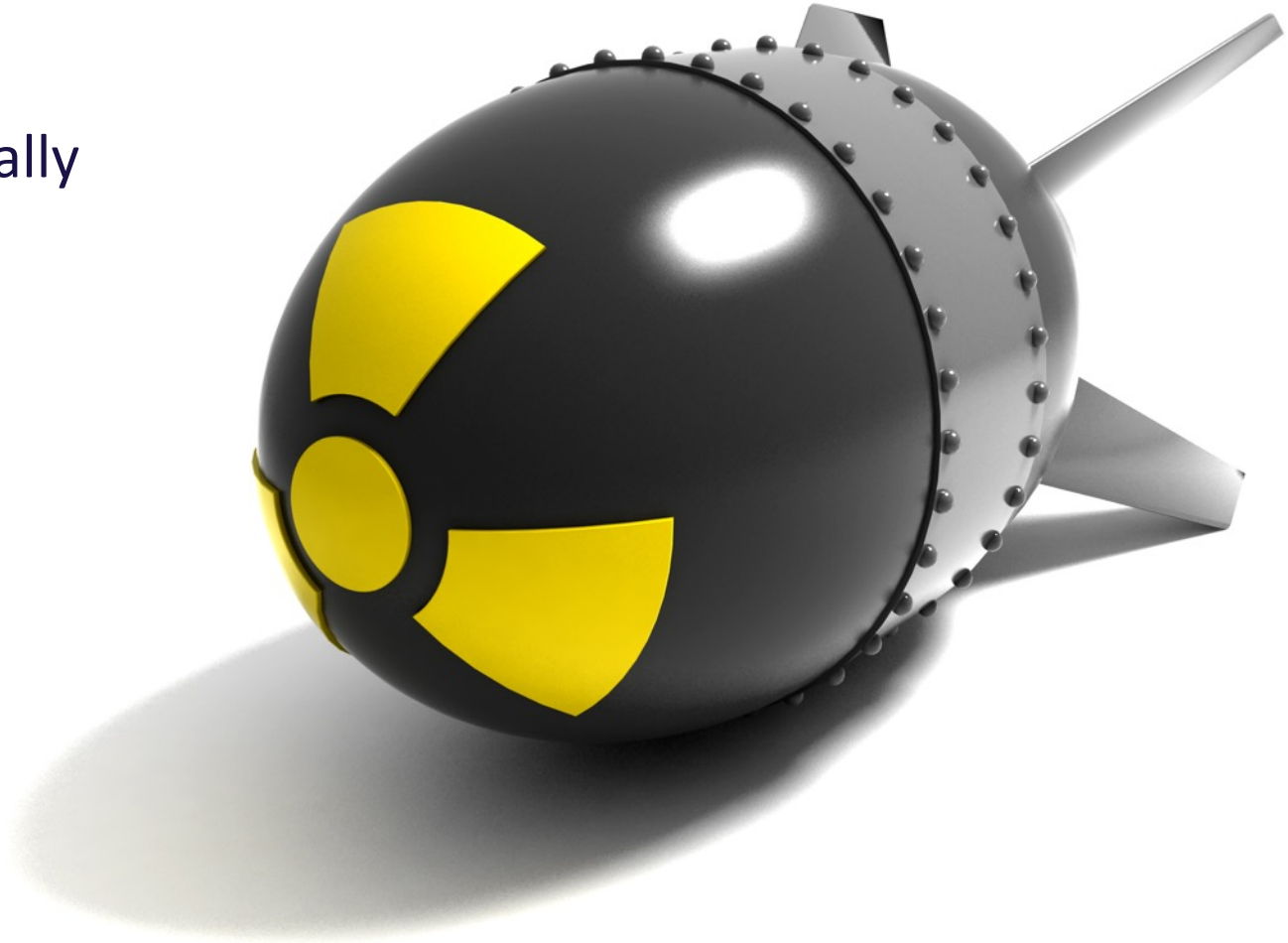


Radar architecture

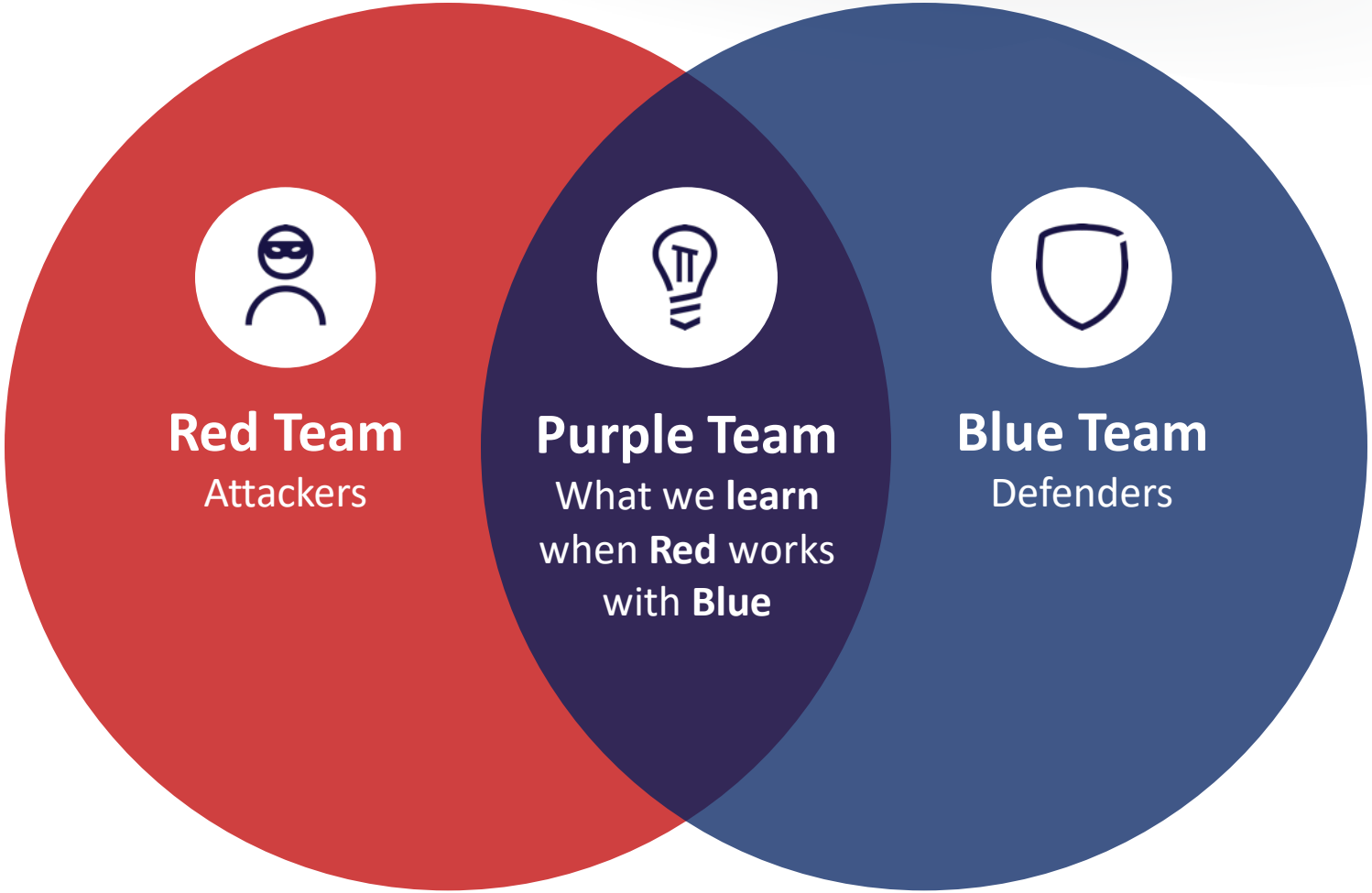


Our goal: Managing the blast radius of failure

- **News flash:** IT professionals are human beings and may occasionally make mistakes.
- **How can we limit the impact of those mistakes?**
  - Small, frequent releases
  - Modern development practices
  - Rethink the way we structure our cloud resources



