SRV308

Securing Serverless Applications

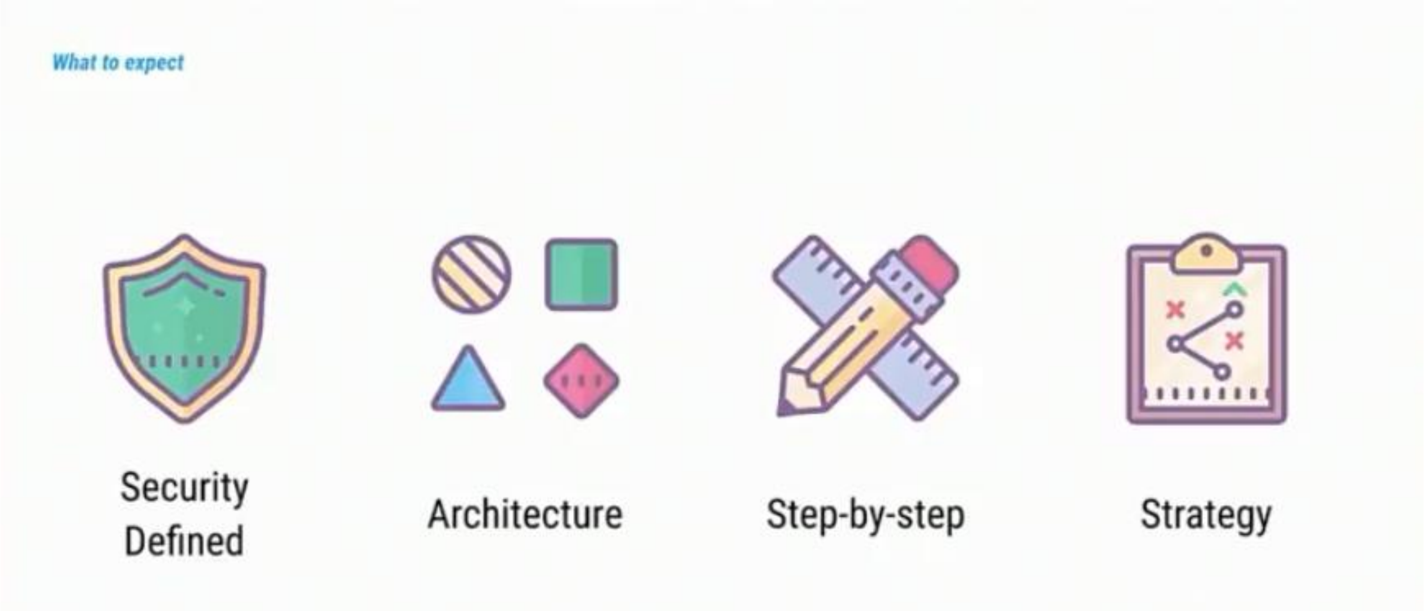
Step-by-step

Mark Nunnikhoven

Vice President, Cloud Research, Trend Micro

