



San Francisco | March 4–8 | Moscone Center



SESSION ID: CSV-T09

Security at the Speed of DevOps

Steve Martino

SVP, Chief Information Security Officer
Cisco

Sujata Ramamoorthy

Sr. Director, Information Security
Cisco

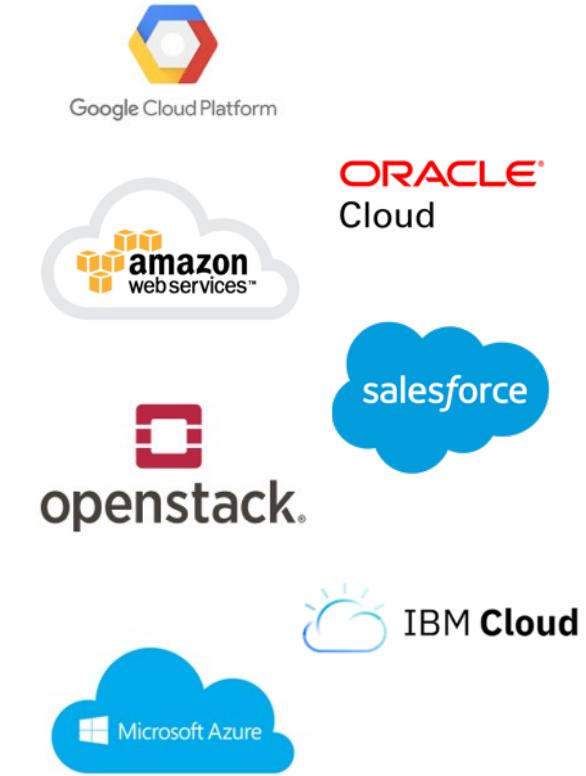
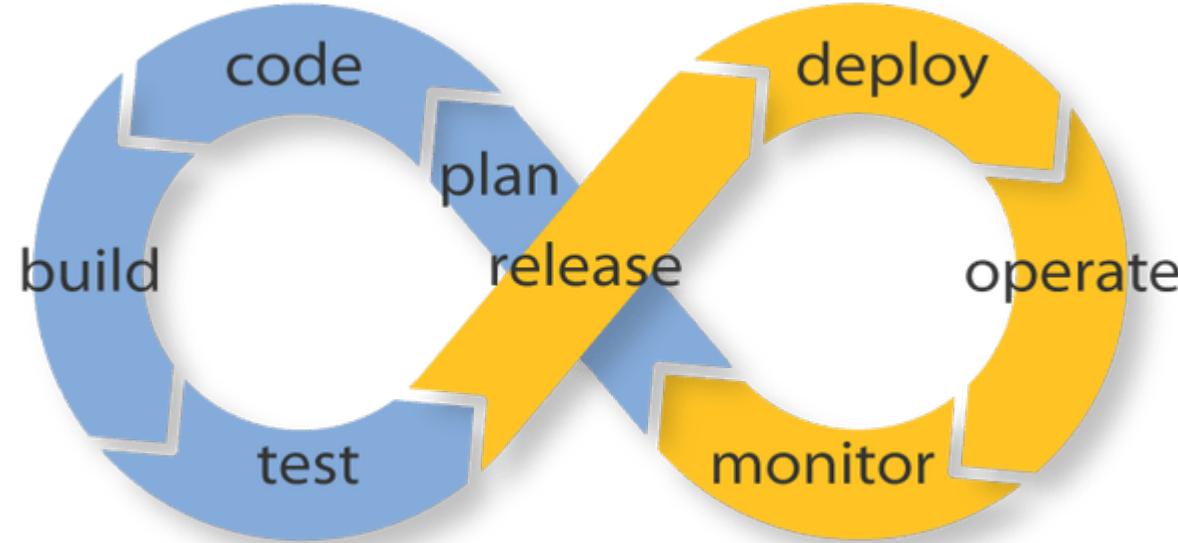
#RSAC

RSA®Conference2019

Our Move to Embed Security in DevOps |

An abstract graphic in the background features a dense web of thin, light blue lines forming a complex network or mesh pattern against a dark purple background. This visual metaphor represents connectivity, data flow, and the interconnected nature of security and development in modern technology.

DevOps Practices Paired with Cloud Adoption



Endless Possibilities:

DevOps can create an endless loop of release and feedback for all code and deployment targets

Success Criteria



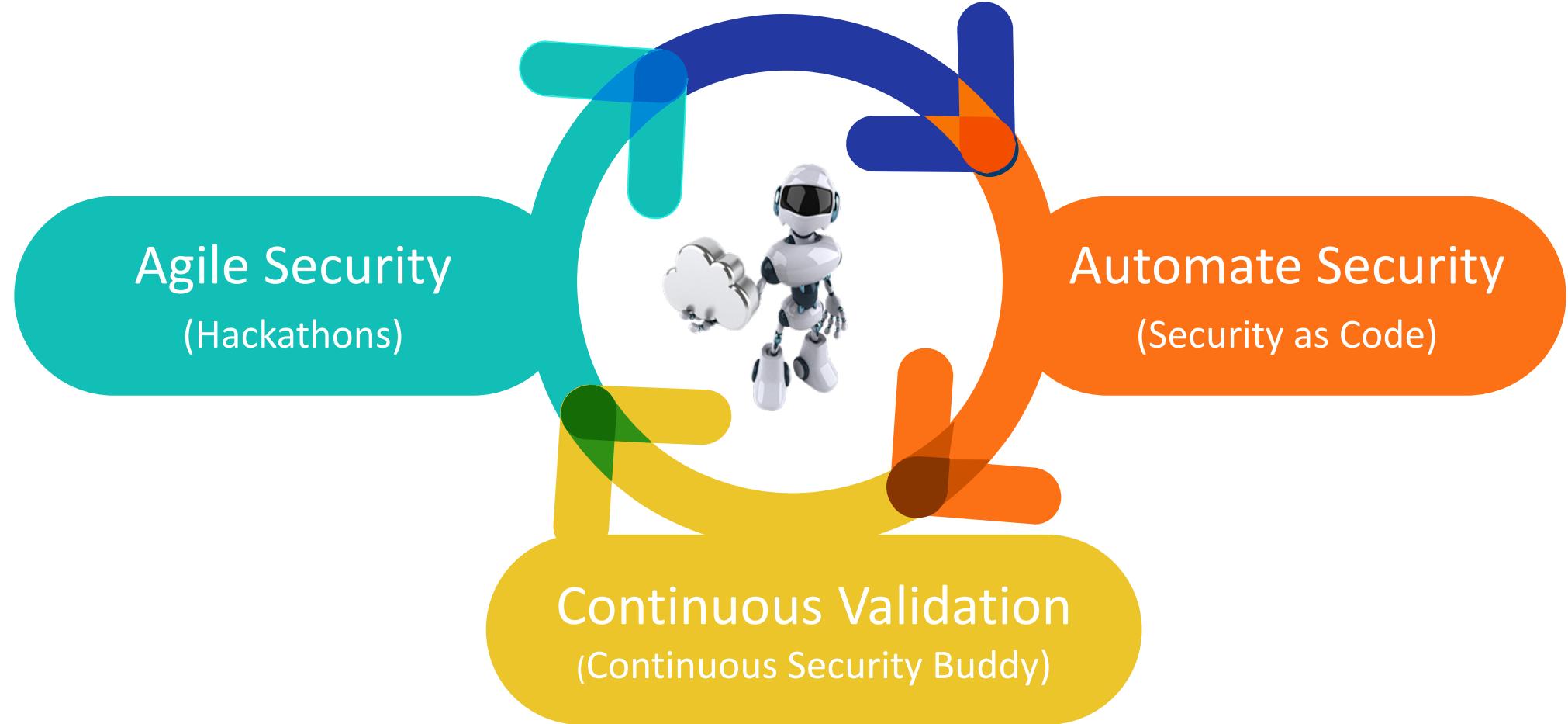
Time to Value

RSA®Conference2019

Operational Change



How Do We Drive DevSecOps?



