ATO on AWS

Eric Baran
DevOps Segment Leader – Regulated Industries

ATO Sales Kick Off 2019

Why did we decide to build this program?

Our customers asked us to.

ato authority to operate on aws

aws

What Regulatory Standards are we building for?

ACCELERATING TIME TO COMPLIANCE IN THE AWS CLOUD

International Traffic and Arms Regulation

FedRAMP Moderate and High

DOD Security Req's Guide IL 2, 4 and 5

Criminal Justice Information Service Security Policy

Health Insurance Portability & Accountability Act

IRS Publication 1075

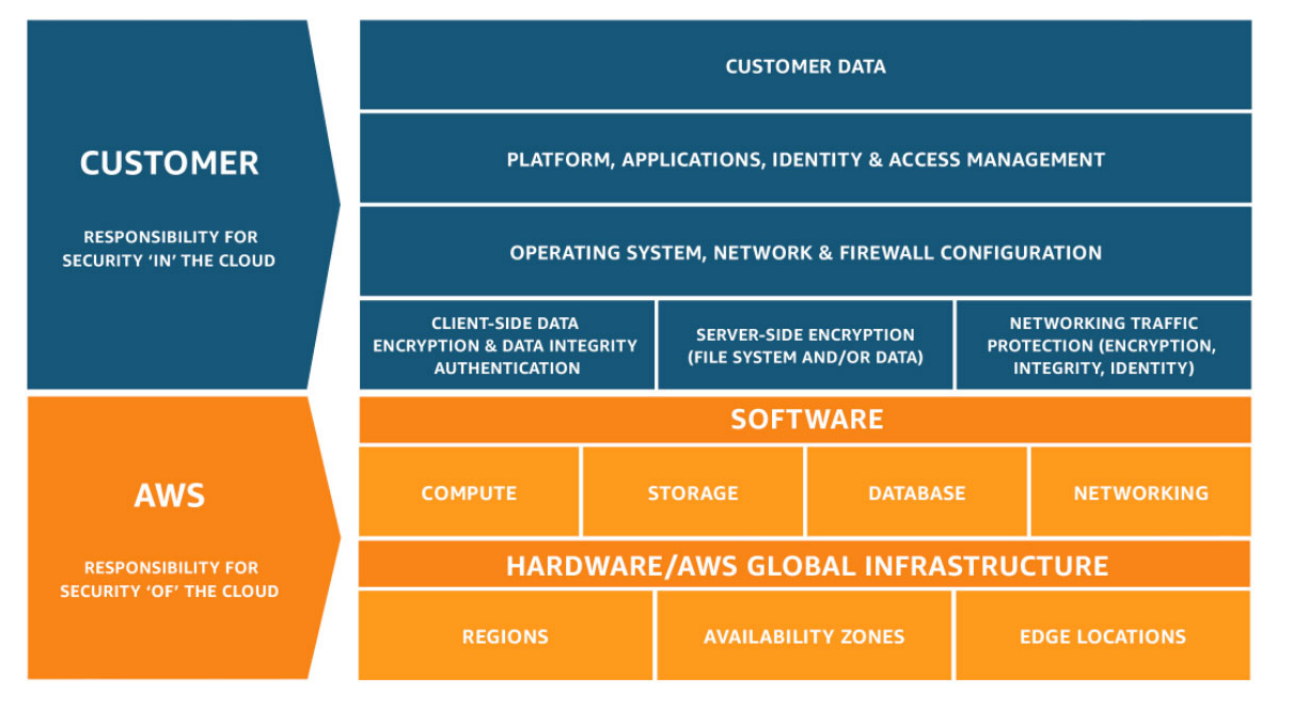
Federal Information Processing Standard Pub

SP 800-53 (rev 4)
SP 800-171

ato authority to operate on aws

aws

AWS Shared Responsibility Model



ato authority to operate on aws

aws

Problem Statement – Why can't we be Agile?

Security and risk management leaders continue to labor over **"How"** do they secure current, legacy and cloud resources consistently within their limited constraints.

While cloud services has provided streamlined ways to achieve innovation through the principles of DevSecOps and Developer Self-Service, regulated customers are still under mandate to follow strict security, governance, and accreditation standards, which are delivered during the production deployment phase.

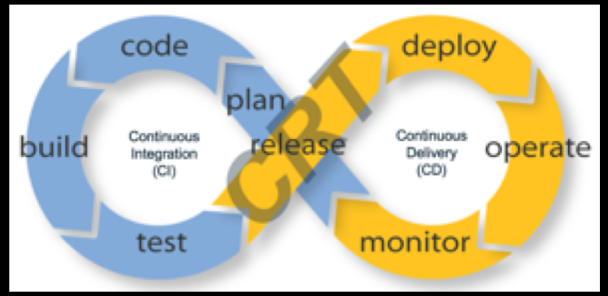
ato authority to operate on aws

aws

Solution Overview: SAO

Develop an **AWS Security Automation and Orchestration (SAO)** repository for constraining, tracking, publishing continuous security configurations, integration, deployments and treatments which are certified against common security frameworks (e.g. FedRAMP, DoD CC SRG, IRS 1075,CIS, PCI, etc.)