AWS re:Invent

aws



What to expect

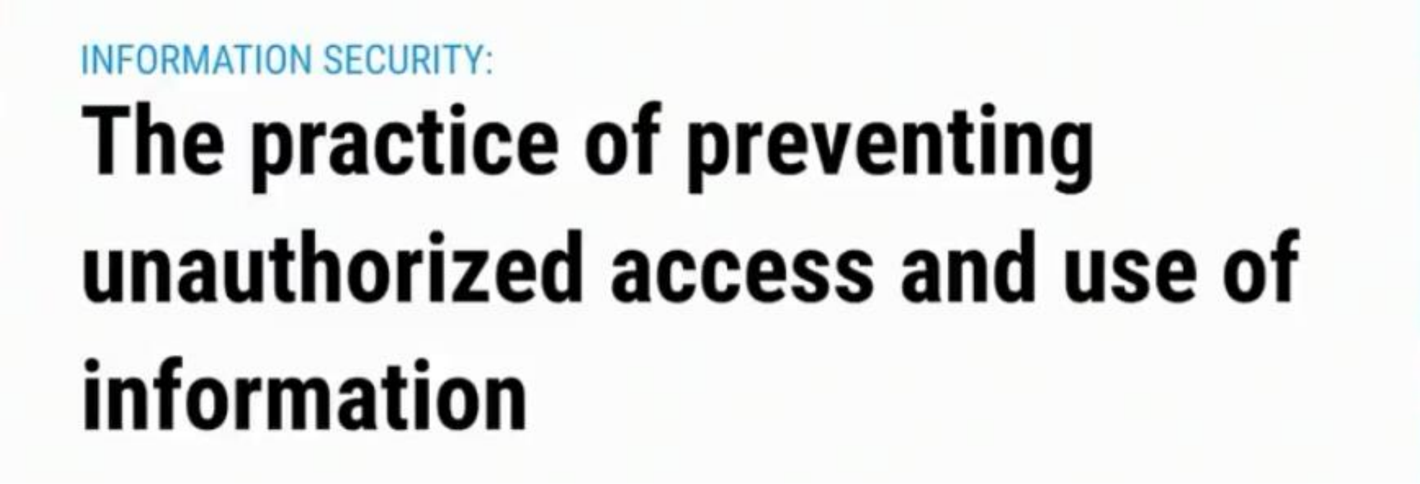
Security Defined

Architecture

Step-by-step