What's a Security Hackathon?

You may think it's this:



It's more like this:



Hackathon Goals

Complete and publish
top security guardrails
for AWS

Pre-Work Planning

- Identify top security use cases in AWS
- Team member assignment

Event Logistics

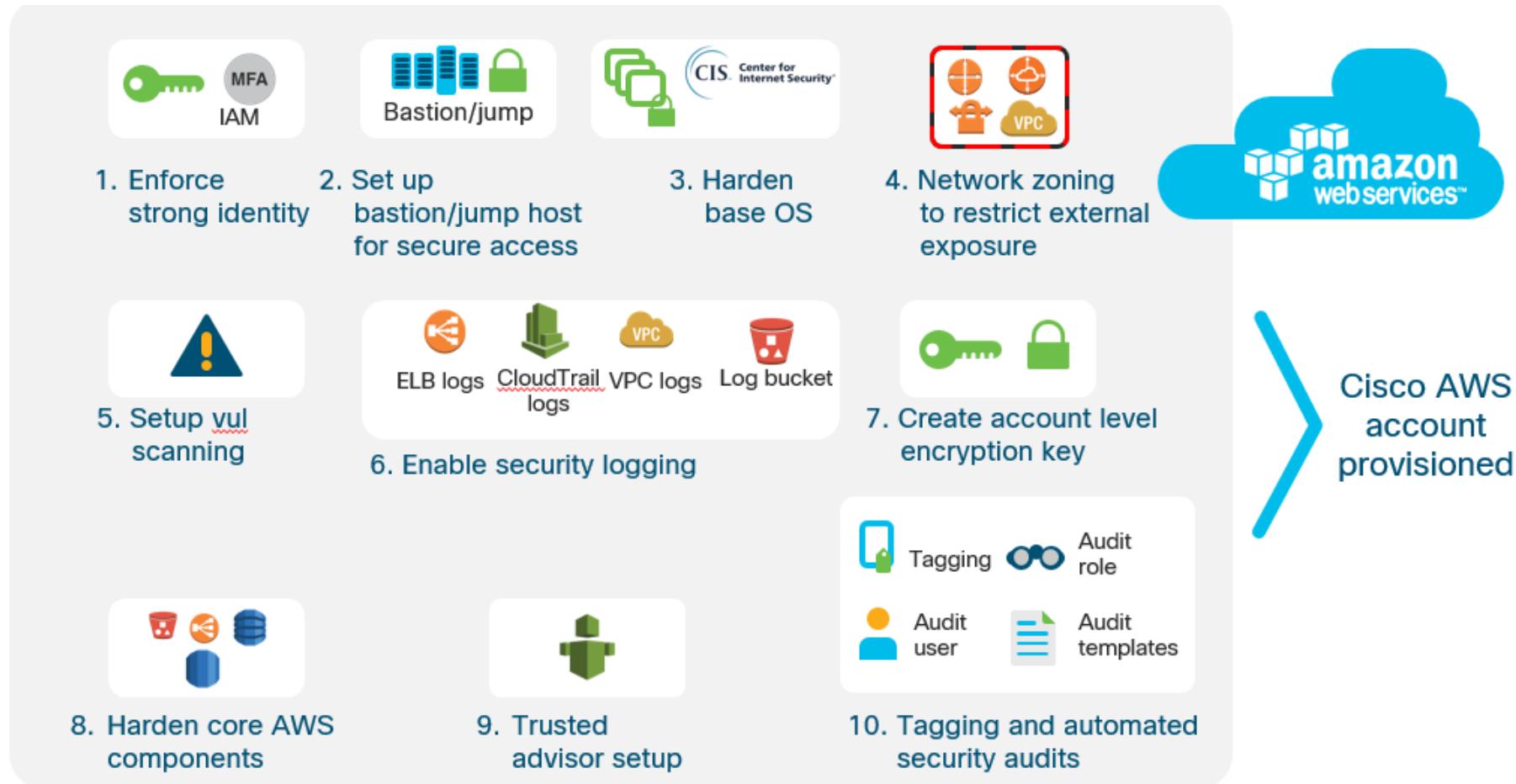
- Run in sprints
- Sprint readout
- Peer reviews
- Definition of Done (DOD)
- Document Findings

Retrospective

- What worked / Didn't work
- Improvements
- Next steps

Security Guardrails for Cisco AWS Accounts

New AWS account request



RSA® Conference 2019

Visual Walk-Through



Manual Account Provisioning

PRODUCTS & SERVICES

[AWS Console](#)[FAQs](#)

RELATED LINKS

[Documentation](#)[Articles & Tutorials](#)[Developer Tools](#)[Public Data Sets](#)[Amazon Machine Images \(AMIs\)](#)[Videos & Webinars](#)[What's New](#)[Manage Your Resources](#)[Sign In to the Console](#)

AWS Management Console

Access and manage Amazon Web Services through a simple and intuitive web-based user interface. You can also use the [AWS Console mobile app](#) to quickly view resources on the go.

Get Started with AWS for Free

[Create a Free Account](#)[Or Sign In to the Console](#)

Receive twelve months of access to the [AWS Free Usage Tier](#) and enjoy AWS Basic Support features including, 24x7x365 customer service, support forums, and more.

Features

Administer your AWS account

The Console facilitates cloud management for all aspects of your AWS account, including monitoring your monthly spending by service, managing security credentials, or even setting up new IAM Users.

All IaaS AWS administration, management, and access functions in the AWS Console are available in the AWS API and CLI. New AWS IaaS features and services provide full AWS Console functionality through the API and CLI at launch or within 180 days of launch.

Access and manage Amazon Web Services through a simple, intuitive web-based user interface. You can also use the [AWS mobile app](#) to quickly view resources on the go.

Get Started with AWS for Free

[Create a Free Account](#)

[Or Sign In to the Console](#)

Receive twelve months of access to the [AWS Free Usage Tier](#) and enjoy AWS Basic Support features including, 24x7x365 customer service, support forums, and more.

Features

Administer your AWS account

The Console facilitates cloud management for all aspects of your AWS account, including monitoring your monthly spending by service, managing security credentials, or even setting up new IAM Users.

All IaaS AWS administration, management, and access functions in the AWS Console are available in the AWS API and CLI. New AWS IaaS features and services provide full AWS Console functionality through the API and CLI at launch or within 180 days of launch.

Finding Services in the AWS Console

There are several ways for you to locate and navigate to the services you need. On Console Home, you can utilize the search functionality, select services from the *Recently visited services* section, or expand the *All services* section to browse through the list of all the services offered by AWS.

At any time, you can also select the *Services* menu in the top level navigation bar, which includes the search functionality and the list of all services, either grouped, or arranged alphabetically.

Access and manage your AWS services using the intuitive web-based console or the mobile app to quickly get started.

Features

Administer your AWS account

The Console facilitates creating and managing security credentials for your AWS account.

All IaaS AWS administrative tasks are performed through the AWS Management Console. You can access all IaaS features and services from the AWS Management Console.

Finding Services

There are several ways for you to find the services you need. To search for a service by name, use the search functionality, select services from the navigation bar, or browse all the services offered by AWS.

