
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

ENT220

Shipping securely: How strong security can be your strategic advantage

Clarke Rodgers

Director, AWS Enterprise Strategy
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why does it matter?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why does it matter?



Deploy products faster

FICO®

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why does it matter?



Deploy products, faster



Respond better to the unexpected



Fannie Mae®

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why does it matter?



Deploy products faster



Respond better to the unexpected



Customer trust

PHILIPS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why does it matter?



Deploy products, faster



Respond better to the unexpected



Customer trust



Scale Operations

Southwest

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why does it matter?



Deploy products faster



Respond better to the unexpected



Customer trust



Scale Operations



Speed up innovation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why does it matter?



Deploy products, faster

FICO



Respond better to the unexpected

Fannie Mae



Customer trust

PHILIPS



Scale Your Operations

Southwest



Speed up innovation

aws

aws

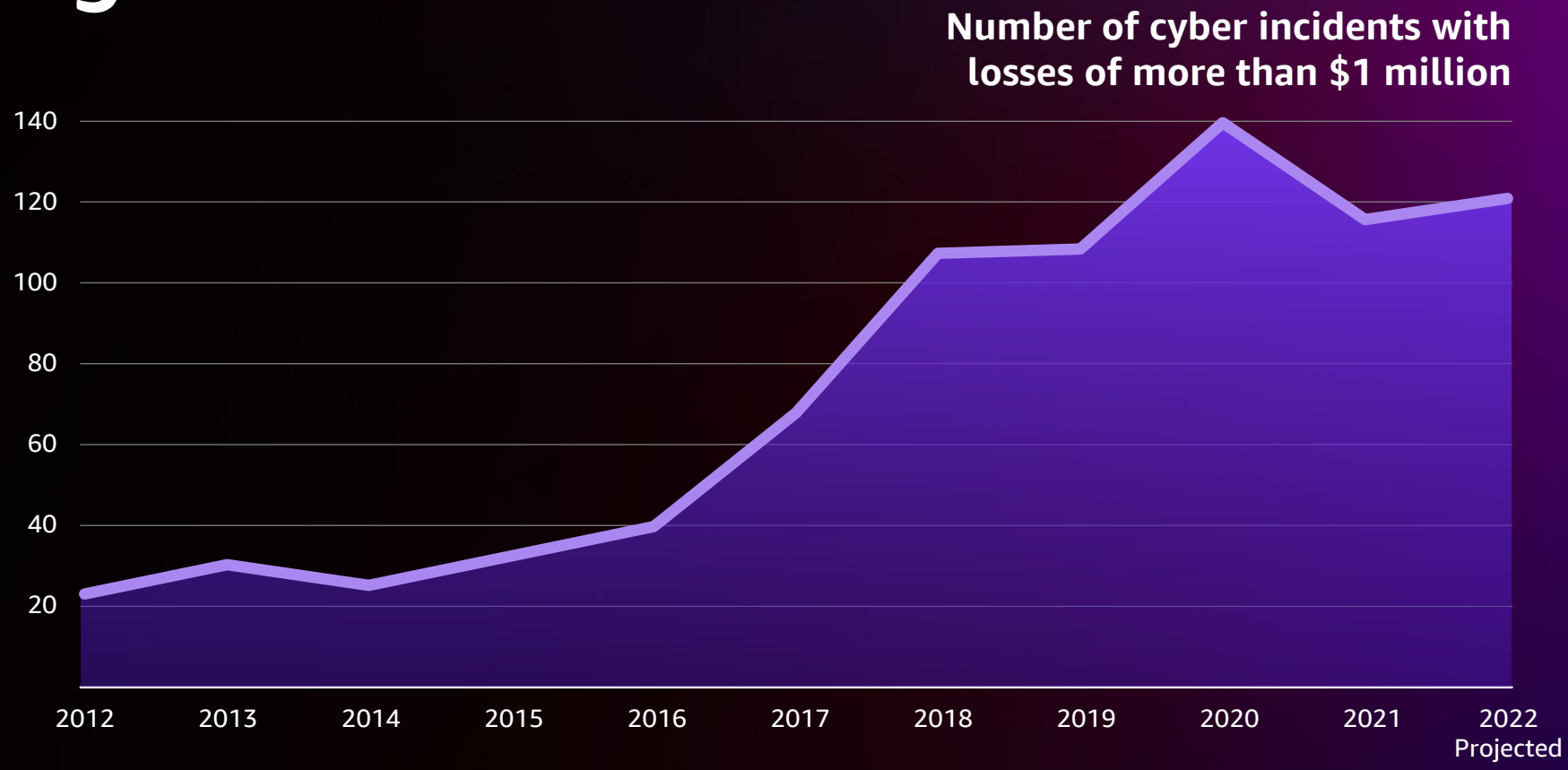
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How did we get here?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What has changed?

Sophistication and scale of security events continues to accelerate



"The stereotypical hacker working alone is no longer the main threat. Today, cyberhacking is a multibillion-dollar enterprise, complete with institutional hierarchies and R&D budgets. Attackers use advanced tools, such as artificial intelligence, machine learning, and automation."

Forbes, "Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know", 2022

Chart from Center for Strategic & International Studies tracker of "Significant Cyber Incidents" as of end of August 2022

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

"We're not playing checkers, we're playing chess. And we're playing chess at 150 miles per hour, on the internet, with everybody watching."

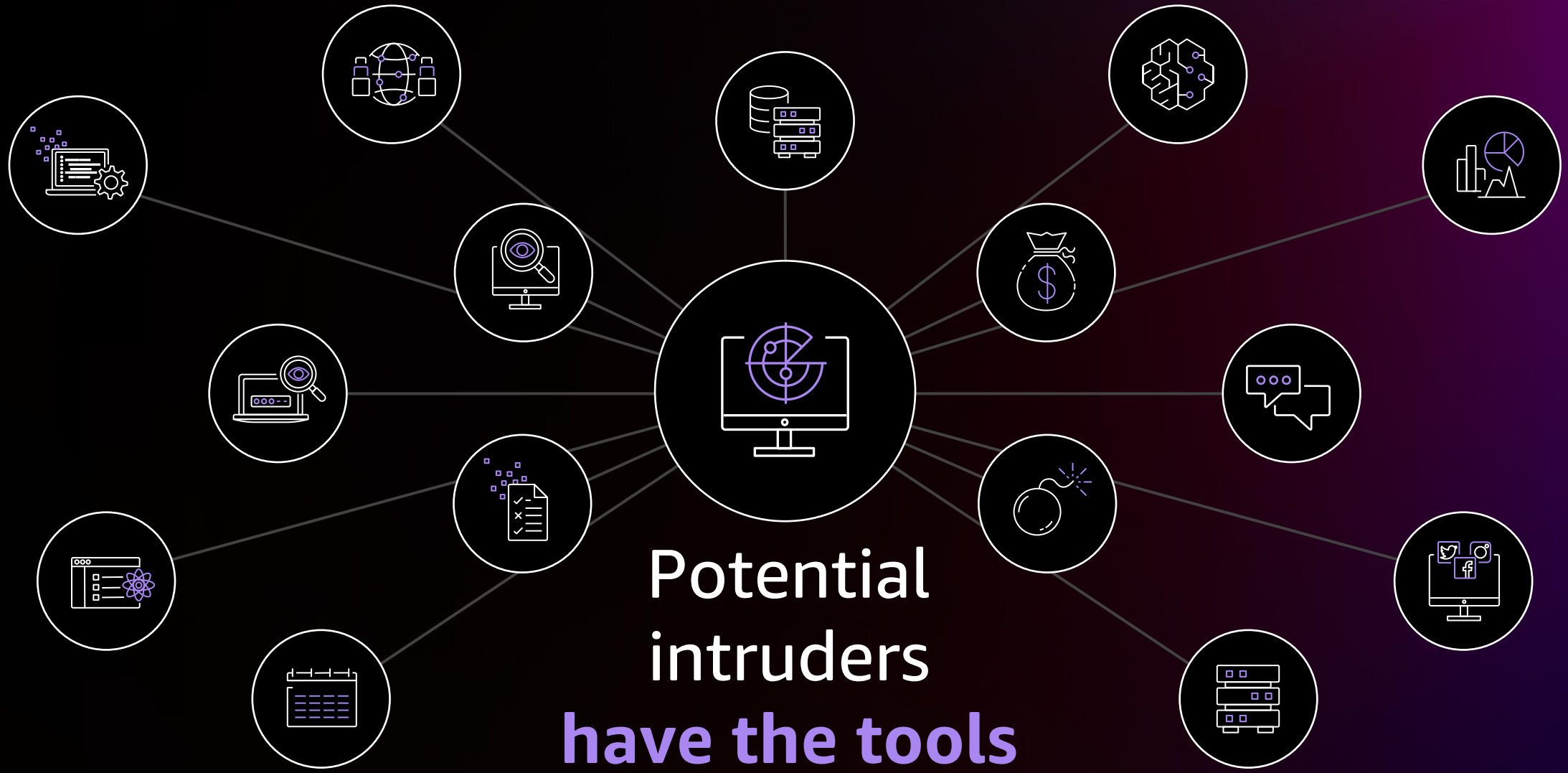


CJ Moses

AWS Chief Information Security Officer

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What has changed?