SAO will facilitate the orientation and association of **DevOps** and **Security** practices, changes and coordination of **Continuous Integration (CI)**, **Continuous Delivery (CD)** and **Continuous Risk Treatment (CRT)*** of an AWS customer account and/or multiple accounts.



* CRT is a process and technology approached which is designed to detect, maintain and in *MOST* case correct security, compliance and threats associated with an organization's solution and service deployment within their AWS account. CRT processes monitor security controls in real-time to ensure the risk and/or threat treatment (Control Intent) is working as designed or at least within an intended margin of acceptance base on guard rails, swim lanes and/or rules built into the control to allow for business operations.

Thank You!

Selling ATO on AWS – The Pitch

Eric Baran
DevOps Segment Leader – Regulated Industries

ATO Sales Kick Off 2019

ato authority to operate on aws

aws

Agenda – Selling ATO on AWS – Days 1 and 2

1. Review: What is the Pitch? Let's review.

2. Better Together: Why does the AWS seller care about this program. What is the critical problem we address?

3. Better Together: Why should you as partners care about innovating under the ATO on AWS program?

4. What is the core mission of our team in 2019?

5. What are our goals, how will we measure success?

ATO on AWS – The 101 Pitch

ato authority to operate on aws

aws

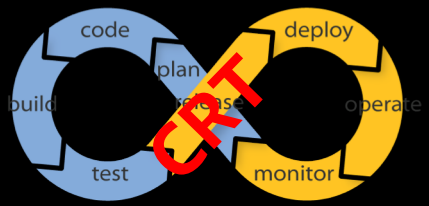
Traditional verses Cloud (Modernized) – Governance

Traditional – Governance

- Information and technology (IT) governance is a subset discipline of corporate governance, focused on information and technology (IT) and its performance and risk management.
- The interest in IT governance is due to the on-going need within organizations to focus value creation efforts on an organization's strategic objectives and to better manage the performance of those responsible for creating this value in the best interest of all stakeholders.

Cloud – Governance

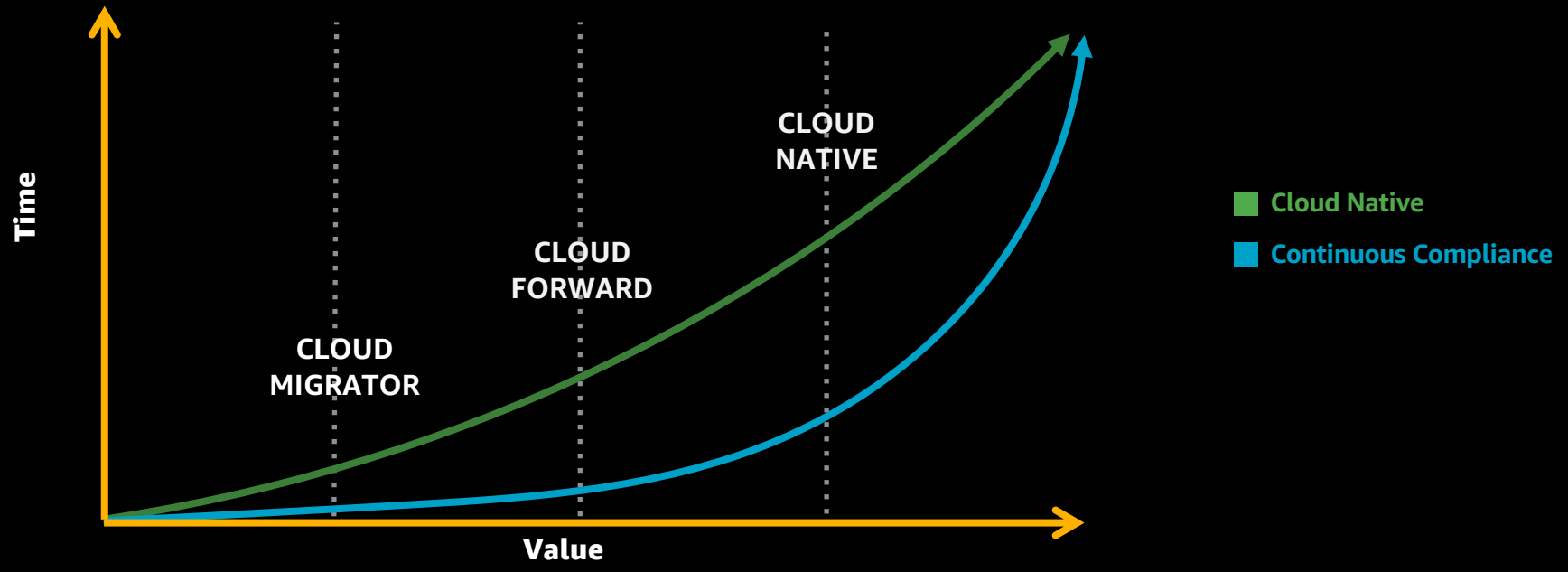
- Technology drives your governance alignment
- Governance is a “Shared Responsibility”
- Automation is the ***Key*** to successful governance
- Pre-Cloud decision making process are paramount (e.g. service selection, policies, frameworks architecture, data protections, etc.).
- Focus is on Continuous Risk Treatments (CRT)