At any time, you can also sign in to the AWS Management Console to view all services, either grouped by service or by category.

Create an AWS account

Email address

aws-demo-account@cisco.com

Password

Vatgen-kytzo5-cyf0z

Strong Password

Confirm password

Vatgen-kytzo5-cyf0z

Strong Password

AWS account name i

Cisco AWS Demo Account

Continue

[Sign in to an existing AWS account](#)

© 2019 Amazon Web Services, Inc. or its affiliates.

All rights reserved.

[Privacy Policy](#) | [Terms of Use](#)

Get Started for Free

Account

Console

Access to the AWS

Amazon AWS Basic
Services, 24x7x365 support, forums, and

CloudWatch Metrics

CloudWatch Logs

I. New AWS
Services

CloudWatch Metrics

CloudWatch Logs

Search
through the list of
AWS services

CloudWatch Metrics

CloudWatch Logs

CloudWatch Metrics

CloudWatch Logs

AWS Manager

Access and manage AWS services from an intuitive web-based user interface or our mobile app to quickly view and analyze your usage.

Features

Administer your AWS account

The Console facilitates cloud management, including managing security credentials.

All IaaS AWS administration, including managing IaaS features and services provided by AWS.

Finding Services in the AWS Marketplace

There are several ways for you to find the right functionality, select services from the Marketplace, and view all the services offered by AWS.

At any time, you can also select services from the Marketplace to view all services, either grouped, or

Please select the account type and complete the fields below with your contact details.

Account type i

Professional Personal

Full name

Cisco AWS Demo Account

Company name

Cisco Systems

Phone number

4255551212

Country/Region

United States

Address

170 W Tasman Dr

Apartment, suite, unit, building, floor, etc.

City

San Jose

State / Province or region

CA

Postal code

95134



Check here to indicate that you have read and agree to the terms of the [AWS Customer Agreement](#)

Create Account and Continue

AWS for Free

Create Account

View the Console

Get started with AWS for Free. Get free access to the AWS Basic Support tier, including, 24x7x365 support, developer forums, and more.

Manual CSB Install

AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.

 Example: Relational Database Service, database, RDS

▶ Recently visited services

▼ All services

-  **Compute**
 - EC2
 - Lightsail 
 - ECR
 - ECS
 - EKS
 - Lambda
 - Batch
 - Elastic Beanstalk
 - Serverless Application Repository
-  **Management & Governance**
 - CloudWatch
 - AWS Auto Scaling
 - CloudFormation
 - CloudTrail
 - Config
 - OpsWorks
 - Service Catalog
 - Systems Manager
 - Trusted Advisor
-  **AWS Cost Management**
 - AWS Cost Explorer
 - AWS Budgets
 - AWS Marketplace Subscriptions
-  **Mobile**
 - AWS Amplify
 - Mobile Hub
 - AWS AppSync
 - Device Farm

AWS Management Console



Services ▾

Resource Groups ▾



admin/bparriot@cisco.com @

History

Console Home

S3

CodeCommit

CloudFormation

CloudSearch

IAM

Cloudformation|

CloudFormation

Create and Manage Resources with Templates

ECS

Blockchain

EKS

Amazon Managed Blockchain

Athena

Alexa for B

EMR

Amazon Ch

CloudSearch

WorkMail

Elasticsearch Service

Kinesis

End User

▼ All services

Compute

EC2

Lightsail ↗

ECR

ECS

EKS

Lambda

Batch

Elastic Beanstalk

Serverless Application Repository

Management & Governance

CloudWatch

AWS Auto Scaling

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Systems Manager

Trusted Advisor

AWS Cost Management

AWS Cost Explorer

AWS Budgets

AWS Marketplace Subscriptions

Mobile

AWS Amplify

Mobile Hub

AWS AppSync

Device Farm

Filter: Active ▾ By Stack Name

Create a stack

AWS CloudFormation allows you to quickly and easily deploy your infrastructure resources and applications on AWS. You can use one of the templates we provide to get started quickly with applications like WordPress or Drupal, one of the many sample templates or create your own template.

You do not currently have any stacks. Choose **Create new stack** below to create a new AWS CloudFormation stack.

[Create new stack](#)

Create a StackSet

A StackSet is a container for AWS CloudFormation stacks that lets you provision stacks across AWS accounts and regions by using a single AWS CloudFormation template.

[Create new StackSet](#)

Design a template

Templates tell AWS CloudFormation which AWS resources to provision and how to provision them. When you create a CloudFormation stack, you must submit a template.

To build and view templates, you can use the drag-and-drop tool called AWS CloudFormation Designer. You drag-and-drop the resources that you want to add to your template and drag lines between resources to create connections. To use Designer to create a template or to open and modify a template, choose

[Design template.](#)[Design template](#)

Filter: Active ▾ By Stack Name

Create a stack

AWS CloudFormation allows you to quickly and easily deploy your infrastructure resources and applications on AWS. You can use one of the templates we provide to get started quickly with applications

Create a stack

AWS CloudFormation allows you to quickly and easily deploy your infrastructure resources and applications on AWS. You can use one of the templates we provide to get started quickly with applications like WordPress or Drupal, one of the many sample templates or create your own template.

You do not currently have any stacks. Choose **Create new stack** below to create a new AWS CloudFormation stack.

Create new stack

Templates tell AWS CloudFormation which AWS resources to provision and how to provision them. When you create a CloudFormation stack, you must submit a template.

To build and view templates, you can use the drag-and-drop tool called AWS CloudFormation Designer. You drag-and-drop the resources that you want to add to your template and drag lines between resources to create connections. To use Designer to create a template or to open and modify a template, choose **Design template**.

Design template

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

[Design template](#)

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Select a sample template

Upload a template to Amazon S3

[Choose File](#) no file selected

Specify an Amazon S3 template URL

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

[Design template](#)

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Upload a template to Amazon S3

[Choose File](#) no file selected

Specify an Amazon S3 template URL

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template

Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

[Design template](#)

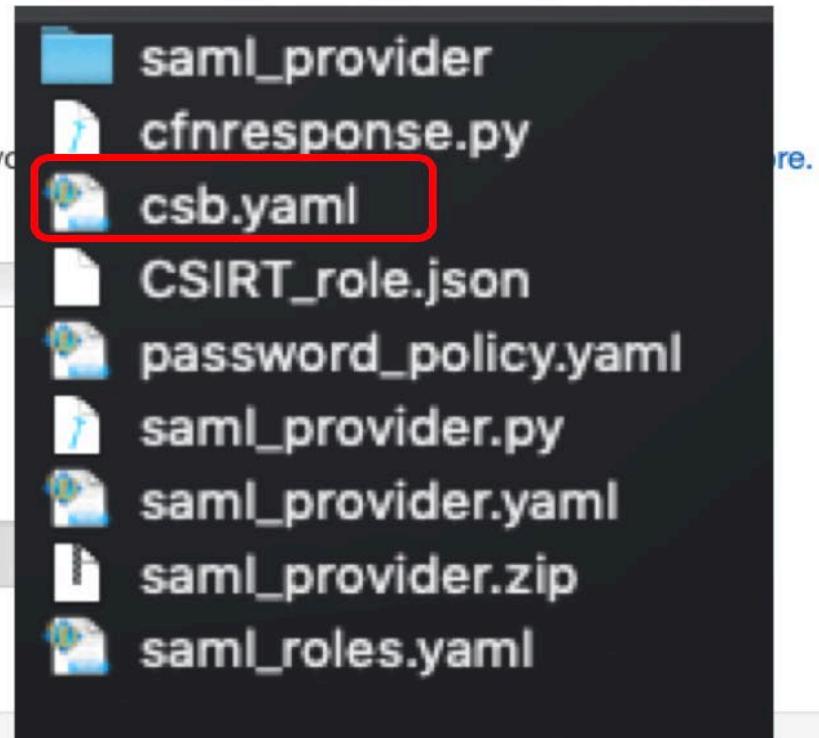
Choose a template

A template is a JSON/YAML-formatted text file that describes your stack's resources.