Potential intruders **have the tools**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Things have gotten messy



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

"So long as governments keep shelling out far more money to hackers to leave vulnerabilities wide open than companies do to close them shut, defense will be handicapped."



Nicole Perlroth

Author & Reporter

This Is How They Tell Me the World Ends: The Cyber-Weapons Arms Race

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What does shipping securely look like?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Evolution of shipping securely



	Aware	Bolted-on	Embedded
Lines of defense	Network-based controls	Identity-based controls with entitlement review	Zero Trust architectures
Access control	Human direct access	Mix of system and human access to data	Humans have no direct access to data
Questions	What happened?	Why did it happen?	How can we be sure that it doesn't happen again?
Culture	Security team's job	Product owner's job	Everyone's job
Responsiveness	Reactive	Monitors and reacts	Proactive
Talent development	Training available on employee time	Hired by security team	Embedded knowledge required across teams
Tooling	Point and click – console	Transitioning to engineering mindset	Automated tooling

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shipping securely



Reacts



Protects



Differentiates



Enables

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

And yet . . .

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“By 2025, a single, centralized cybersecurity function will not be agile enough to meet the needs of digital organizations. CISOs must reconceptualize their responsibility matrix to empower Boards of Directors, CEOs and other business leaders to make their own informed risk decisions.”

Gartner

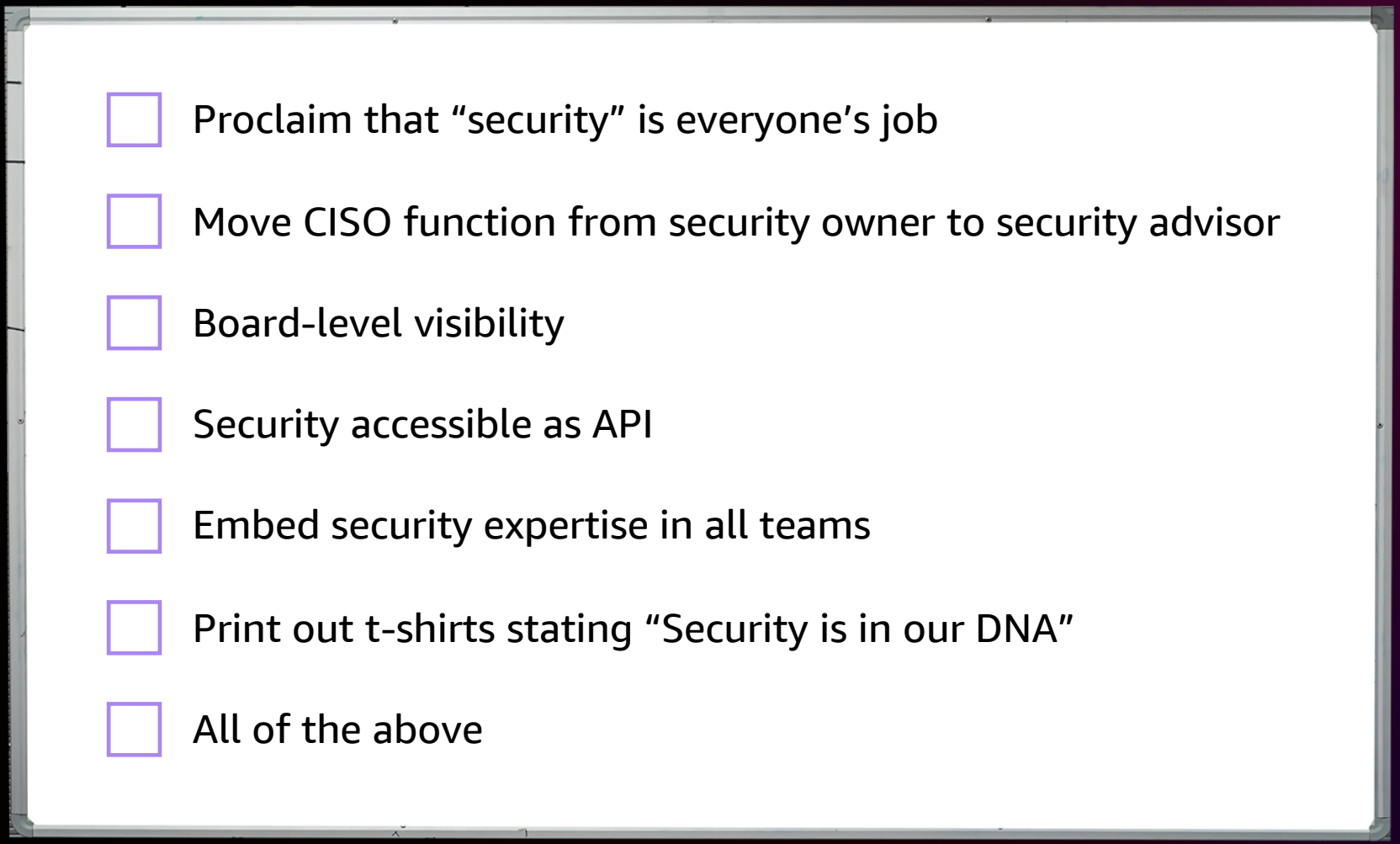
Source: https://gtnr.it/3EpVfdq

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How to realize the vision of shipping securely

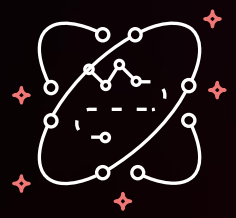
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How to realize the vision of shipping securely



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Realizing the vision of shipping securely



Culture

Beliefs, values, and behaviors that create a culture of security

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Realizing the vision of shipping securely



Culture

Beliefs, values, and behaviors that create a culture of security



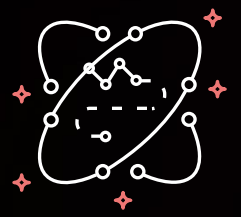
Organization

Structure and roles that accelerate business value

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Realizing the vision of shipping securely



Culture

Beliefs, values, and behaviors that create a culture of security



Organization

Structure and roles that accelerate business value



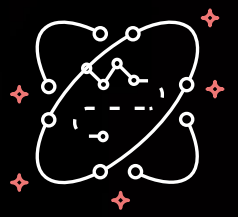
Mechanisms

Processes that enable and scale effective security outcomes

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Realizing the vision of shipping securely



Culture

Beliefs, values, and behaviors that create a culture of security



Organization

Structure and roles that accelerate business value



Mechanisms

Processes that enable and scale effective security outcomes

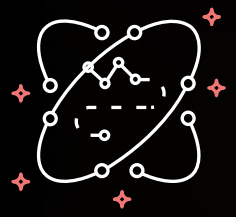


Execution

Automation and engineering excellence

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Culture

Fact-based culture that empowers people to act

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

"There is no consequence for reporting something in error; we would much rather investigate than not hear about it."

AWS Security

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“We find the people that are inclined to figure out, ‘How do I break things?’ And asking ‘How do I break things?’ leads naturally to, ‘How do I fix them so they can’t be broken again?’”