ato authority to operate on aws

aws

Stages of Security Automation and Orchestration

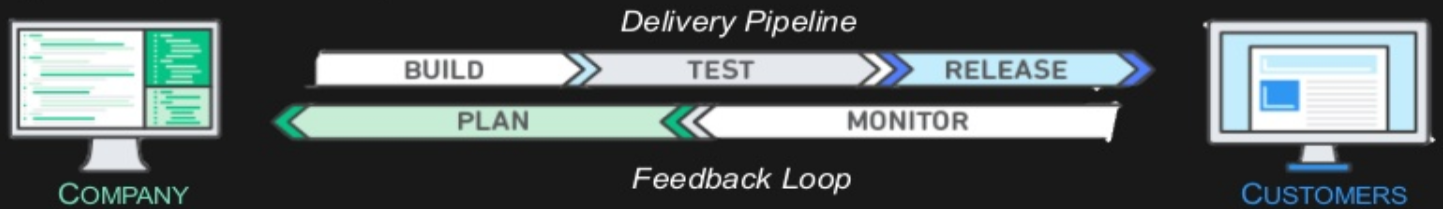


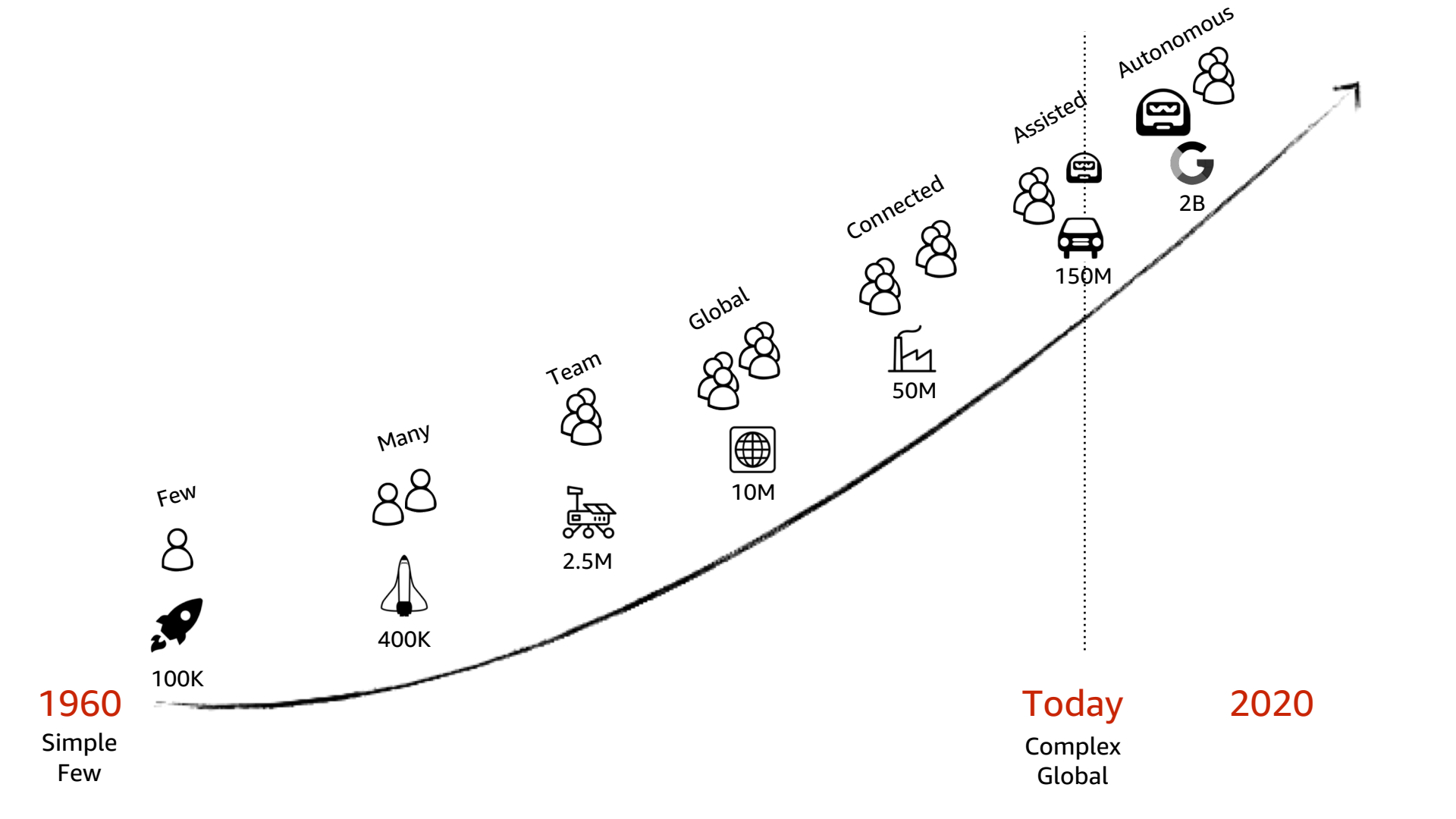
ato authority to operate on aws

aws

WHAT IS DEVSECOPS?