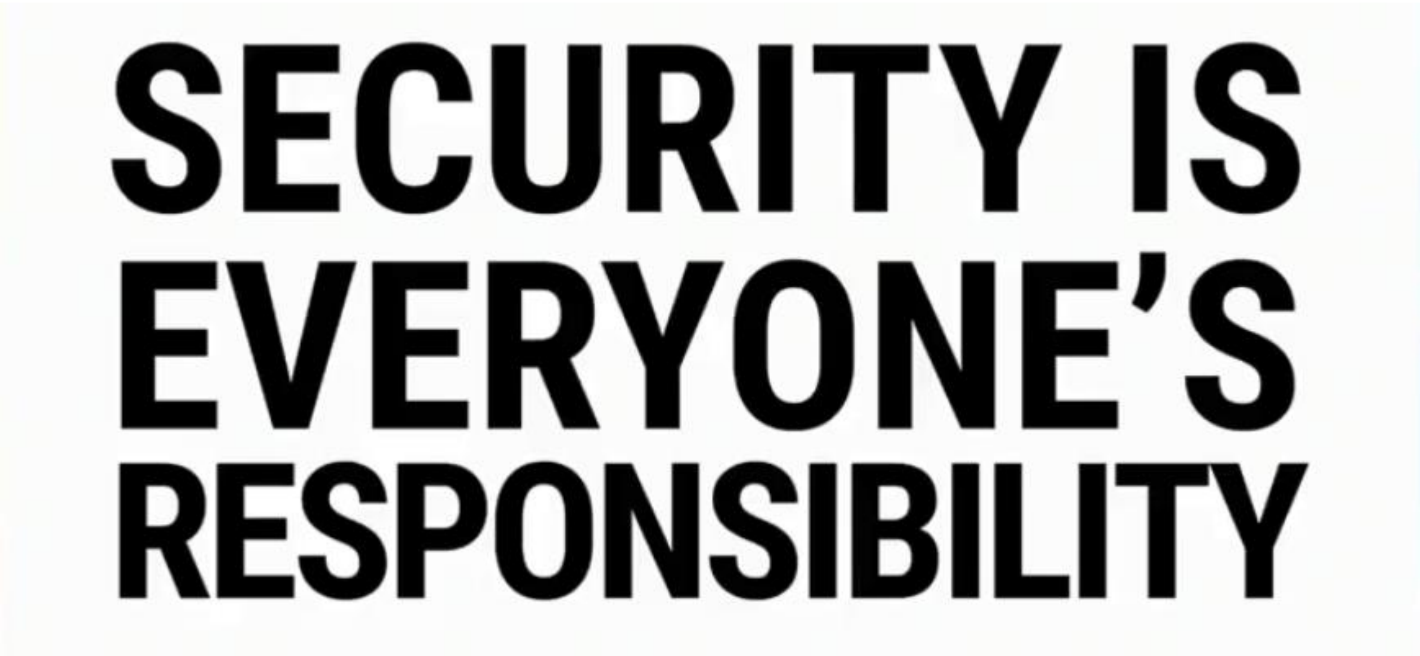
Strategy

Security Defined

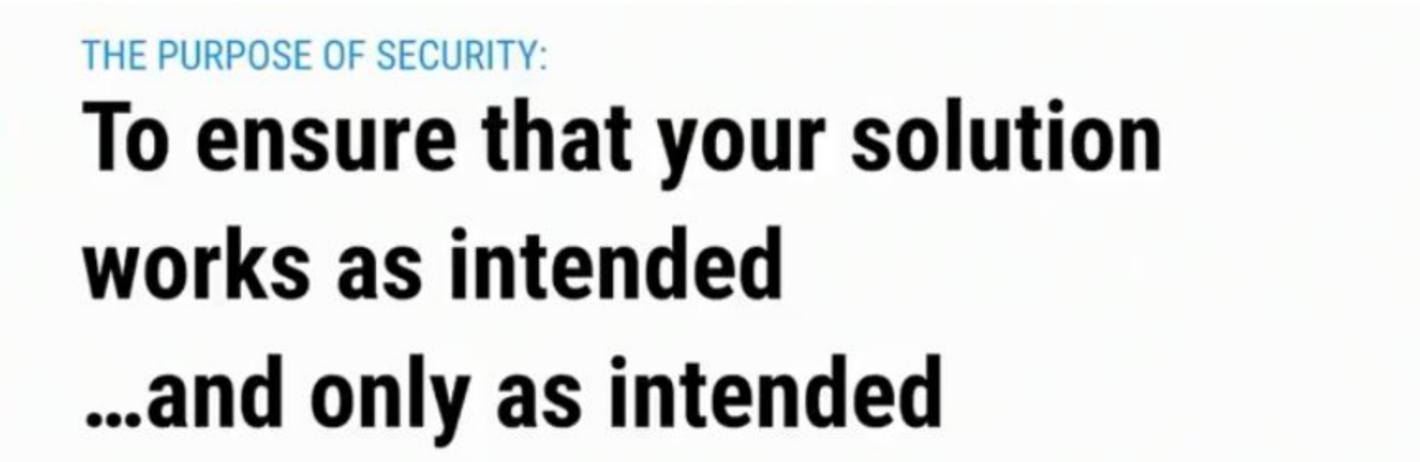


INFORMATION SECURITY:

The practice of preventing unauthorized access and use of information



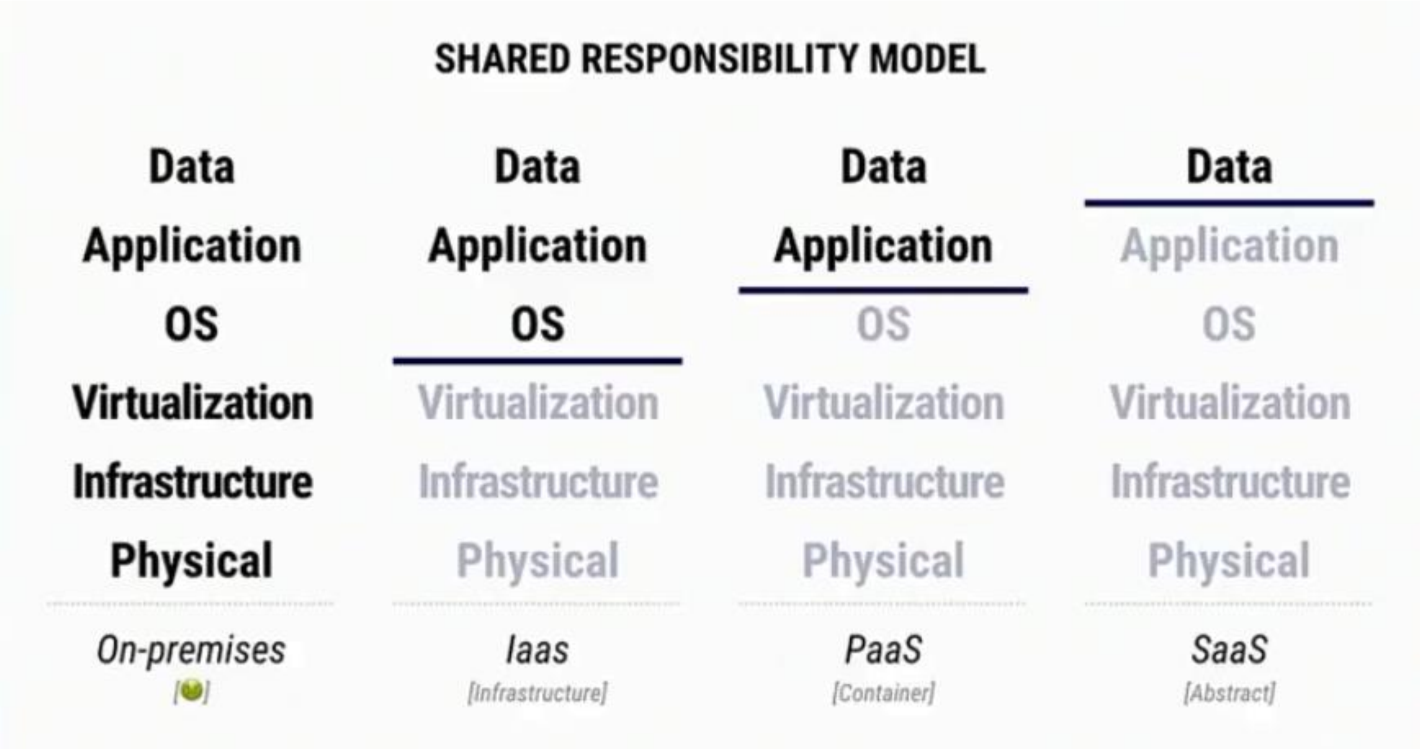
SECURITY IS EVERYONE'S RESPONSIBILITY



THE PURPOSE OF SECURITY:

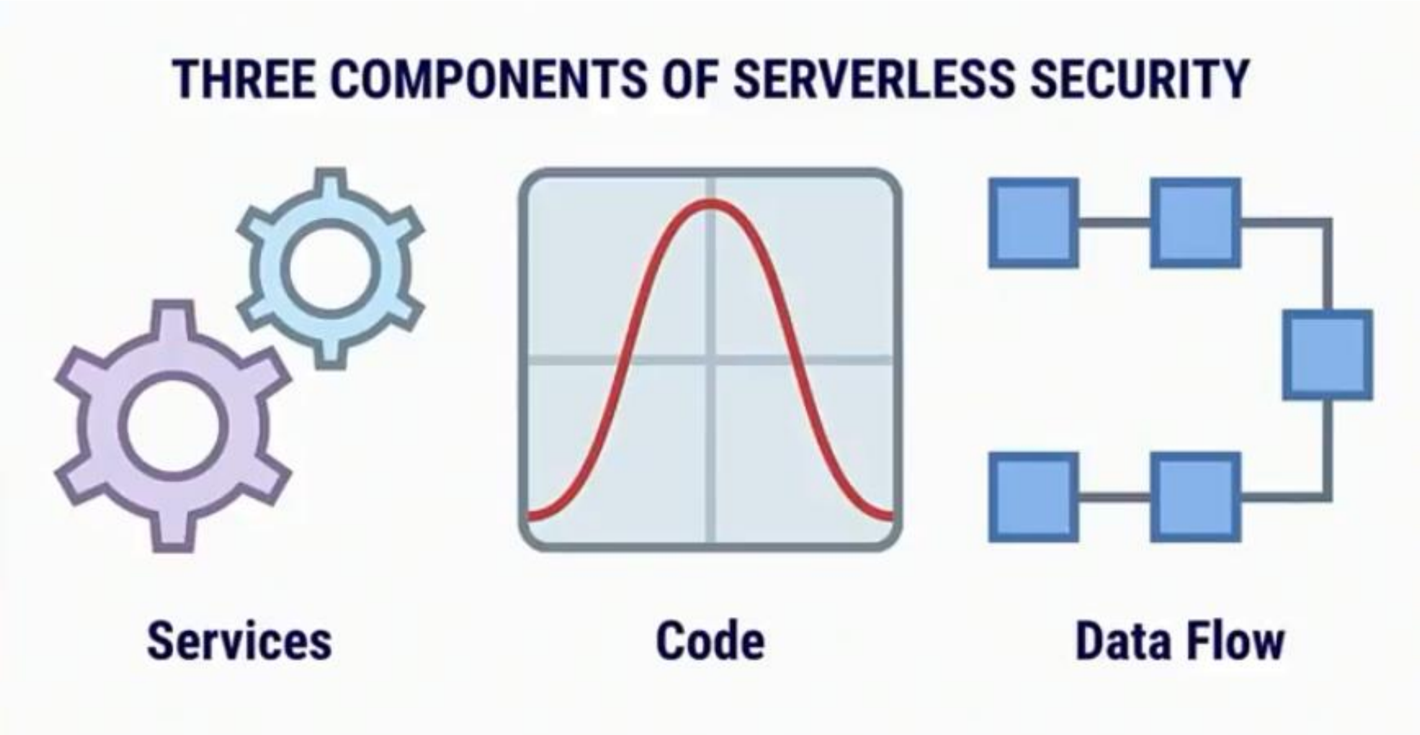
To ensure that your solution works as intended