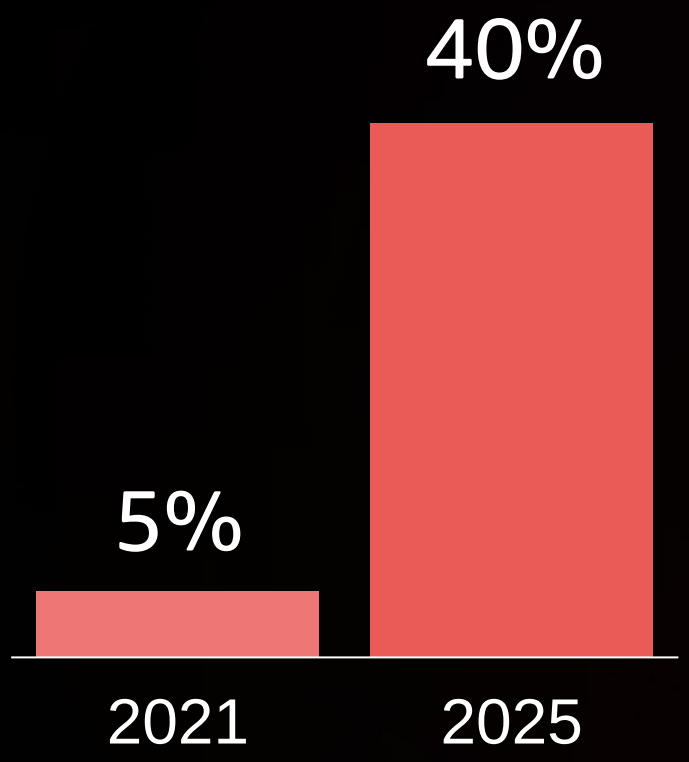


Eric Brandwine

AWS VP & Distinguished Engineer

https://youtu.be/79xR0NSruXM

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



By 2025 40% of programs will deploy socio-behavioral principles to influence security culture across the organization, up from 5% in 2021

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Source: Gartner Predicts 2022: A look into the most critical issues facing Cybersecurity leaders

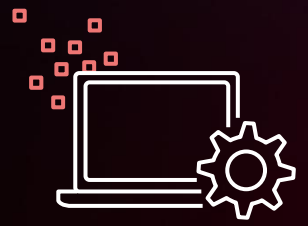


Engage

Executive sponsorship	Executive engagement
Security principles to justify decisions	Security principles to guide decisions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.





Engage

Enable

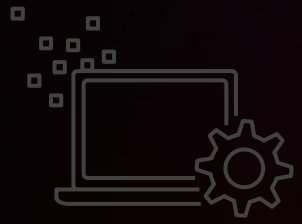
Democratize access to security tools	Democratize actions using security
Having security tools available	Make security tooling easy to use

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Engage



Enable



Educate

Selective security literacy	Security proficiency as a core skill
Lack of common definitions	Common understanding and vocabulary

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Engage



Enable



Educate



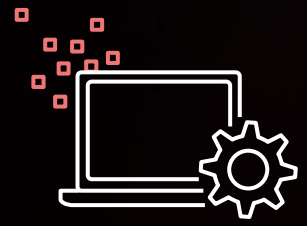
Eliminate

Not my job	Everyone’s job
Source of conflict	Source of enablement

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Engage



Enable



Educate



Eliminate

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Weasel words

Better
Clearly
Around
Faster
Lower
Many
Higher
Greater
Nearly
Often
Significant
Probably
Worse
Usually
Very

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“We **shipped** secure products this quarter”	“We continue to maintain security throughout the **life cycle of our products**”
“Security **slows** us down”	“Security is a **business enabler** and is connected directly to our objectives”
“We **fixed** the security production issue”	“We **reduced the risk** of disruption to this critical business application.”

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



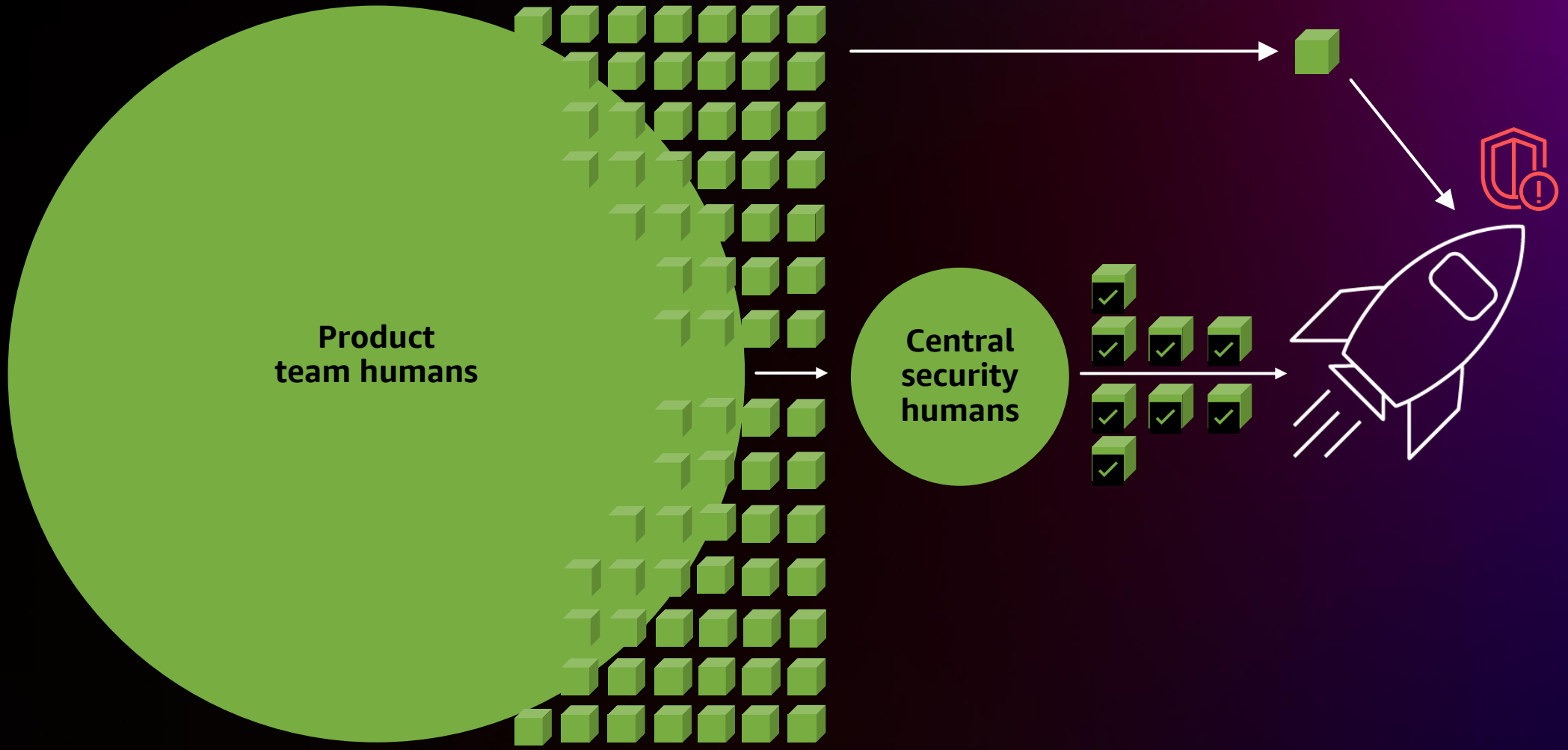
Organization

Organize for agility, not control

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What got you here will not keep you here