- Union of software development, security, compliance and operations
- Migration of Agile continuous development into continuous integration, continuous delivery, and continuous compliance.
- DevSecOps Model
  - No Silos – Puts emphasis on communication, collaboration and cohesion between disciplines
  - Best practices for change, configuration, and deployment automation
  - Deliver apps/services at a faster pace
  - High speed product updates
  - Everything is code




Few
100K
Many
400K
Team
2.5M
Global
10M
Connected
50M
Assisted
150M
Autonomous
2B
1960
Simple
Few
Today
Complex
Global
2020

PERIODIC TABLE OF DEVOPS TOOLS (V2) (V1)

EMBED DOWNLOAD ADD

Os	Open Source
Fr	Free
Fm	Freemium
Pd	Paid
En	Enterprise

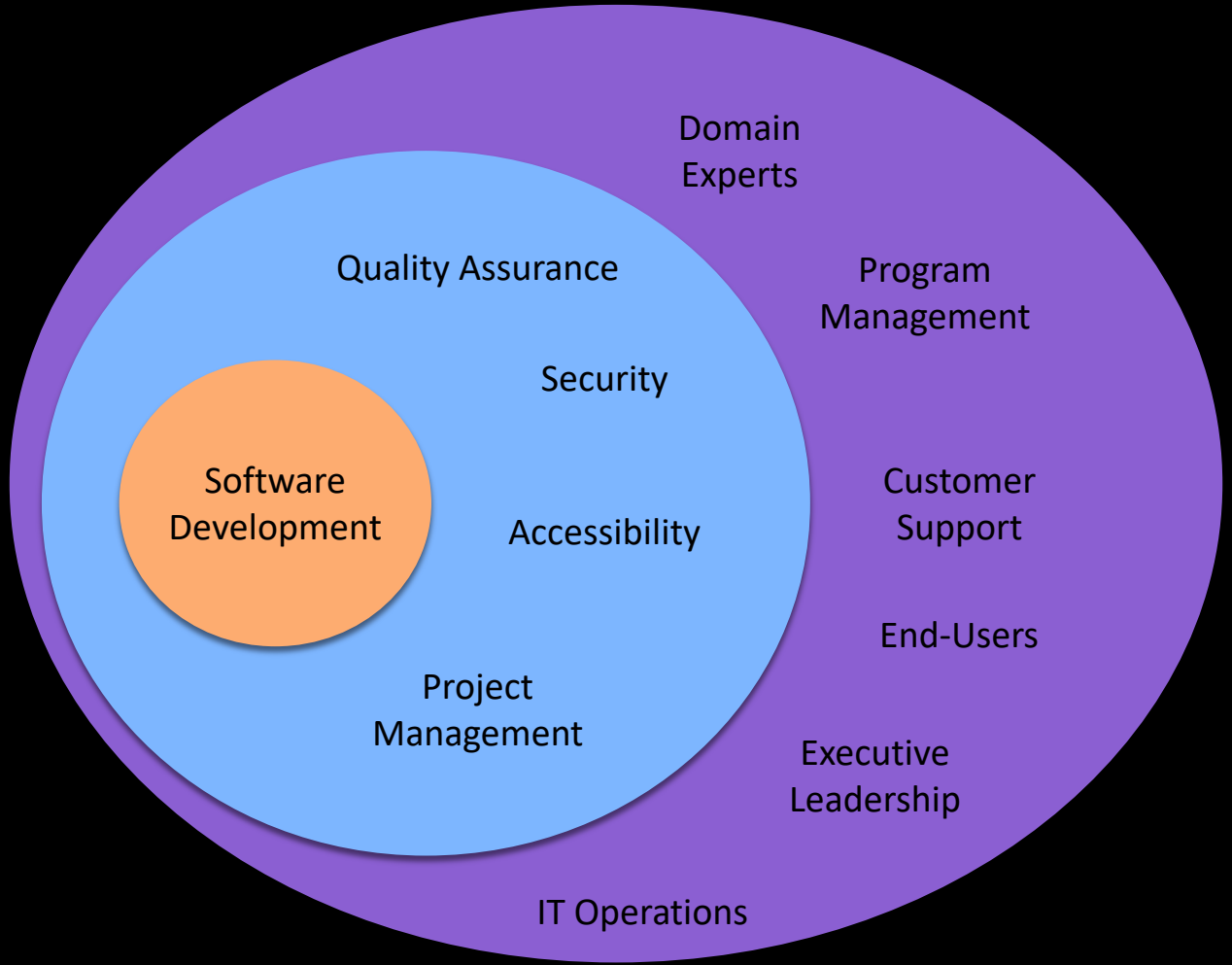
SCM	Database Mgmt	Build
CI	Repo Mgmt	Testing
Deployment	Config / Provisioning	Containerization
Cloud / Iaas / Paas	Release Mgmt	Collaboration
BI / Monitoring	Logging	Security