- Upload a template to Amazon S3

[Choose File](#) no file selected

- Specify an Amazon S3 template URL



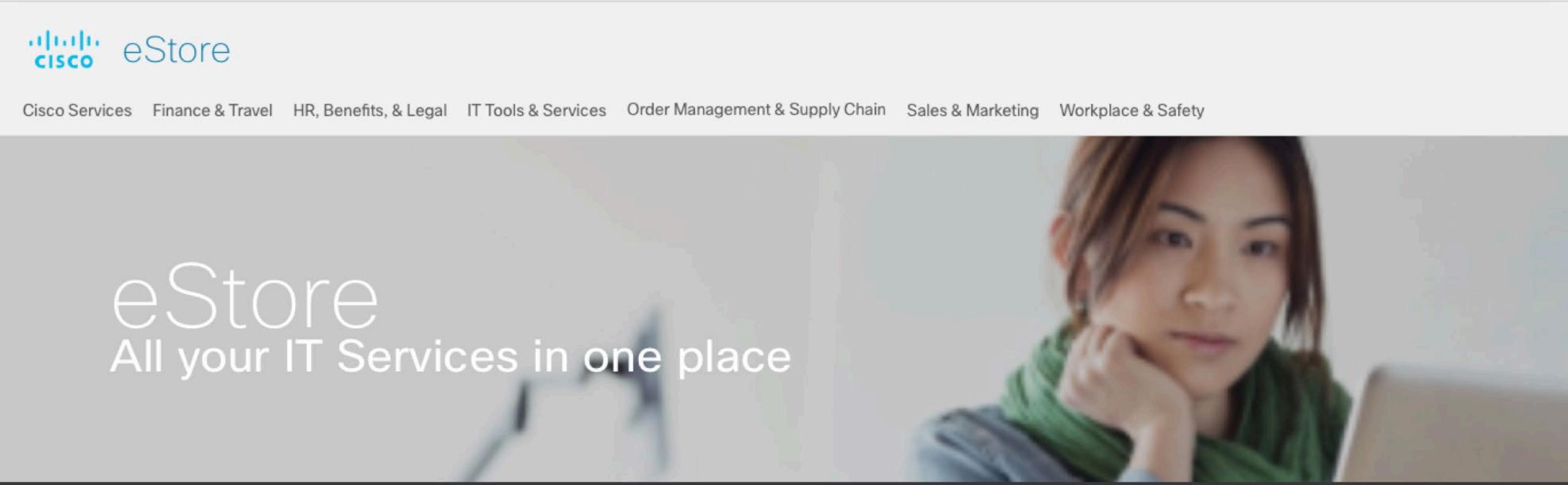
Manual CSB Installation

	File	CF Stack Name	AWS Resource Modified/Created
1	csb.yaml	InfosecAuditorRole	Lambda Role Auditor Role
2	CSIRT_role.json	InfosecCSIRTRole	Cisco Security Incident Response Role
3	password_policy.yaml	IAMPasswordRole	Password Policy
4	saml_provider.yaml	CiscoSSOSAMLProvider	Identity Provider Lambda Role
5	saml_roles.yaml	CiscoSSOSAMLRoles	admin role devops role
6	vuln_mgmt_scanner	CiscoScanner	Lambda Role Cross Account Role

Automated Provisioning

eStore

All your IT Services in one place

A blurred background image of a woman with long brown hair, wearing a green scarf, looking thoughtfully at a laptop screen. The screen shows a colorful bar chart.

What are you looking for?



Explore Collections

[Show all](#)[Sales Teams](#)[Frequent Travelers](#)[Cisco Essentials](#)[Engineering Teams](#)[Hiring Managers](#)[IT Teams](#)

eStore

All your IT Services in one place

AWS



Services

[Amazon Web Services - Create Account](#)[Oracle Business Intelligence Enterprise Edition \(OBIEE\) - Configuration and General Requests](#)

Explore

Show

Sales Teams

Frequent Travelers

Cisco Essentials

Engineering Teams

Hiring Managers

IT Teams



Amazon Web Services - Create Account

Create an account on AWS and begin your development effort in public cloud while automatically leveraging Cisco's enterprise agreement for pricing and Infosec's Continuous Security Buddy for policy adherence. eStore will route your request for the appropriate leadership and financial approvals so that you can focus on building your application.

Order

Order for Others

Specification ▾





AWS - Create Account

Create an account on AWS and begin your development effort in public cloud while automatically leveraging Cisco's eStore Agreement for pricing and Infosec's Continuous Security Buddy for policy adherence. eStore will route your request to the appropriate leadership and financial approvals so that you can focus on building your application.

tion ▾



**Order****Order for Others**Amazon Web Services - Create Account X

Create an account on AWS and begin your development effort in public cloud while automatically leveraging Cisco's enterprise agreement for pricing and Infosec's Continuous Security Buddy for policy adherence. eStore will route your request for the appropriate leadership and financial approvals so that you can focus on building your application.

▼ Recipient Information

Recipient

Email Address

Demo User

Username (CEC ID)

Demo_user@cisco.com

Phone

Demo_user

▼ Account Information

Department

ID

(used for billing purposes - If charges apply)

Cisco Business Unit/Org

Name

 1234567

Financial Analyst (CEC ID):

Security Business Group

RootEmailId

random

This email ID will be used as root user ID for AWS account. It has to be a unique email ID and this

Demo_user@cisco.com

Submit**Cancel**

Account

natically leveraging Cisco's
erance. eStore will route your
ilding your application.



Create an account on AWS and begin your development effort in public cloud while automatically leveraging Cisco's enterprise agreement for pricing and Infosec's Continuous Security Buddy for policy adherence. eStore will route your request for the appropriate leadership and financial approvals so that you can focus on building your application.

Order**Order for Others****Recipient Information**

Recipient	Demo User
Email Address	Demo_user@cisco.com
Username (CEC ID)	Demo_user
Phone	(425) 555-1212