Organization

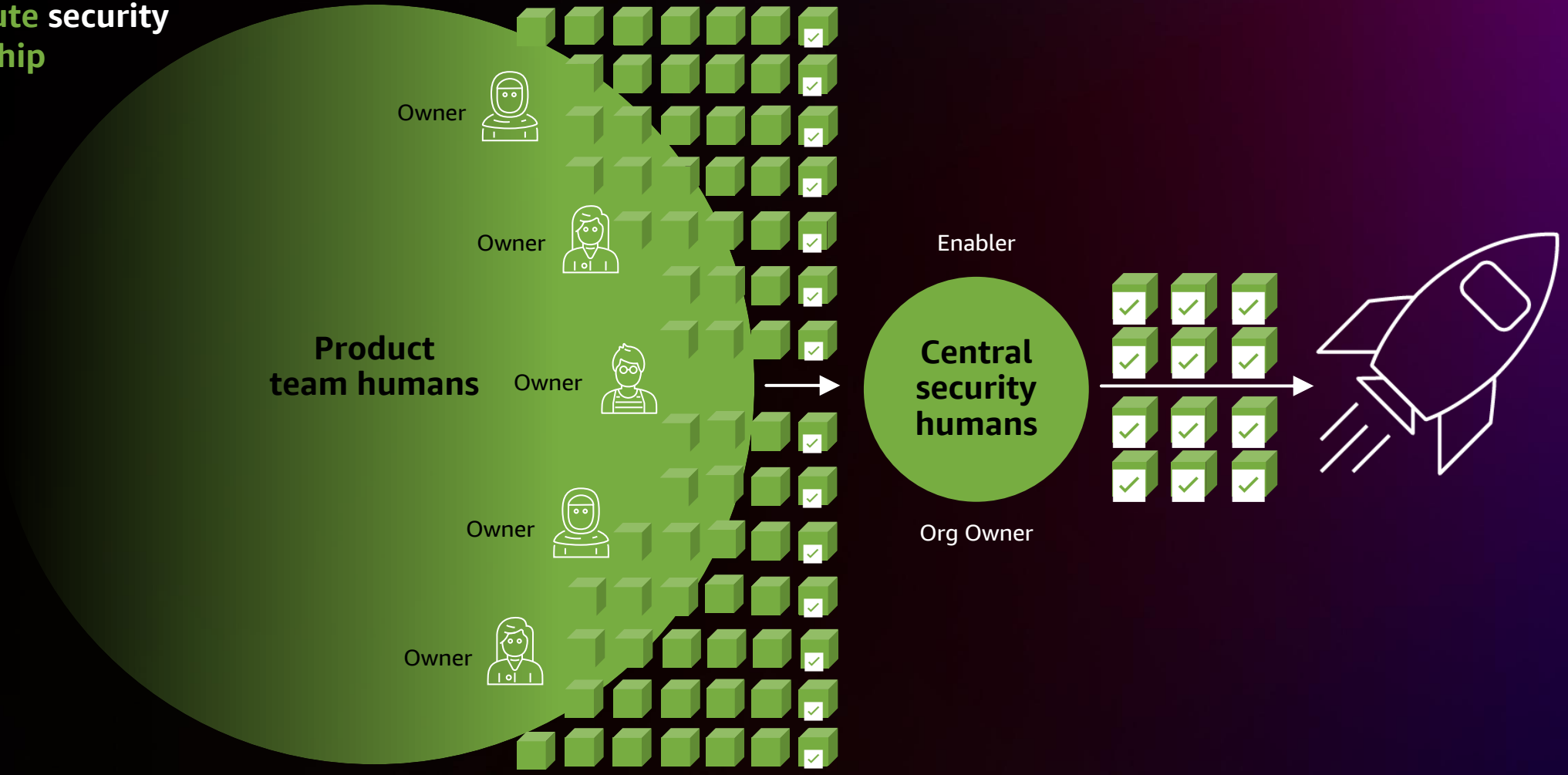


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Moving fast, delivering securely

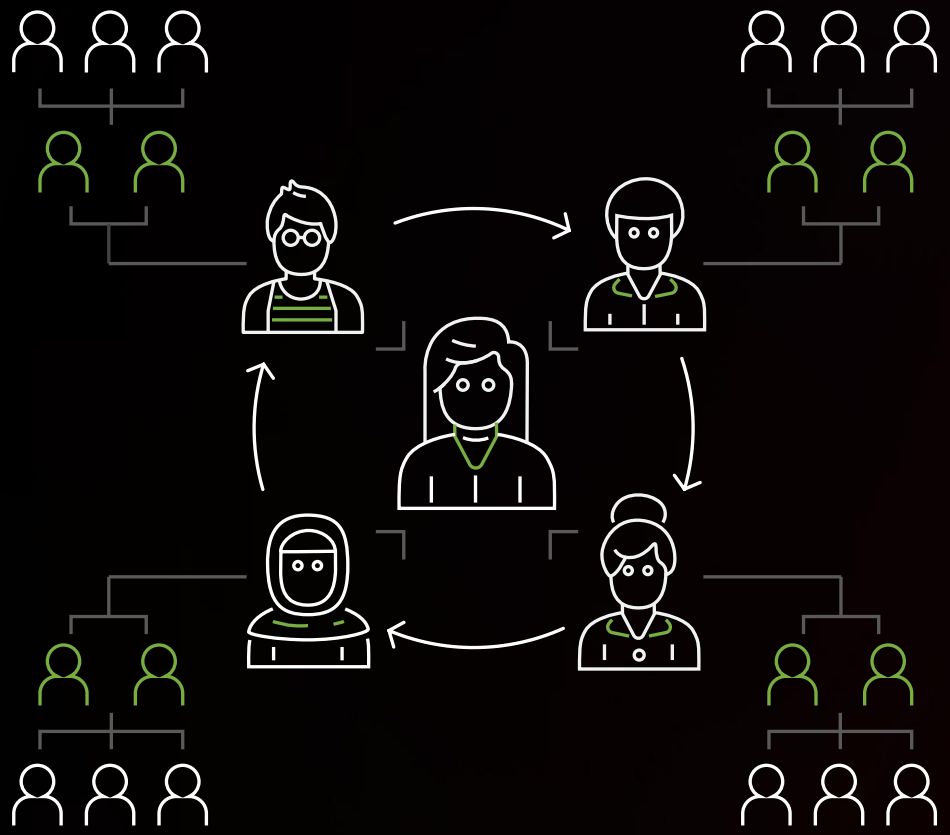
Organization

Distribute security ownership



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security-driven organization



- Align around outcomes, not activity
- Embrace autonomous cross-functional teams
- Teams are expected and empowered to act
- Operate with a ”you build it, you run it, and you own security for it” mentality

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Distribution of security ownership

Organization



Product team

Owner

"We own the security of what we build and run"



Security team

Org owner | Enabler

"We own the organization's overall security – and enable service teams to deliver and operate securely"*

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

* AWS Security would partner with other organizations to achieve these goals (e.g., platform, builder tools)

Security Guardians

Organization



Product team

Owner

Security Guardian

A member of a product team responsible for understanding and advising their own team on the complete security review process

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Guardians program

Organization

A PROGRAM OWNED BY AWS SECURITY TO DEVELOP AND APPLY APPLICATION SECURITY EXPERTISE WITHIN SERVICE TEAMS



Identify Guardians and set organizational goal

Ramp them up with skills necessary to get them started

Build a community with continual **knowledge sharing**

Gather feedback and **measure** the program's **effectiveness**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Mechanisms

Mechanisms work, not just good intentions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Good intentions never work, you need good mechanisms to make anything happen.”