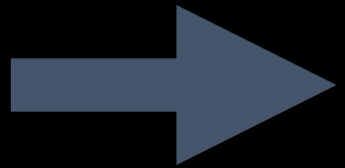
1 Fm Gh Github																		2 Fm Aws Amazon Web Services
3 Os Gt Git	4 Pd Dm DBmaestro												5 En Ch Chef	6 En Pu Puppet	7 Os An Ansible	8 En Sl Salt	9 Os Dk Docker	10 Pd Az Azure
11 Fm Bb Bitbucket	12 Os Lb Liquibase												13 Os Ot Otto	14 En Bl BladeLogic	15 Os Va Vagrant	16 Fr Tf Terraform	17 Os Rk rkt	18 En Gc Google Cloud Platform
19 Os Gl GitLab	20 En Rg Redgate	21 Os Mv Maven	22 Os Gr Gradle	23 Os At ANT	24 Os Fn FitNesse	25 Fr Se Selenium	26 Os Ga Gatling	27 Fr Dh Docker Hub	28 Os Jn Jenkins	29 Pd Ba Bamboo	30 Os Tr Travis CI	31 Pd Gd Deployment Manager	32 Os Sf SmartFrog	33 Os Cn Consul	34 Os Bc Bcfg2	35 Os Lxc Linux Containers	36 En Rs Rackspace
37 Os Sv Subversion	38 En Dt Datical	39 Os Gt Grunt	40 Os Gp Gulp	41 Os Br Broccoli	42 Fr Cu Cucumber	43 Os Cj Cucumber.js	44 Fr Qu Qunit	45 Os Npm npm	46 Fm Cs Codeship	47 Pd Vs Visual Studio	48 Fm Cr CircleCI	49 Fr Cp Capistrano	50 Fr Ju JuJu	51 Os Rd Rundeck	52 Os Cf CFEngine	53 Fr Ds Swarm	54 Os Op OpenStack
55 En Hx Helix	56 En Dp Delphix	57 Fr Sb sbt	58 Os Mk Make	59 Os Ck CMake	60 Fr Jt JUnit	61 Fr Jm JMeter	62 Fr Tn TestNG	63 Os Ay Artifactory	64 Fm Tc TeamCity	65 Fm Sh Shippable	66 Os Cc CruiseControl	67 En Ry RapidDeploy	68 Fm Cy CodeDeploy	69 En Oc Octopus Deploy	70 En No CA Nolio	71 Os Kb Kubernetes	72 Fm Bx Bluemix
73 En Cw ISPW	74 En Id Idera	75 Os Msb MSBuild	76 Os Rk Rake	77 Fr Pk Packer	78 Os Mc Mocha	79 En Xltv XL TestView	80 Os Jm Jasmine	81 Os Nx Nexus	82 Os Co Continuum	83 Fm Ca Continua CI	84 Pd So Solano CI	85 En Xld XL Deploy	86 En EB ElasticBox	87 Fm Dp Deploybot	88 En Ud UrbanCode Deploy	89 Fr Fl Fleet	90 Os Os OpenShift

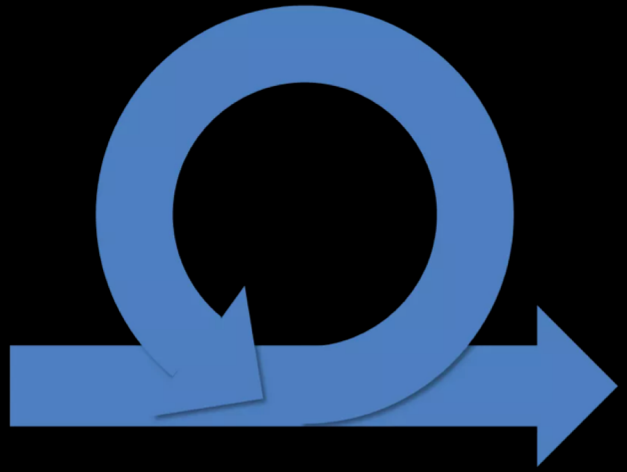
XebiaLabs
Deliver Faster

Follow @xebialabs

91 En Xlr XL Release	92 En Ur UrbanCode Release	93 En Bm BMC Release Process	94 En Hp HP Codar	95 En Au Automic	96 En Pl Plutora Release	97 En Sr Serena Release	98 Pd Tfs Team Foundation	99 Fm Tr Trello	100 Pd Jr Jira	101 Fm Rf HipChat	102 Fm Sl Slack	103 Fm Fd Flowdock	104 Pd Pv Pivotal Tracker	105 En Sn ServiceNow
106 Os Ki Kibana	107 Fm Nr New Relic	108 Os Ni Nagios	109 Os Zb Zabbix	110 En Dd Datadog	111 Os El Elasticsearch	112 En Ss StackState	113 En Sp Splunk	114 Fm Le Logentries	115 Fm Sl Sumo Logic	116 Os Ls Logstash	117 Os Gr Graylog	118 Os Sn Snort	119 Os Tr Tripwire	120 En Ff Fortify


Domain Experts
Quality Assurance
Program Management
Security
Software Development
Customer Support
Accessibility
End-Users
Project Management
Executive Leadership
IT Operations