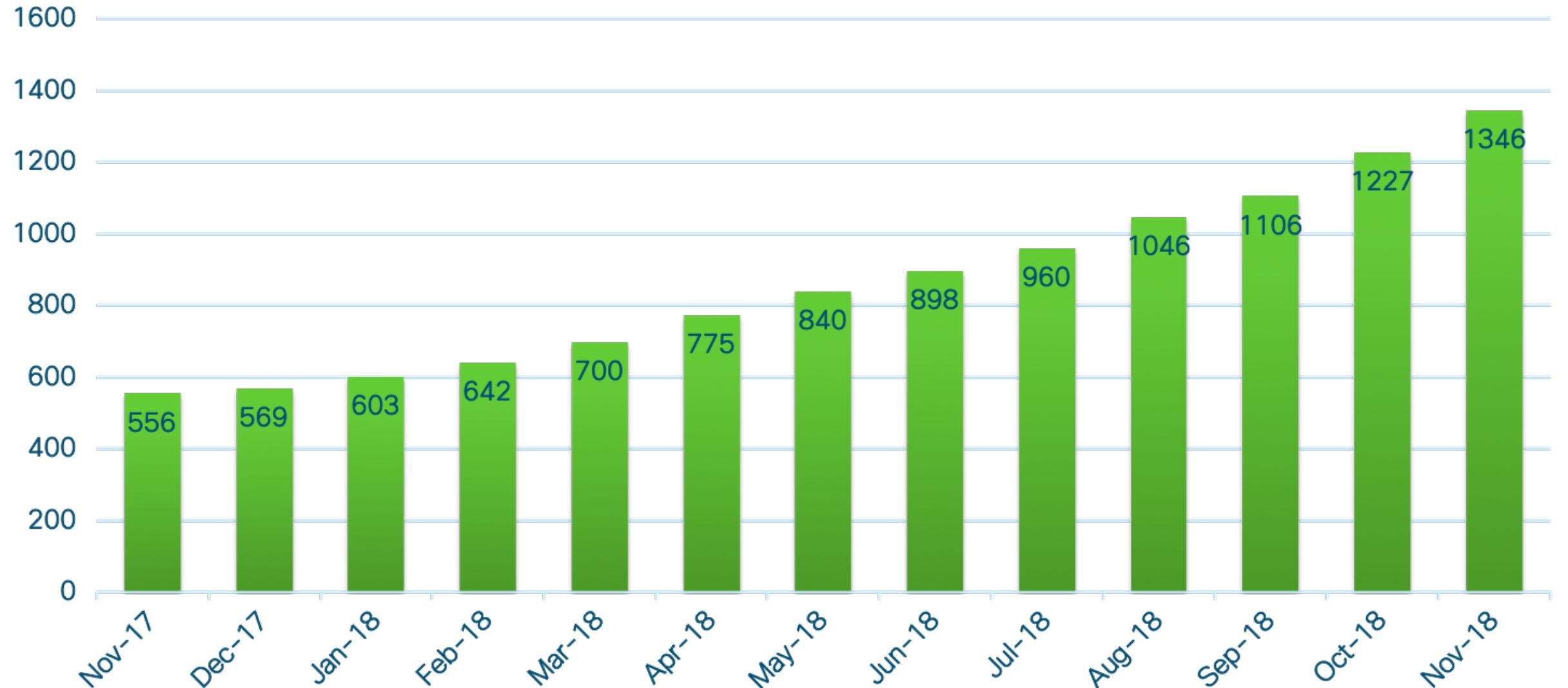
Account Information

Department ID	1234567
Cisco Business Unit/Org Name	Security Business Group
Financial Analyst (CEC ID):	random
RootEmailId	Demo_user@cisco.com

This email ID will be used as root user ID for AWS account. It has to be a unique email ID and this

Submit**Cancel**

CSB Installed AWS Accounts

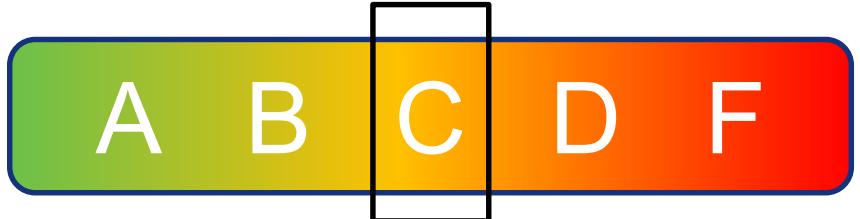


Reporting Baseline

Daily Reporting



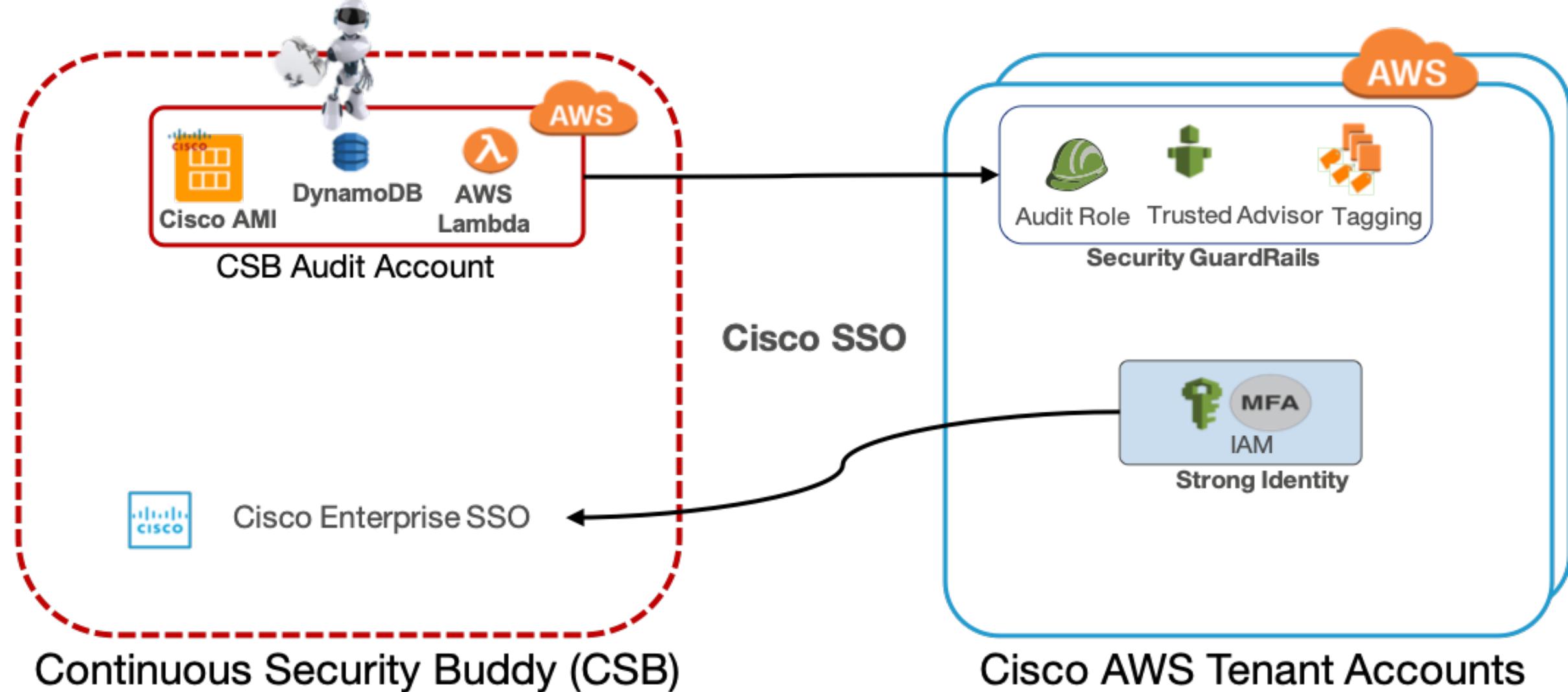
Overall Risk Score:



Section	Section Score
1. Identity and Access Management	- 80/100
2. Network Security	- 90/100
3. Storage (S3 buckets)	- 90/100
4. Tagging	- 0/100
5. External Vulnerabilities	- 100/100
6. CIS AWS Benchmarks	- 90/100
7. Trusted Advisor Checks	- Not Scored

IAM Changes

SSO Insertion



Section 1: Identity and Access Management

Compliance Score: 85.0%

1. IAM users without MFA enabled [SEC-CRE-MULTIFAC]: [None]
2. MFA enabled on Root user? [SEC-CRE-MULTIFAC]: No
3. MFA Compliance [SEC-CRE-MULTIFAC] (0/0): 100.0%
4. Access Key Rotation Violation (90+ days) [SEC-OPS-REVOKE]: (total = 1)
 1. <root_account>
5. Cisco SSO Enabled? [SEC-CRE-SSO]: Yes
6. Login using root account (logins in last 7 days): [None]

AWS Management Console

AWS services

Find Services

You can enter names, keywords or acronyms.