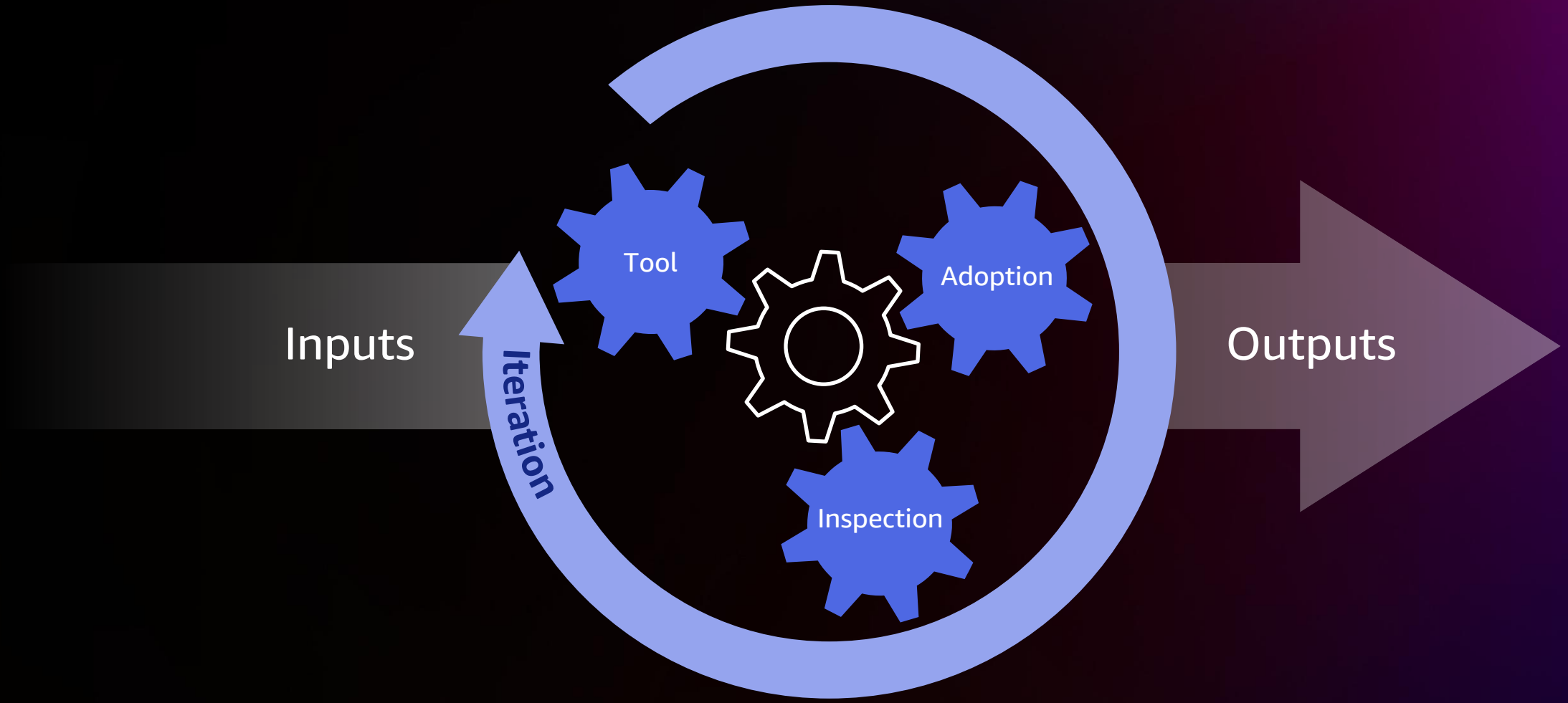


Jeff Bezos

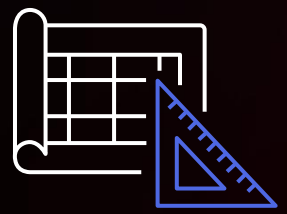
Founder and Executive Chair, Amazon, Inc.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A mechanism is a complete process



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Measurement

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

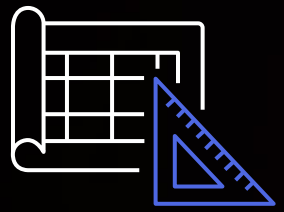


Measurement



Governance

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Measurement



Governance



Tooling

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Measure the right thing, not everything



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Measurement

"When a measure becomes a target, it ceases to be a good measure."

Goodhart's law





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Beware of watermelon goals



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Beware of watermelon goals

Retention rate



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Beware of watermelon goals

Retention rate

Engagement rate



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Rethinking measurement

Number of tickets tracked	Staleness of tickets
Time to resolution	Human engagement
Proximate cause	Root cause
Risk identification	Risk analysis
RTO/RPO	Re-hydration time
Cost per incident	Continuous program costs

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Measurement



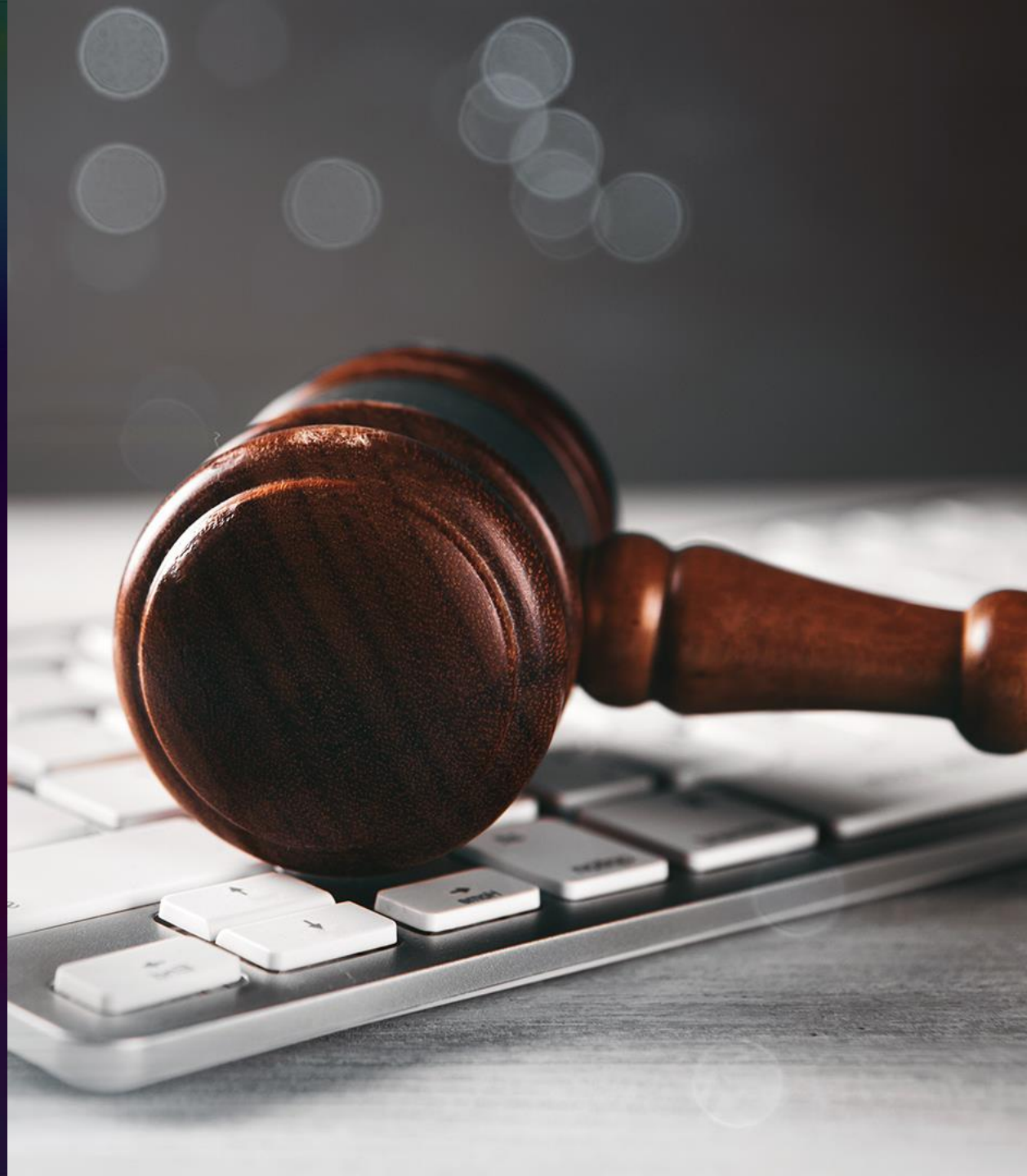
Governance



Tooling

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Govern to enable, not restrict



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How?

Establish tenets before policies and procedures

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Examples of tenets



We will make the secure path the path of least resistance



We enable our customers to do the right thing easily and by default



Mistakes will happen. Don't let the same one happen twice.



Speed will not result in poor security and compliance



Being secure and compliant will not result in slow progress and creation of siloes

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How?

Establish tenets before policies and procedures

Centralize objectives, decentralize implementation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

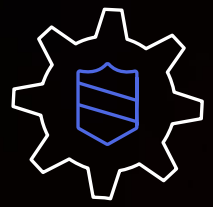
Centralize security, governance, and auditing objectives



Centrally design security, governance, and auditing objectives



Policies are consistently enforced



Implement pipeline-as-a-service so security requirements are built in



Automated audit evidence as part of functional requirements

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How?

Establish tenets before policies and procedures

Centralize objectives, decentralize decisions

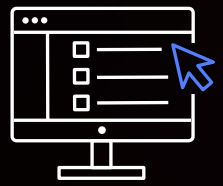
Operate with transparency

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Dashboards, metrics, reporting, and review



Hold regular security business reviews



Create dashboards reflecting the security/compliance of workloads



Build a sense of competition and ownership between product and business owners



Recognize program compliance

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How?