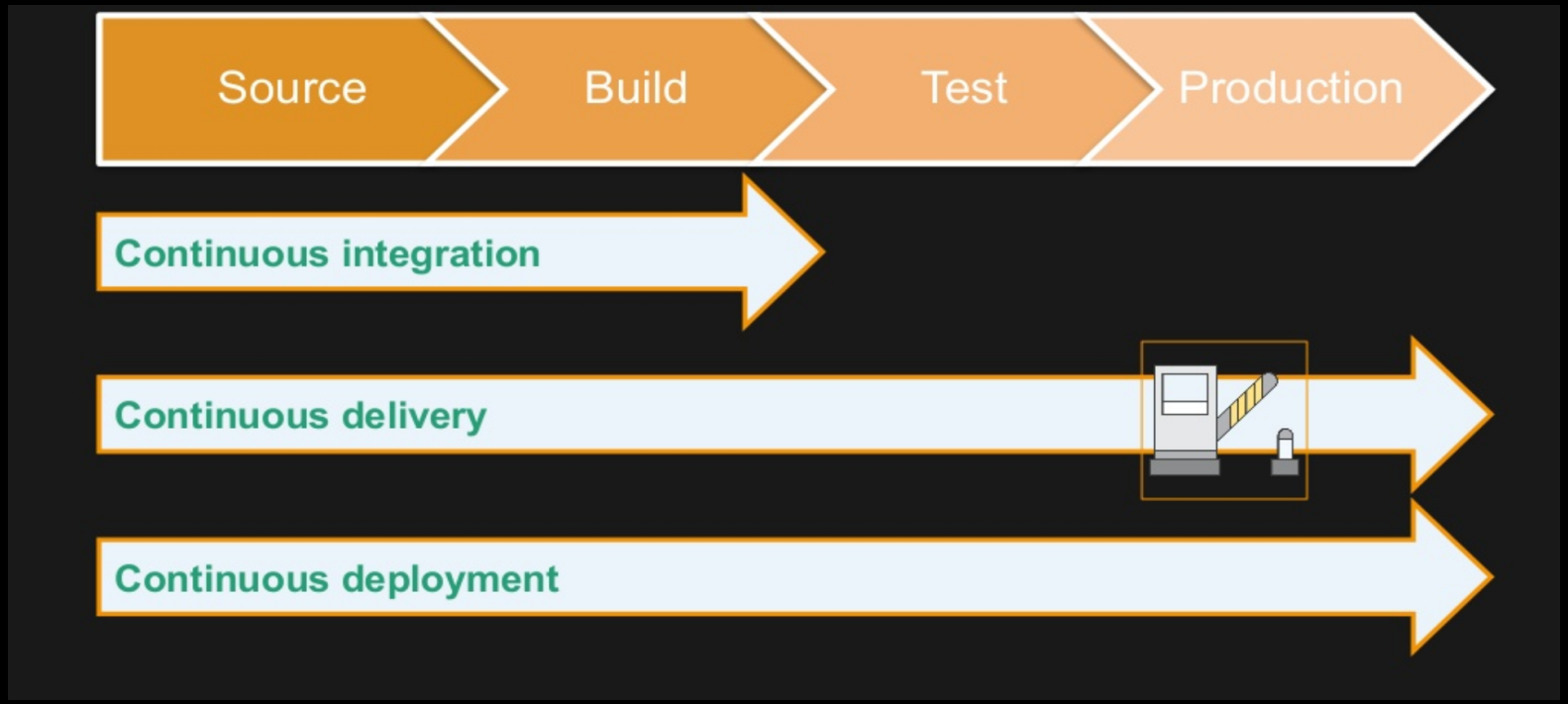




ato authority to operate on aws

aws

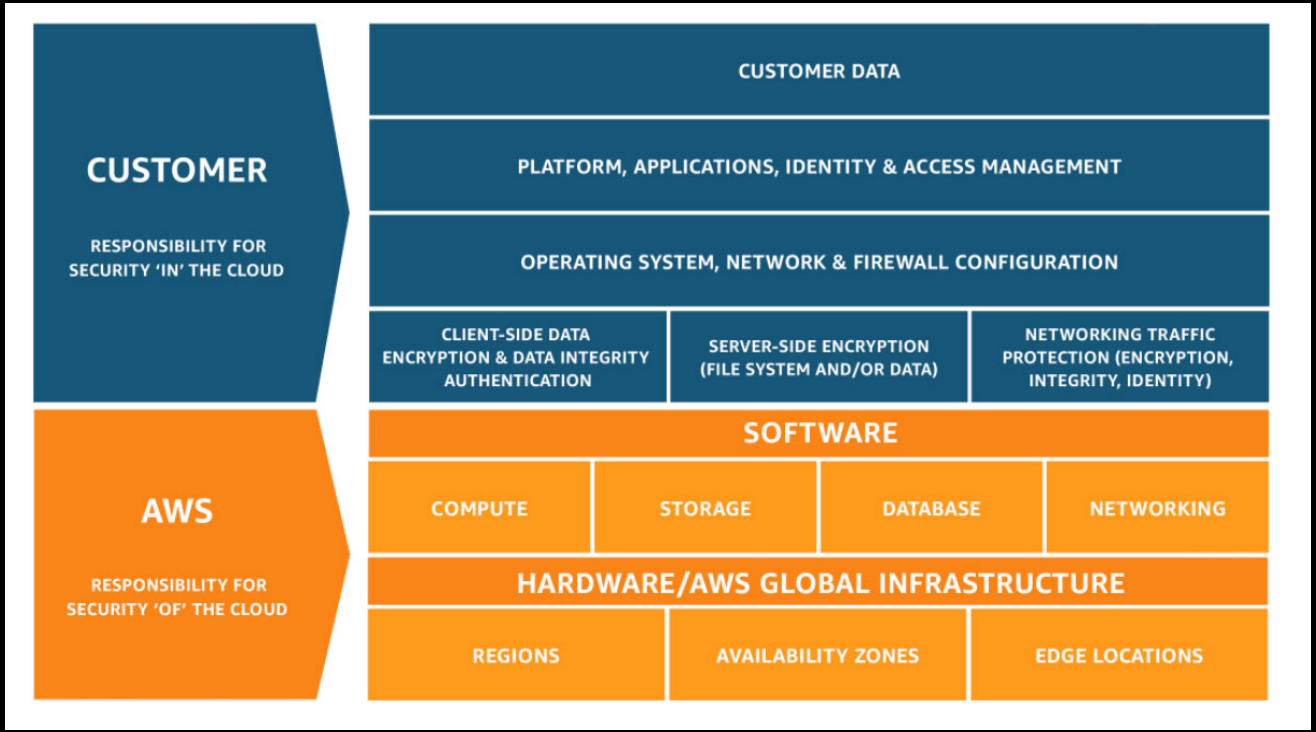
DEVSECOPS RELEASE PROCESSES: LEVELS



ato authority to operate on aws

aws

AWS Shared Responsibility Model



ato authority to operate on aws

aws

What Regulatory Standards are we building for?

ACCELERATING TIME TO COMPLIANCE IN THE AWS CLOUD

International Traffic and Arms Regulation

FedRAMP Moderate and High

DOD Security Req's Guide IL 2, 4 and 5

Criminal Justice Information Service Security Policy

Health Insurance Portability & Accountability Act

IRS Publication 1075

Federal Information Processing Standard Pub

SP 800-53 (rev 4)
SP 800-171

ato authority to operate on aws

aws

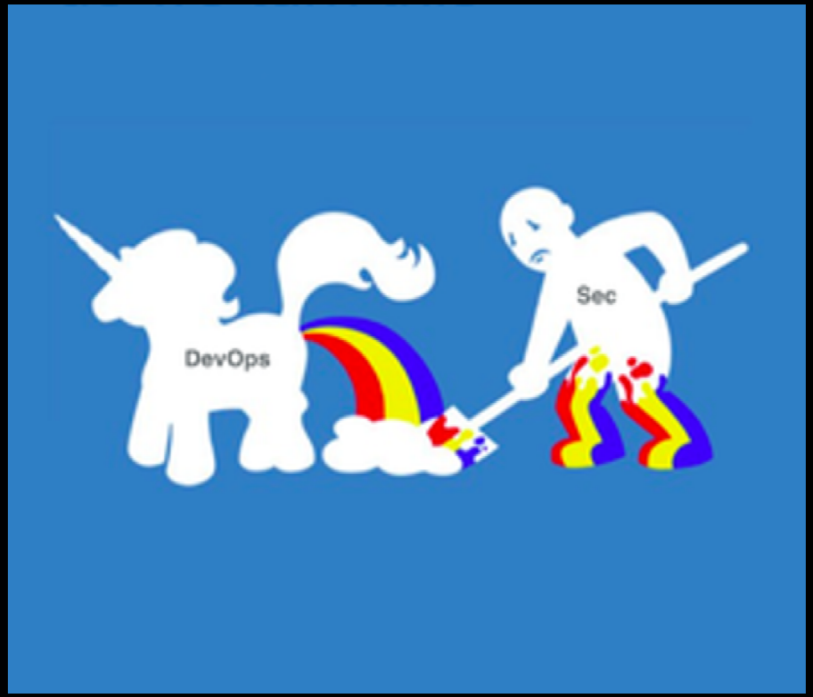
Developer Self-Service – In a Compliance Oriented World

DevOps enables the CI/CD pipeline which is the basis of automation within AWS.

The biggest challenge is breaking out of the traditional security structures and eliminating the divide between developers, operations, and security.

The CI/CD pipeline is the foundation for creating a repeatable, reliable and constantly improving process for taking software from concept to a secure, complaint production solution.