 Example: Relational Database Service, database, RDS



IAM

S3

 CodeCommit

 CloudSearch

► All services

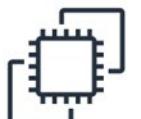
Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine

With EC2

2-3 minutes



Build a web app

With Elastic Beanstalk

6 minutes



Build using virtual servers

With Lightsail

1-2 minutes



IAM Resources

Users: 0

Roles: 26

Groups: 2

Identity Providers: 1

Customer Managed Policies: 3

Security Status

 2 out of 5 complete.



Delete your root access keys



Activate MFA on your root account



IAM Resources

Users: 0

Roles: 26

Groups: 2

Identity Providers: 1

Customer Managed Policies: 3

Security Status

 2 out of 5 complete.



Delete your root access keys



Delete your AWS root account access keys, because they provide unrestricted access to your AWS resources. Instead, use IAM user access keys or temporary security credentials. [Learn More](#)

[Manage Security Credentials](#)



Activate MFA on your root account





You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

[Continue to Security Credentials](#)

[Get Started with IAM Users](#)



Don't show me this message again

- ▲ Password
- ▲ Multi-factor authentication (MFA)
- ▼ Access keys (access key ID and secret access key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Mar 1st 2019		AKIAIXKW3FI4YWLQJJQ	N/A	N/A	N/A	Active	Make Inactive Delete

[Create New Access Key](#)



Important Change - Managing Your AWS Secret Access Keys

As described in a [previous announcement](#), you cannot retrieve the existing secret access keys for your AWS root account, though you can still create a new root access key at any time. As a [best practice](#), we recommend [creating an IAM user](#) that has access keys rather than relying on root access keys.

- ▲ Password
- ▲ Multi-factor authentication (MFA)
- ▼ Access keys (access key ID and secret access key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

Created
Mar 1st 2019

Create New Access Key

Import

Are you sure you want to delete the access key with ID AKIAIXKW3FI4YWLQJJQ?

Warning: If you delete an access key, any requests signed with that access key ID and secret access key will fail.
You cannot reactivate a deleted access key.

As described in a [previous announcement](#), you cannot retrieve the existing secret access keys for your AWS root account, though you can still create a new root access key at any time. As a [best practice](#), we recommend [creating an IAM user](#) that has access keys rather than relying on root access keys.

Status	Actions
Active	Make Inactive Delete

- ▲ CloudFront key pairs
- ▲ X.509 certificate
- ▲ Account identifiers

IAM Resources

Users: 0

Roles: 26

Groups: 2

Identity Providers: 1

Customer Managed Policies: 3

Security Status

 3 out of 5 complete.



Delete your root access keys



Activate MFA on your root account



Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. [Learn More](#)

[Manage MFA](#)

Your Security Credentials

Use this page to...

...the IAM Console.

To learn more about...

▼ Password

You use an em...
that contains n...

Click here to c...

▲ Multi-factor

▲ Access ke...

▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

[Continue to Security Credentials](#)

[Get Started with IAM Users](#)



Don't show me this message again

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- ▲ Password
- ▼ Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

[Activate MFA](#)

- ▲ Access keys (access key ID and secret access key)
- ▲ CloudFront key pairs
- ▲ X.509 certificate
- ▲ Account identifiers

Your Security

Use this page to manage th

To learn more about the typ

▲ Password

▼ Multi-factor authen

Use MFA to increase the

Activate MFA

▲ Access keys (acce

▲ CloudFront key pa

▲ X.509 certificate

▲ Account identifiers

Manage MFA device



Choose the type of MFA device to assign:

Virtual MFA device

Authenticator app installed on your mobile device or computer

U2F security key

⚠ Your browser does not support U2F. [Learn more](#)

YubiKey or any other compliant U2F device

Other hardware MFA device

Gemalto token

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)

Cancel

Continue

Set up virtual MFA device



1. Install a compatible app on your mobile device or computer

See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

590971

MFA code 2

137054

Cancel

Previous

Assign MFA

Your Security

Use this page to manage th

To learn more about the typ

▲ Password

▼ Multi-factor auth

Set up virtual MFA device



✓ You have successfully assigned virtual MFA

This virtual MFA will be required during sign-in.

Close

Use MFA to increase the security of your AWS environments. Signing in to IAM-protected accounts requires a user name, password, and an authentication code from an MFA device.

Device type	Serial number	Actions
Virtual	arn:aws:iam::060094927536:mfa/root-account-mfa-device	Manage

▲ Access keys (access key ID and secret access key)

▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers

AWS Management Console

IAM Resources

Users: 1

Roles: 26

Groups: 1

Identity Providers: 1

Customer Managed Policies: 3

Security Status

4 out of 4 complete

- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

 **AWS Cost Management**
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions

 **Mobile**
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

[Serverless Application Repository](#)

[Trusted Advisor](#)

Tagging Example

Section 4: Tagging

Compliance Score: 0.0%

1. Non-compliant Resources [SEC-OPS-ASTMGT-2]: (total = 31)

S3 Buckets: (total = 10)

1. [REDACTED] eu-west-1

2. [REDACTED] east-1

3. [REDACTED]

4. elasticbeanstalk-us-[REDACTED]

5. [REDACTED]

..... and 5 more

EC2 Instances: (total = 21)

1. [REDACTED] 8e8b (us-east-1)

2. [REDACTED] 6789 (ap-south-1)

3. [REDACTED] 9b3c (us-east-1)

4. [REDACTED] 05b3 (ap-south-1)

Section 4: Tagging

Compliance Score: 0.0%

1. Non-compliant Resources [SEC-OPS-ASTMGT-]

S3 Buckets: (total = 10)

- 1. [REDACTED] eu-west-1
 - 2. [REDACTED] east-1
 - 3. [REDACTED]
 - 4. elasticbeanstalk-us-[REDACTED]
 - 5. [REDACTED]

..... and 5 more

EC2 Instances: (total = 21)

1. [REDACTED]8e8b (us-east-1)
 2. [REDACTED]6789 (ap-south-1)
 3. [REDACTED]9b3c (us-east-1)
 4. [REDACTED]05b3 (ap-south-1)

Section 4: Tagging

Compliance Score: 0.0%

1. Non-compliant Resources [SEC-OPS-ASTMGT-]

EC2 Instances: (total = 21)

1. [REDACTED]8e8b (us-east-1)
 2. [REDACTED]6789 (ap-south-1)
 3. [REDACTED]9b3c (us-east-1)
 4. [REDACTED]05b3 (ap-south-1)

Section 4: Tagging

1. Non-compliant Resource

S3 Buckets: (total = 1)

- 1 [REDACTED]
 - 2 [REDACTED]
 - 3 [REDACTED]
 4. elasticbeanstalk
 - 5 [REDACTED]

..... and 5 more

EC2 Instances: (total : 1)

1. [REDACTED]
 2. [REDACTED]
 3. [REDACTED]
 4. [REDACTED]