Establish tenets before policies and procedures

Centralize objectives, decentralize decisions

Operate with transparency

Automate your bureaucracy

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automate your bureaucracy



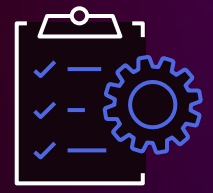
Ticketing System Integration



Compliance by Design



Inspect/self test regularly



Feedback Loops/ Intake Processes

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How?

Establish tenets before policies and procedures

Centralize objectives, decentralize decisions

Operate with transparency

Automate your bureaucracy

Encrypt everything

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Encrypt everything

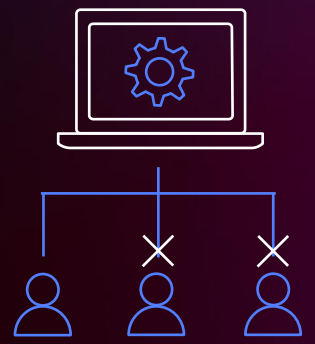


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

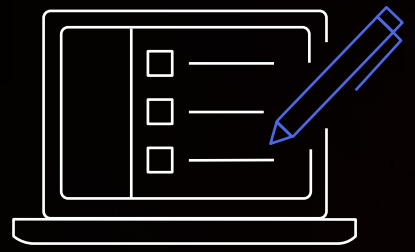
Encrypt everything



Protect your keys;
rotate them often



Restrict permissions on key
management activities



Least privilege



MFA where appropriate

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Measurement



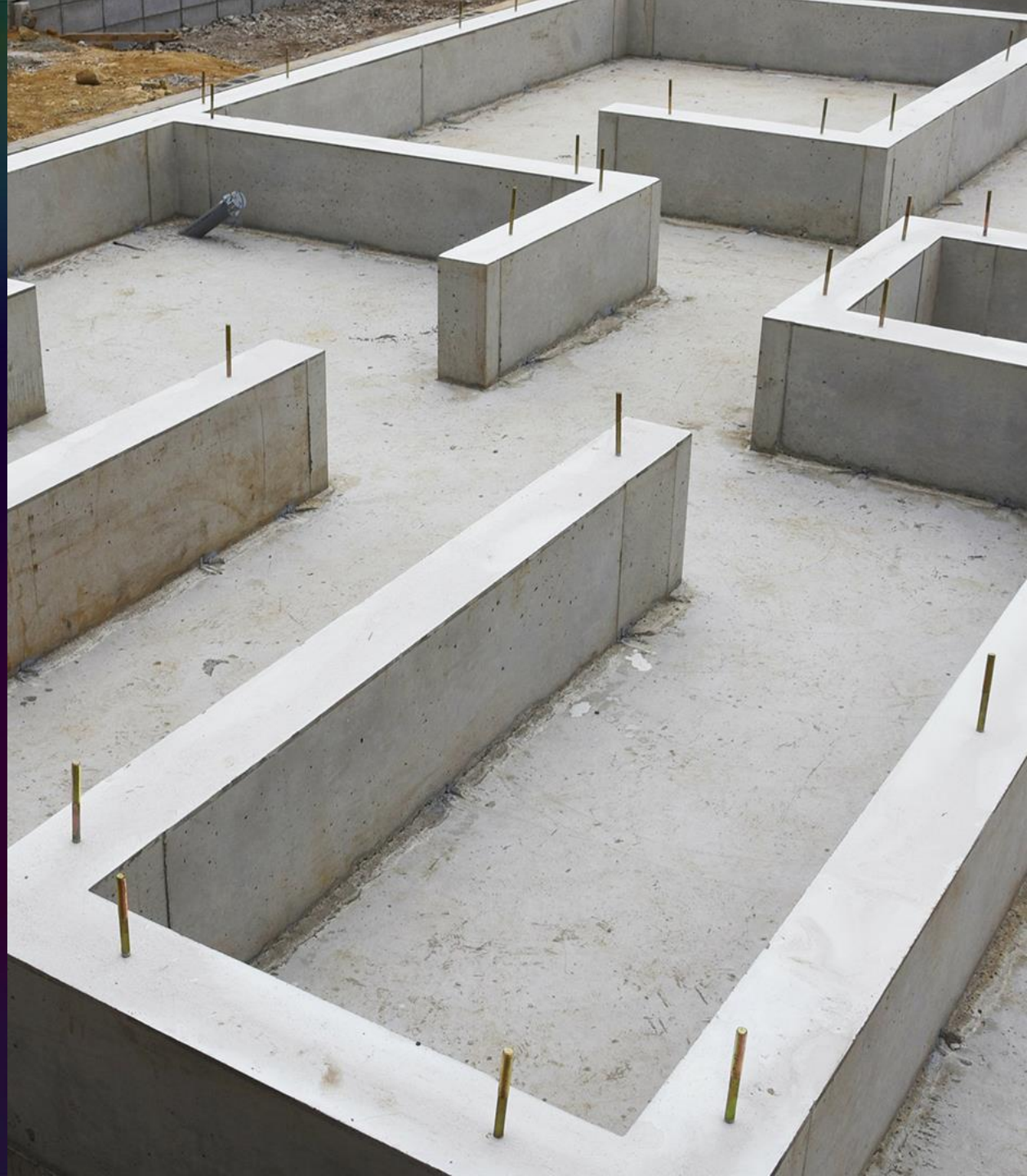
Governance



Tooling

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Build it in, don’t bolt it on

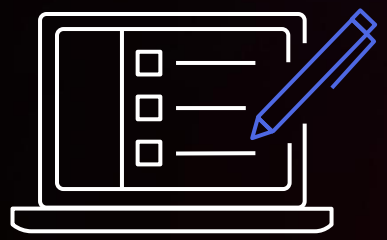


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon examples



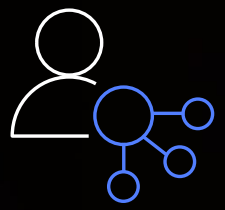
Correction of Error (COE)



Operational Readiness Reviews (ORR)



Working Backwards



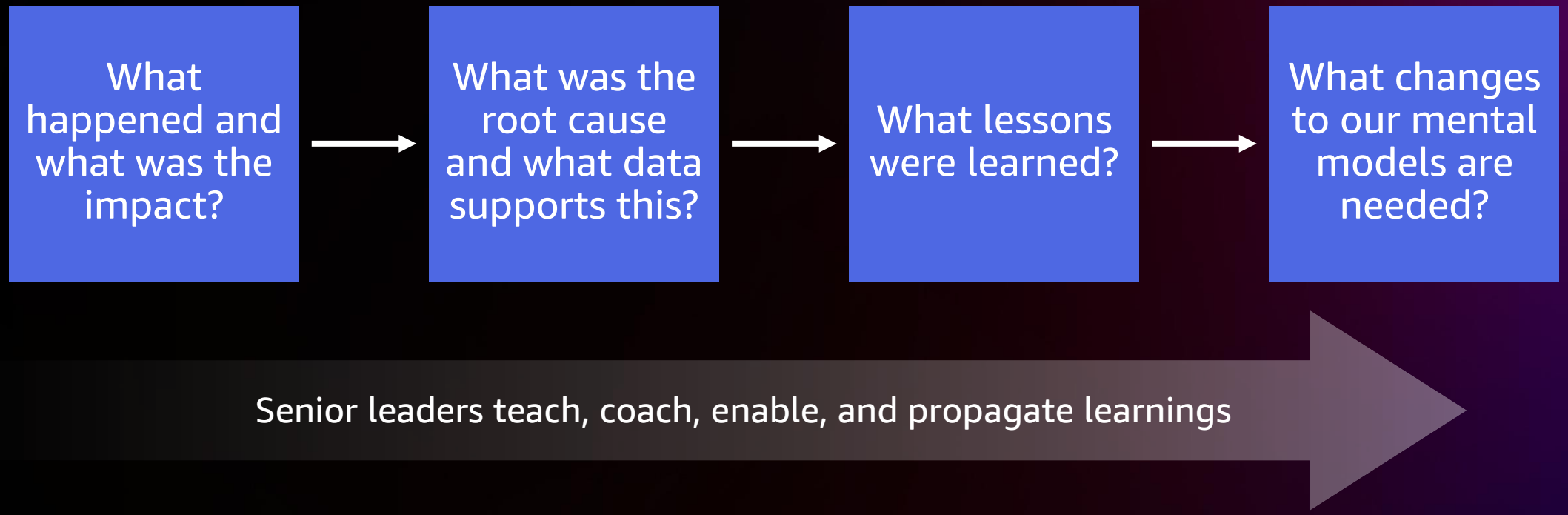
Consistent with Amazon's Ownership Leadership Principle:

"Leaders are owners. They think long term and don't sacrifice long-term value for short-term results. They act on behalf of the entire company, beyond just their own team. They never say 'that's not my job.'"