AWSome! But what actually happens in Regulated environments today?



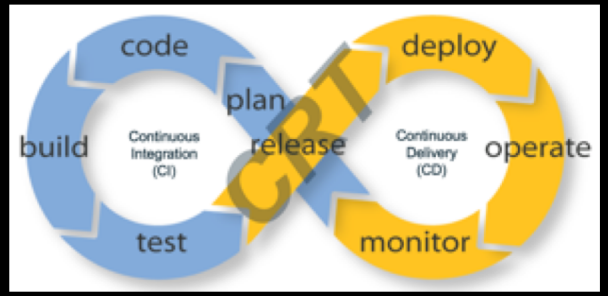
ato authority to operate on aws

aws

Solution Overview: SAO

Develop an **AWS Security Automation and Orchestration (SAO)** repository for constraining, tracking, publishing continuous security configurations, integration, deployments and treatments which are certified against common security frameworks (e.g. FedRAMP, DoD CC SRG, IRS 1075,CIS, PCI, etc.)

SAO will facilitate the orientation and association of **DevOps** and **Security** practices, changes and coordination of **Continuous Integration (CI)**, **Continuous Delivery (CD)** and **Continuous Risk Treatment (CRT)*** of an AWS customer account and/or multiple accounts.



* CRT is a process and technology approached which is designed to detect, maintain and in *MOST* case correct security, compliance and threats associated with an organization's solution and service deployment within their AWS account. CRT processes monitor security controls in real-time to ensure the risk and/or threat treatment (Control Intent) is working as designed or at least within an intended margin of acceptance base on guard rails, swim lanes and/or rules built into the control to allow for business operations.