Compliance Score: 0.0%

Compliance Score: 0.0%

Section 4: Tagging

1. Non-compliant Resource

S3 Buckets: (total = 10)

```
bparriot@ubuntu:~/csb_tenant/csb/src/aws/scripts/resource_tagging$ python ./tagResources.py
Processing Sheet and validating Tags ...
No file errors found
Setting up default values ...
write to AWS
Creating Resource Tags ...
Creating TagSet ...
Added Tags for S3 Bucket:
Creating TagSet ...
Added Tags for S3 Bucket:
Creating TagSet ...

Creating TagSet ...
Added Tags for EC2 Instance:
```

RESOURCE NAME (RESOURCE TYPE)	RESOURCE TAG (KEY)	RESOURCE TAG (VALUE)
DEFAULT RESOURCE (DEFAULT TYPE)	DataClassification	NONE
	Environment	NONE
	ApplicationName	NONE
	ResourceOwner	NONE
	CiscoMailAlias	NONE
	DataTaxonomy	NONE

1. [REDACTED]	Environment	Sandbox
2. [REDACTED]	DataClassification	Cisco Highly Confidential
3. [REDACTED]	DataTaxonomy	DEFAULT
4. [REDACTED]	ResourceOwner	bparriot

1. [REDACTED]	ApplicationName	DEFAULT
2. [REDACTED]	Environment	DEFAULT
3. [REDACTED]	DataClassification	DEFAULT
4. [REDACTED]	DataTaxonomy	DEFAULT
5. [REDACTED]	CiscoMailAlias	DEFAULT
6. [REDACTED]	ResourceOwner	DEFAULT

Report Post-Remediation

Daily Reporting

AWS Security Health Report
(Continuous Security Buddy)
Report Date: February 21, 2019

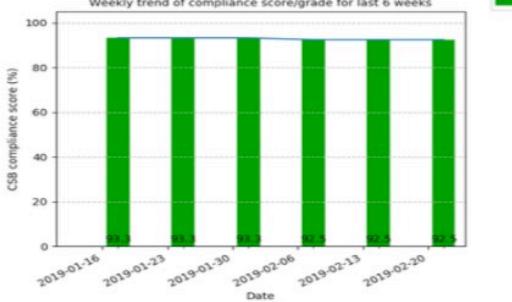
Summary

Tenant CSB Report for Account # [REDACTED]
Tenant CSB Account Details: CSB
Tenant Account Environment: Sandbox
Tenant CSB Contacts: [REDACTED]@cisco.com

Overall Compliance Score: 92.5%
Compliance Grade: A

Key Compliance Failure Areas:
1. Resources without proper tagging [SEC-OPS-ASTMGT-2]

Weekly trend of Compliance Score/Grade



CSB compliance score (%)

CSB compliance score (A)

Date: 2019-01-16, 2019-01-23, 2019-01-30, 2019-02-06, 2019-02-13, 2019-02-20

Section 1: Identity and Access Management Compliance Score: 100.0%

- 1. IAM users without MFA enabled [SEC-CRE-MULTIFAC]: [None]
- 2. MFA enabled on Root user? [SEC-CRE-MULTIFAC]: Yes
- 3. MFA Compliance [SEC-CRE-MULTIFAC] (1/1): 100.0%
- 4. Access Key Rotation Violation (current 2+ years) [SEC-OPS-REVOKE]: [None]
- 5. Cisco SSO Enabled? [SEC-CRE-SSO]: Yes

Overall Risk Score:



Security Metrics

Section

1. Identity and Access Management
2. Network Security
3. Storage (S3 buckets)
4. Tagging
5. External Vulnerabilities
6. CIS AWS Benchmarks
7. Trusted Advisor Checks

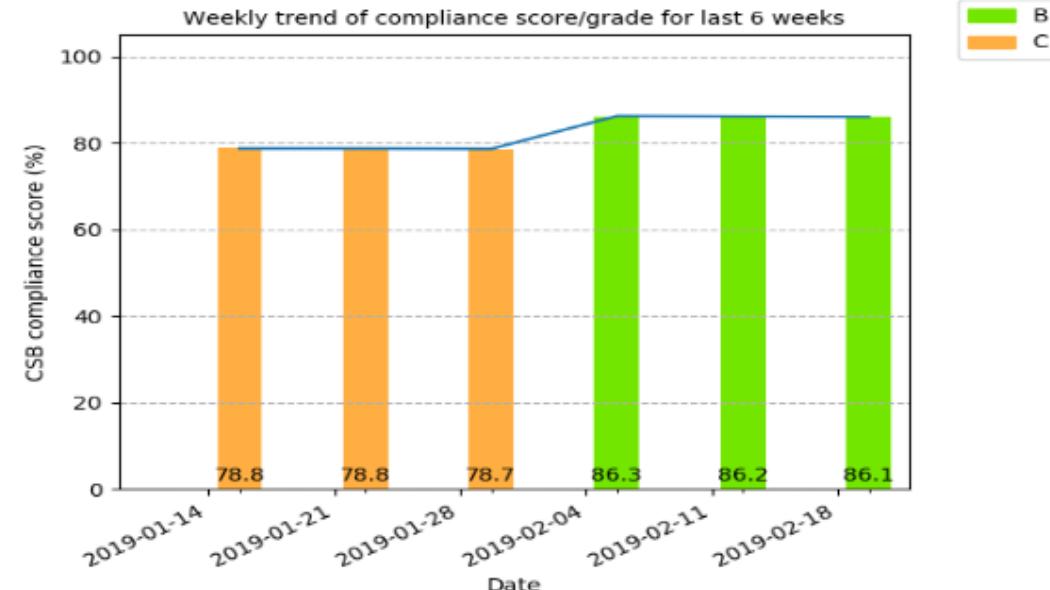
Section Score

- 100/100
- 80/100
- 100/100
- 90/100
- 100/100
- 100/100
- Not Scored

Benefits of CSIRT Integration with CSB

- Enables CSIRT monitoring for each tenant at the:
 - IaaS/platform level
 - NetFlow/VPC Flow level
 - VM/OS level
- Daily CSB reports encourage tenants to improve their scores, reduce their risk of compromise
- When security incidents do occur, CSB provides CSIRT with:
 - Ability to track down owners of Cisco's cloud tenants quickly
 - Quick view into known tenant security gaps
 - Investigator capability in tenant environment
 - Simplifies incident reporting automation
- MTTD improved by automated play runs and case creation
- MTTC improved by automated tenant attribution