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example: amazon Correction of Error



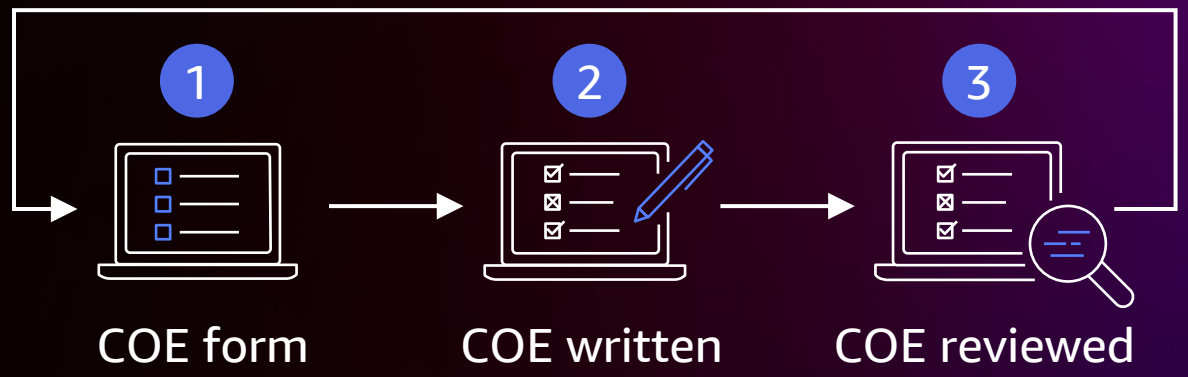
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Making it virtuous

Easy to understand the tools

How to ensure adoption?

Adoption comes with review



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



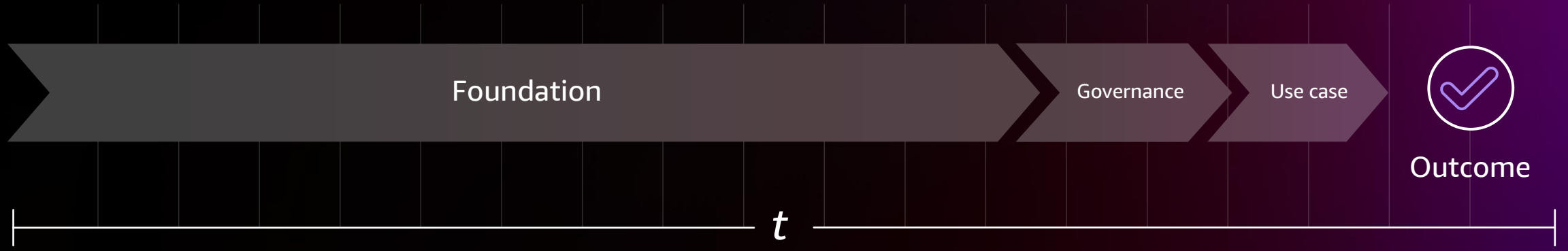
Execution

Think big but execute small

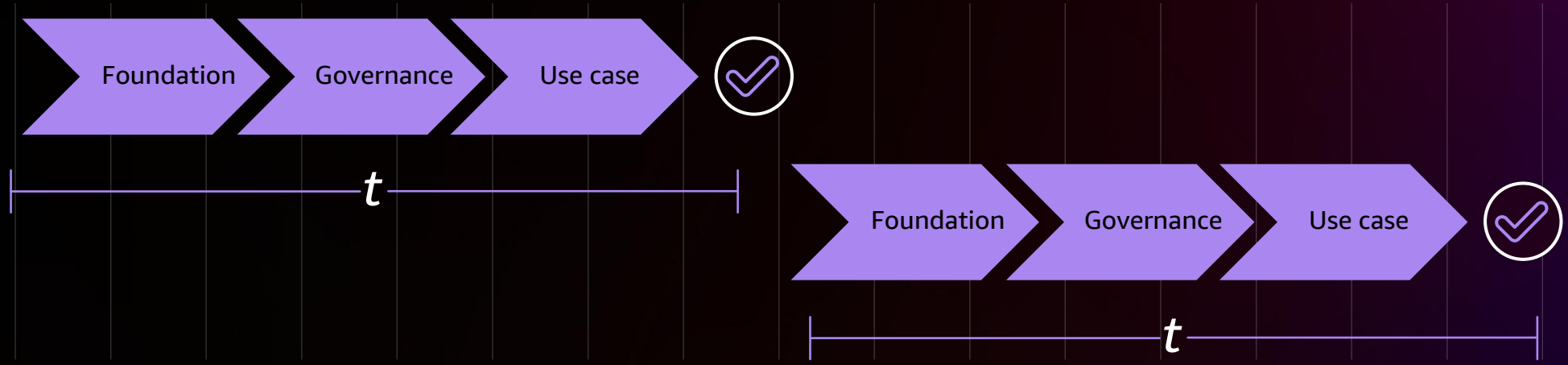
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Time to value

Traditional approach



Iterative approach

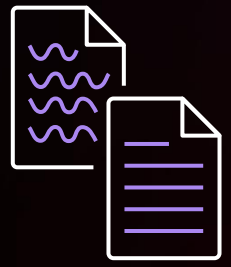


aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Instead

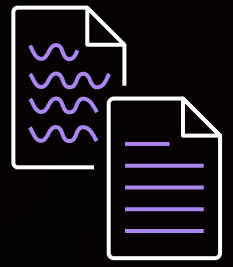


Log everything

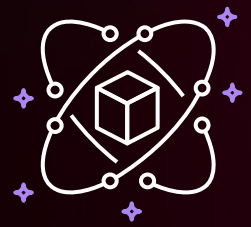
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Instead



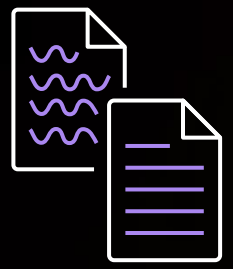
Log everything



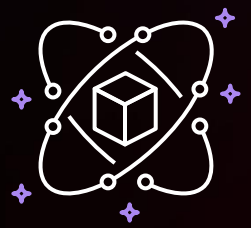
Integrate security into all deployment activities

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Instead



Log everything



Integrate security into all deployment activities



Focus on the security outcome vs. the security tool

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS supports customers' security journey natively



Identity and access management

- AWS Identity and Access Management (IAM)
- AWS IAM Identity Center (successor to AWS Single Sign-On)
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager (AWS RAM)



Detection

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender



Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF – Web application firewall
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS PrivateLink
- AWS Systems Manager



Data protection

- Amazon Macie
- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- AWS Certificate Manager (ACM)
- AWS Secrets Manager
- AWS Client VPN
- AWS Site-to-Site VPN
- Server-Side Encryption



Incident response

- Amazon Detective
- AWS Elastic Disaster Recovery
- AWS Config Rules
- AWS Lambda



Compliance and governance

- AWS Artifact
- AWS Audit Manager
- AWS Control Tower
- AWS Well-Architected Tool
- Amazon Route 53 Application Recovery Controller

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But that's not all...