The Result:
"AWS Trust Boundary In a Box"

1. Templates, Scripts, Functions and Recipes for securely deploying regulated workloads "Type Accreditation" (Pre-Audited), for all stages of Cloud Service adoption, (Migrator, Forward, Native)

2. Defined operational security and compliance tolerances scripts, functions and treatments (e.g. Guard Rails) for constrained secure operations across the DevOPS CI/CD and CRT through the use of **Governance as Code** (GoC) practices

3. Deployable Continuous Risk Treatments (CRT) resources (e.g. AWS & Partners solutions)

ato authority to operate on aws

aws

Customer Case Study - SmartSheet

- Targeted FedRAMP Moderate

- No presence in AWS GovCloud

- Embraced the frame-work, principles, and methodology to accelerate the ATO process.

- 60 Days to their full SaaS in a FedRAMP “Ready” state.
- 30 Days for documentation.

- 90 Days to go up for review.

AWS FedRAMP ATO's issued in 2018

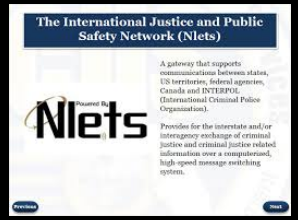
AWS East/West ATO's

US GovCloud ATO's

SAO – Pilot Deployment's in 2018

ATO's & Certifications

ATO's and Certifications in Process



Why do we pitch ATO on AWS this way?

- IT Stakeholders still view cloud as a threat to their current position.
- CISO offices, will tell you “We can do this On-Premise”. Embrace the Challenger Model.
- A standard ISV FedRAMP Moderate authorization averages:
    - 18-24 Months
    - $1,000,000
- “Everything as Code”, keeps the need for critical skill-sets around operations, security, and compliance, while offering an avenue for career re-invention.
- With Cloud becoming the “New-Normal”, not learning these paradigms, is what could lead to role reduction.
- Customers need to understand that it isn’t that hard to learn this.
- The Business Owner needs to be our top priority.

ato authority to operate on aws

aws

Selling ATO on AWS – Why should we get involved?

Eric Baran
DevOps Segment Leader – Regulated Industries

ATO Sales Kick Off 2019

ato authority to operate on aws

aws

The Anatomy of the AWS Account Executive

ato authority to operate on aws

aws

Great – Everything is code…

So what? Why does this matter to me?

ato authority to operate on aws

aws

AWS is Peculiar – Let's explain…

- We are growing. Fast.
- Sales Representatives are coming from all different backgrounds and experience levels.
- Many from large SI's, or ISV's.
- Many understand how to sell to the Data-Center.
- Leadership Principles are real – most important of which is customer obsession.
- Reps are paid on customer success, which for an AWS seller, that means consumption.

ato authority to operate on aws

aws

Why do our reps care about ATO on AWS?

- AWS Sales Reps are getting asked about Security and Compliance, around the published regimes, in 99% of their customer interactions.

- Automation is key to accelerating consumption, (which is why DevSecOps is so important).

- Building in a framework for Security and Compliance automation, allows teams to realize the benefits of innovation.

ato authority to operate on aws

aws

30 Users. 5 Apps. - $500,000 in Dev/Test Alone.

DEV	
Cost of M4 Large	$417
Avg. # of Devs	30
Total for DEV in Cloud	$12,500
TEST	
Avg. # Servers/App	5 (2 web/2 app/1 db)
Avg. # Apps in Test	5
Total for TEST in Cloud	$5,200 (1/2 compute)
$17,700 for Basic Dev/Test in Cloud	
Dev/Ops SERVICES	
30 Users	$2700
10 Agents (build/test/deploy)	$4,300
Cloud-Based Test	$1,400
$6,000 for Dev/Ops Services	

ato authority to operate on aws

aws

ATO on AWS, a “Product” or a “Program”?

- It’s both.

- Anitian launched the first “Productized” version of the package.

- Ultimate vision is to provide our customers the choice and freedom to utilize any tool, or process, to automate Security and Compliance as part of their modernization strategy.

- We are ready to work with you, to help build that choice for our customers.

ato authority to operate on aws

aws

Why should you be part of ATO on AWS?

- Since the RE:Invent announcement/launch of the program, we have uncovered:
    - 56 Net-New Opportunities with 5-10 coming in every week.
    - Crosses ISV, Public Sector, SI, and Regulated Verticals

- You are now part of a “Solution”, solving a critical problem for the AWS Account Teams.
    - Translation = ”They will care about your solution set.”

- Monetize your open source install base.
    - We only package and deploy the paid/enterprise listings of our partners solutions.

- The ATO on AWS Framework can be utilized directly, to advance your own Accreditation charters.

ato authority to operate on aws

aws

What does our team look like for 2019?

- ATO on AWS, is a program within a new SaaS enablement/acceleration team.
    - DevOps
    - Intelligence Community
    - Big Data/Analytics
    - Security and Compliance

- Laser focus on ISV Success with AWS, and your solutions.

- Transform organizations into an “Everything as Code” model, to iterate, and innovate on top of the AWS back-bone.

ato authority to operate on aws

aws

Any Questions?

ato authority to operate on aws

aws