Weekly trend of Compliance Score/Grade



Good Security Posture Requires Continuous Security Monitoring

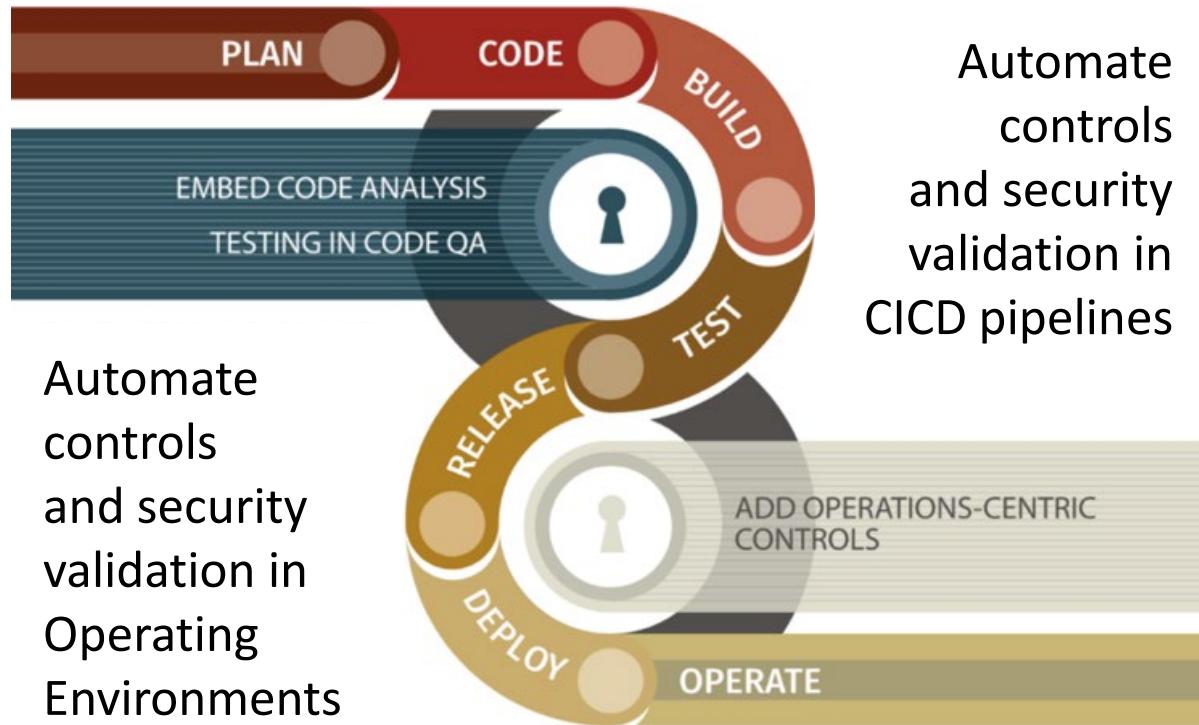
- *March/April 2018:* Tenant installs CSB, CSB reports many security best practice violations
- *April 2018:* Tenant has a case for EC2 instances compromised
- *May 2018:* Bad security behavior continues, tenant has another case for EC2 instance compromised
- *June 2018:* Some improvement in security posture but not enough; another EC2 instance pwned
- *July-Present:* Up and down case trend continues, tenant still needs work on security posture

XaaS Offering ABC With 11 AWS Accounts



DevSecOps: Results

Delivered Continuous Security Buddy (CSB)



Speed: Consistently Implementing Security in Cloud Tenants

3 Weeks -> 4 hours

Scale: Adoption Rate

Offers with CSB

35% at 3 months
72% in 9 months
89% <12 months

Value: Issues Identified and Remediated via Automation

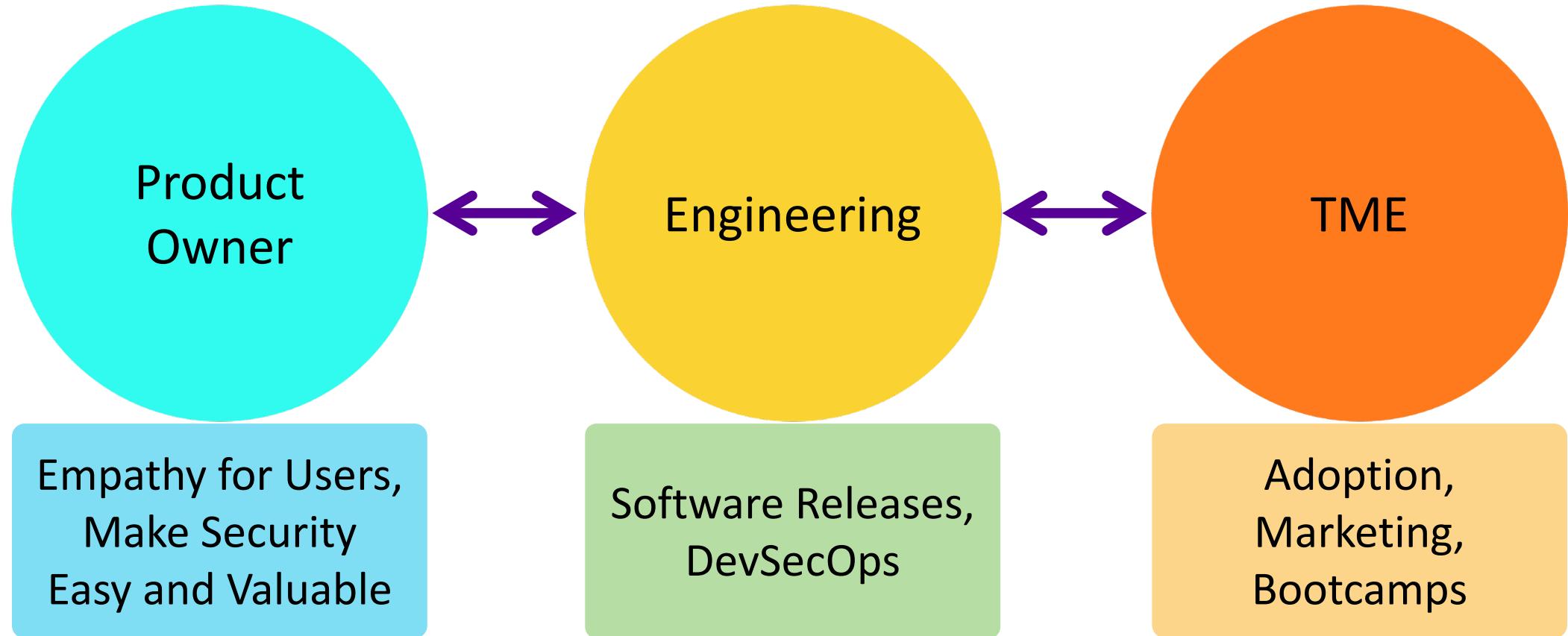
97% of Cisco Cloud Service Offerings have on average 'A' or 'B' Security Report Grade

RSA® Conference 2019

Cultural Effect



Operating as a Product Team



Better Together

Collaboration with Engineering Business Units

"I easily saved 40 hours during each CATO project associated to defining what was wrong and how to fix it. This along with internal lessons learned is what enabled me to shave a full month off the second CATO effort."

~ Software Engineer

InfoSec Operations Effectiveness

"CSB was instrumental in investigating a customer-impacting incident. Had the team done one of the top 3 CSB findings, the incident could have been avoided."

~ CSIRT Manager

Success Criteria



Time to Value

RSA® Conference 2019

Next Steps



Progress

Rinse and repeat with other cloud platforms

Move up the stack

Integrating in to CI/CD pipelines

Programmable Network access policies based on Posture

Infosec DevSecOps team as Customer Zero



RSA® Conference 2019

Lessons Learned



Key Takeaways

Start on this journey... don't wait!

Everything is code

Collaborative Approach: Dev + Sec + Ops

Only way to achieve speed and scale

Get a win and keep going

Learn More



DevSecOps: Win-Win for All

<https://blogs.cisco.com/security/devsecops-win-win-for-all>



DevSecOps: Security at the Speed of Business

<https://blogs.cisco.com/security/devsecops-security-at-the-speed-of-business>



DevSecOps: Automation for Assurance

<https://blogs.cisco.com/security/devsecops-automation-for-assurance>



DevSecOps: Lessons Learned

<https://blogs.cisco.com/security/devsecops-lessons-learned>

Apply What You Have Learned Today

- Next week:
 - Identify where to start your DevSecOps Practice
- Within 3 months:
 - Prioritize use-cases and hold a Hackathon
 - Publish Security Guardrails
- Within 6 months:
 - Automate few of the Guardrails (MVP)
 - Embed automation in the appropriate systems to drive adoption
 - Start a feedback loop with users and iterate

RSA® Conference 2019

Thank you!

@CiscoSecurity

trust.cisco.com