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

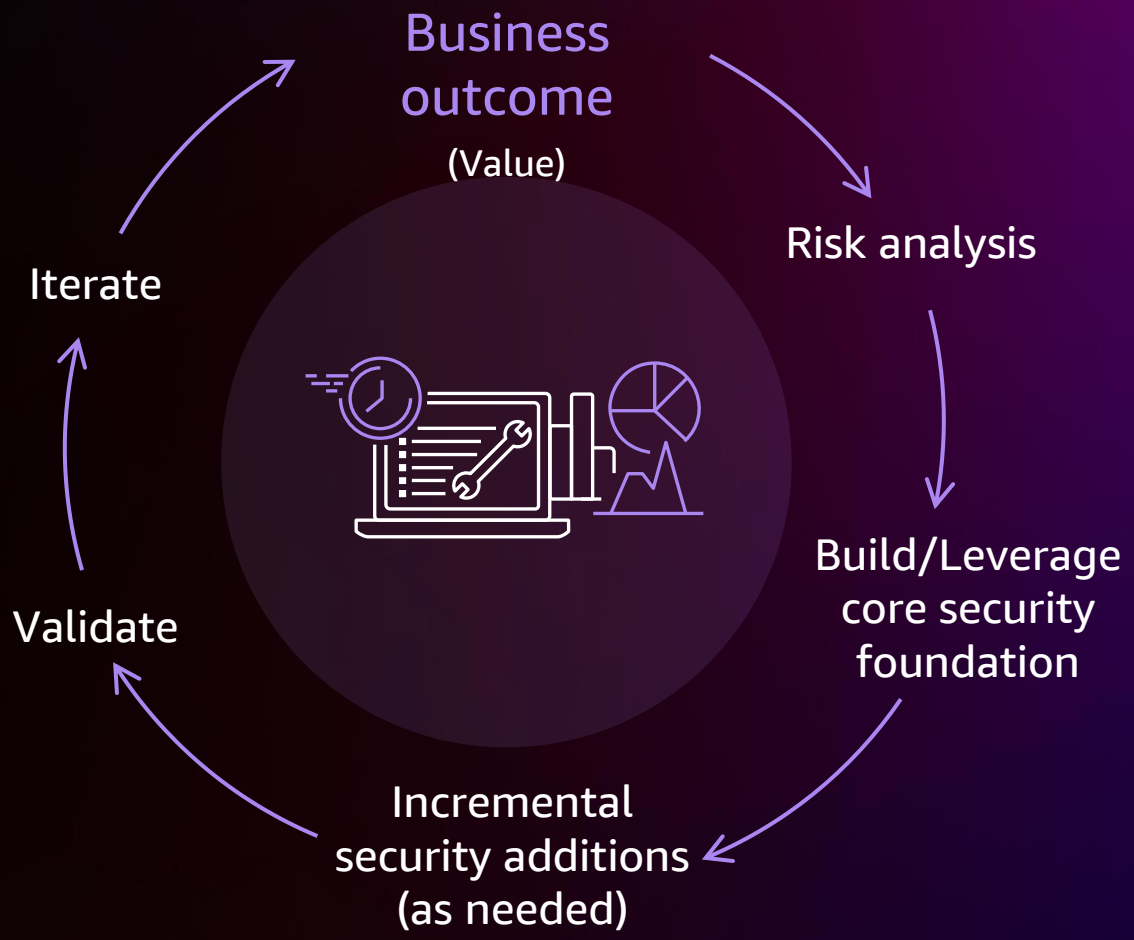
Work backwards from business objectives



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Work backwards from business objectives

1. Start by identifying the business outcome you are driving toward
2. Identify potential risks
3. Build tooling and culture
4. Automate deployments
5. Validate
6. Iterate and adjust



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guiding principles

Culture	Fact-based culture that empowers people to act
Organization	Organize for agility, not control
Mechanisms	Mechanisms work, not just good intentions Measurement | Measure the right thing, not everything Governance | Govern to enable, not restrict Tooling | Build it in, don’t bolt it on
Execution	Log everything Integrate security into all deployment activities Focus on the security outcome vs. the security tool

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We are here to help

Need peer-level executive guidance?

aws Enterprise Strategy

- ✓ Mental models and strategies based on the firsthand experience of former CXOs
- ✓ Get peer-level sounding board and sparring partner

Inspire and accelerate your digital transformation

Want to build a security practice?

aws Professional Services

- ✓ Develop the confidence and technical capability to migrate your most sensitive workloads to the AWS Cloud

Jumpstart your innovation flywheel

Have a strategy and need help executing it?

aws AWS Partner Network (APN)

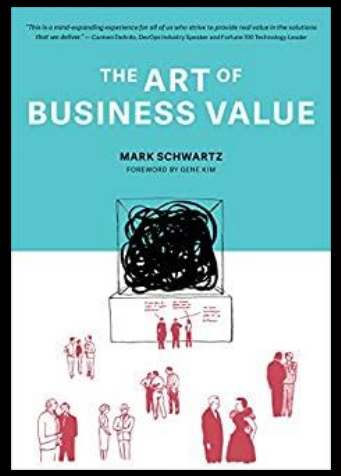
- ✓ Security and compliance consulting partners
- ✓ Security and compliance technology partners

Come with an idea, leave with a solution

aws

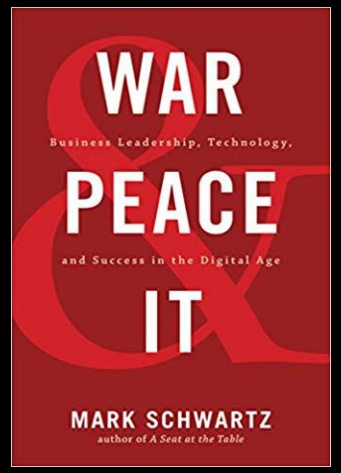
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Like to read?



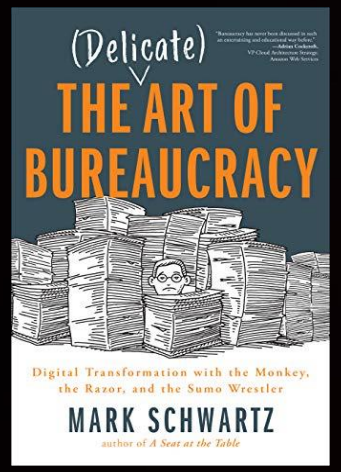
The Art of Business Value

https://amzn.to/3URoHP6



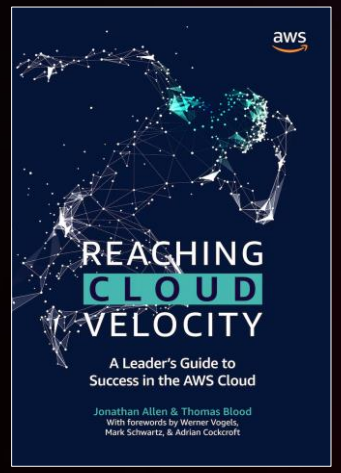
War and Peace and IT

https://amzn.to/2WeAw83



The Art of Bureaucracy

https://amzn.to/3URoADa



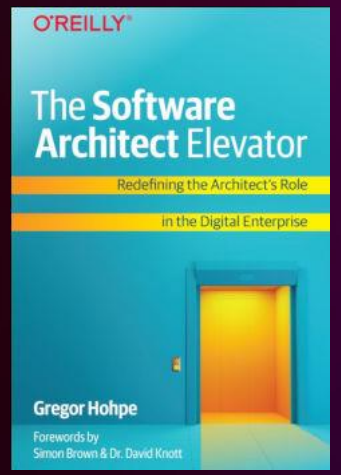
Reaching Cloud Velocity

https://amzn.to/3UxYbdF



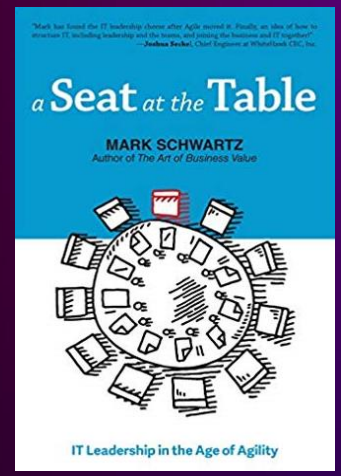
Cloud Strategy

https://amzn.to/3hFUG6E



The Software Architect Elevator

https://amzn.to/3G8Q2rI



A Seat at the Table

https://amzn.to/3TwjqLu

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

aws Executive Insights

Self-service digital content written for executives

https://go.aws/3UutxSl

conversations with LEADERS aws Executive Insights

Podcast: Featuring discussions with executive leaders

https://spoti.fi/3WUL9sn

aws Executive Connection

LinkedIn: Community for business and technology leaders

https://bit.ly/3g6x9Lo

aws Cloud Enterprise Strategy Blog

Blog channel for technical and non-technical executives in an enterprise

https://go.aws/3WTNJPo

aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.