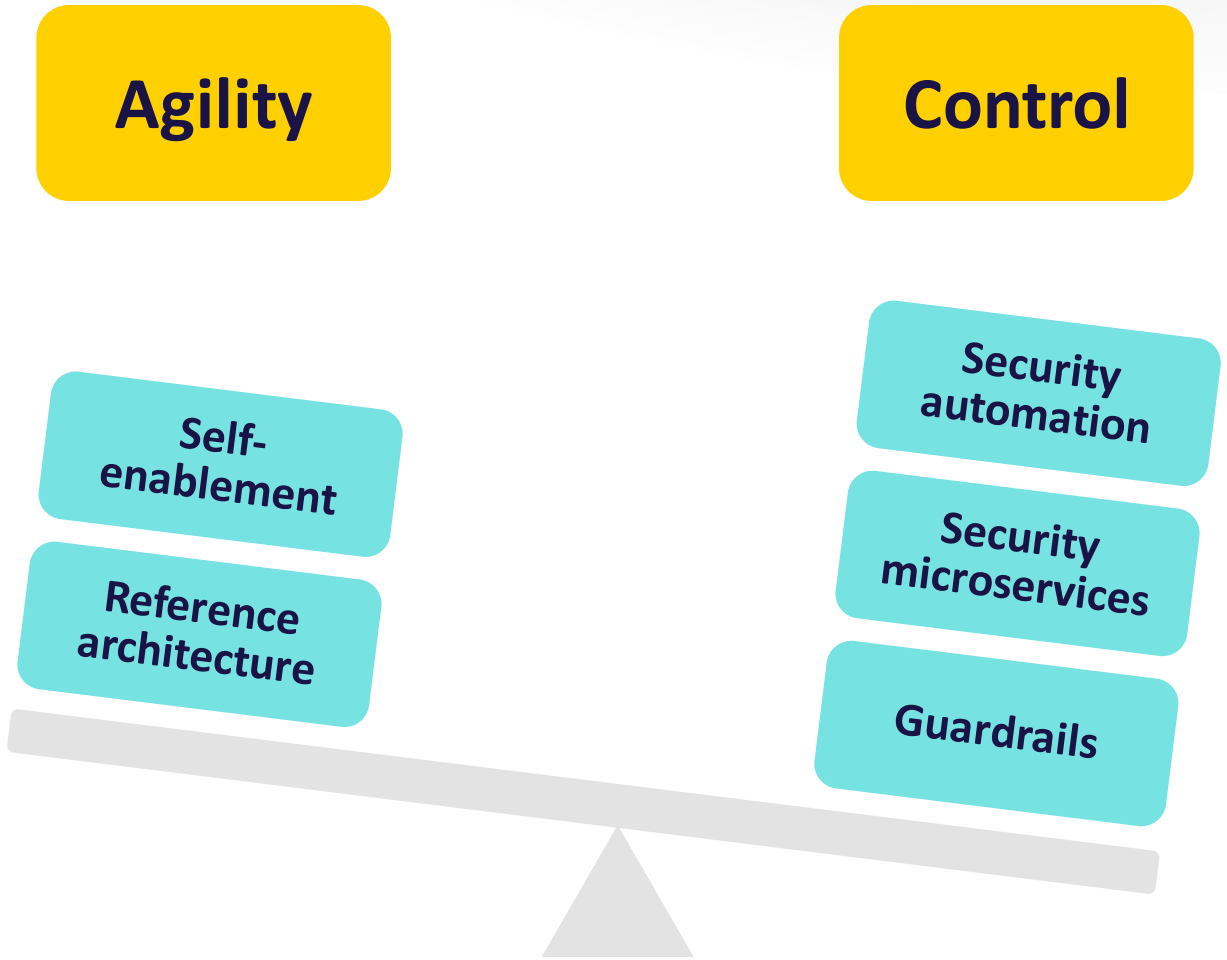
Offensive Security: Red, Blue, and Purple Teams



RSAConference2020

Conclusions

Governance as an enabler



Credit: Michael St. Onge, AWS

The future of SecOps: Behind the 8 ball…

SecOps is behind the 8 ball, by definition. The deck is stacked against us…

We need to think differently…

Embrace automation instead of fearing it.

We are entering a new world…

Security is largely built into the technology stacks which run our infrastructure.

We must change how we do things…

Embrace processes which will most likely make you uncomfortable.

Mike Rothman, Securosis 11/10/17

Hacking our culture

Security as a document

Security as code