...and only as intended



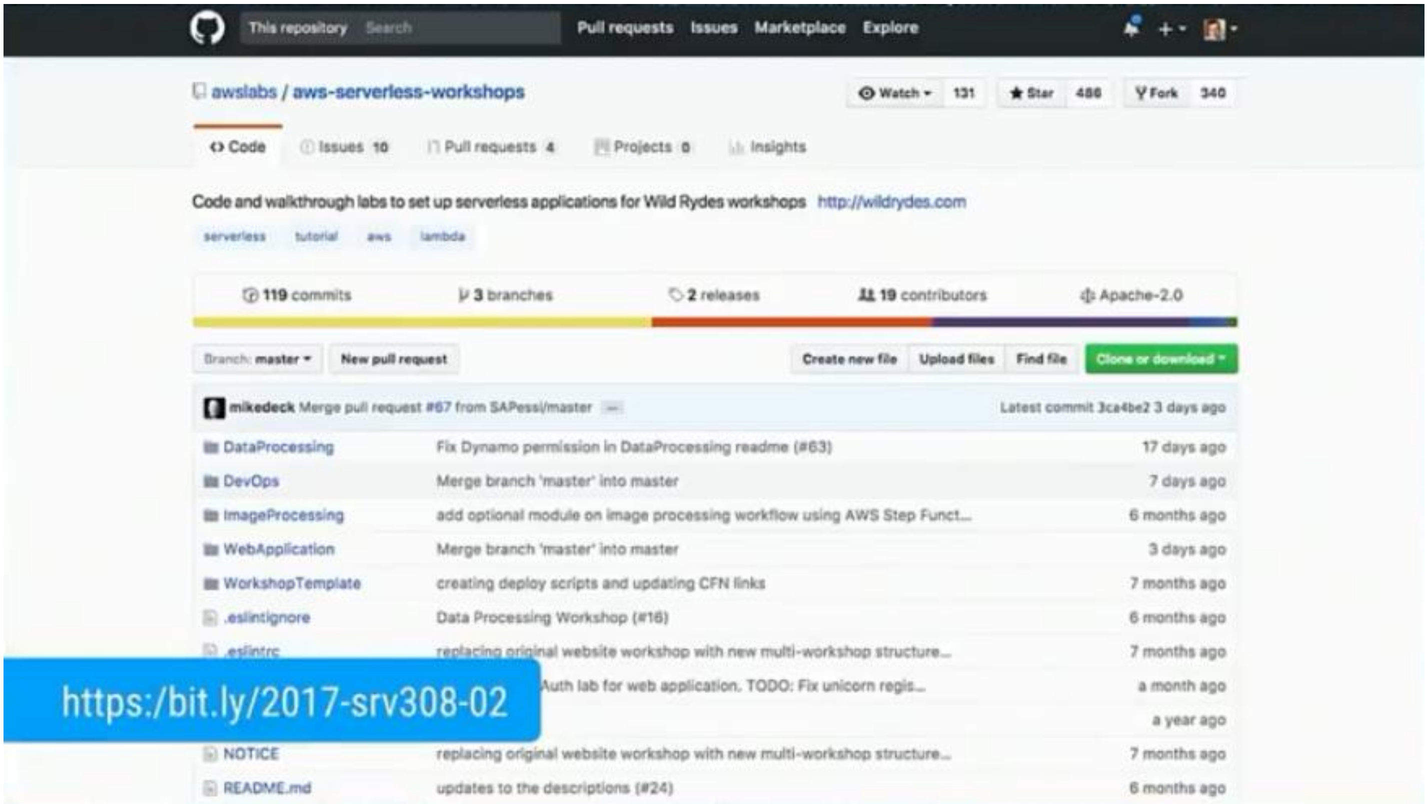
SHARED RESPONSIBILITY MODEL

Data	Data	Data	Data
Application	Application	Application	Application
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical
On-premises	*Iaas*	*PaaS*	*SaaS*
[●]	*[Infrastructure]*	*[Container]*	*[Abstract]*



THREE COMPONENTS OF SERVERLESS SECURITY

https:/bit.ly/2017-srv308-01



awslabs / aws-serverless-workshops

Code and walkthrough labs to set up serverless applications for Wild Rydes workshops http://wildrydes.com

serverless tutorial aws lambda

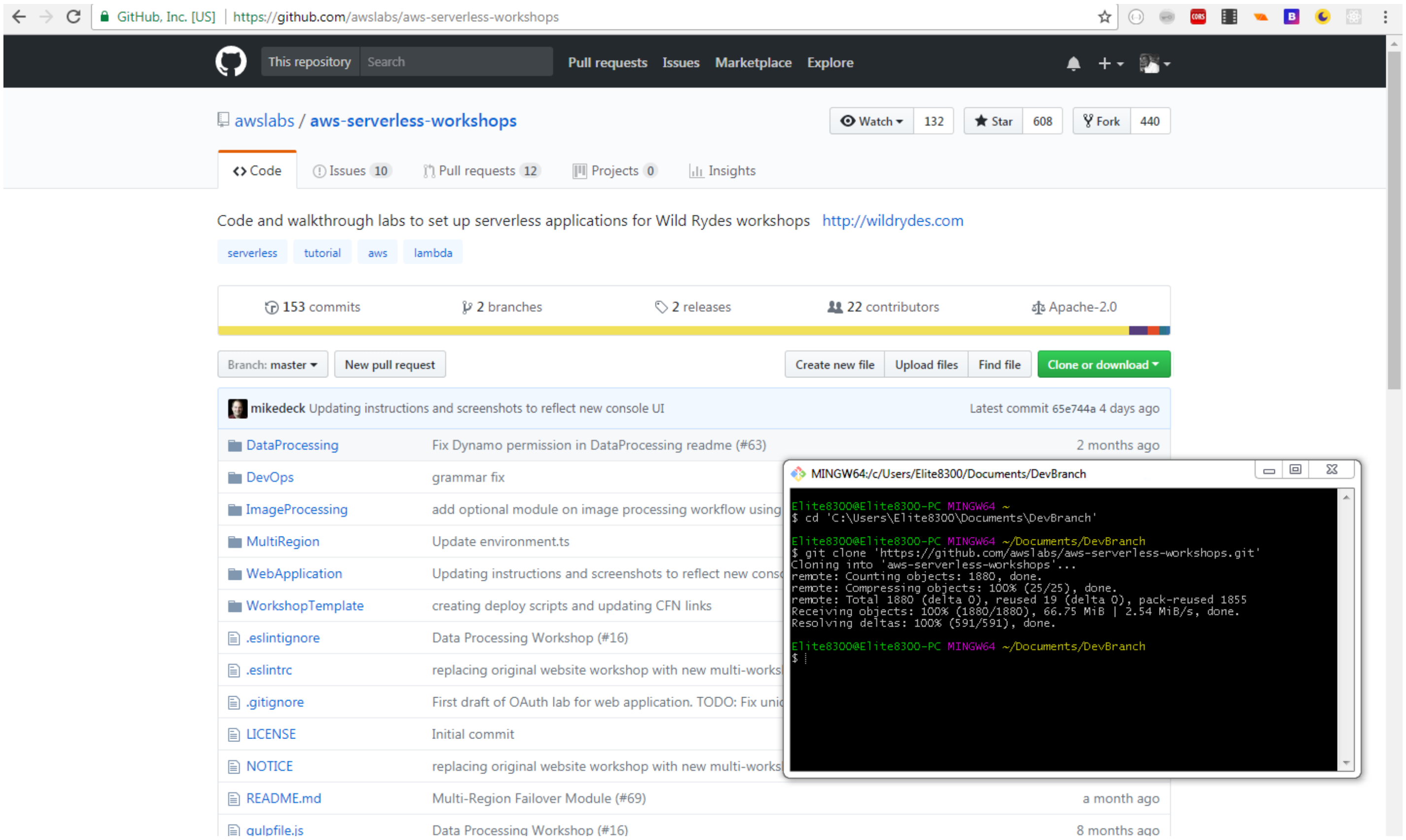
119 commits · 3 branches · 2 releases · 19 contributors · Apache-2.0

mikedeck Merge pull request #67 from SAPessi/master … Latest commit 3ca4be2 3 days ago

DataProcessing	Fix Dynamo permission in DataProcessing readme (#63)	17 days ago
DevOps	Merge branch 'master' into master	7 days ago
ImageProcessing	add optional module on image processing workflow using AWS Step Funct…	6 months ago
WebApplication	Merge branch 'master' into master	3 days ago
WorkshopTemplate	creating deploy scripts and updating CFN links	7 months ago
.eslintignore	Data Processing Workshop (#16)	6 months ago
.eslintrc	replacing original website workshop with new multi-workshop structure…	7 months ago
	Auth lab for web application. TODO: Fix unicorn regis…	a month ago
		a year ago
NOTICE	replacing original website workshop with new multi-workshop structure…	7 months ago
README.md	updates to the descriptions (#24)	6 months ago

https:/bit.ly/2017-srv308-02

The code for this session is available at the following aws-labs link



GitHub, Inc. [US] | https://github.com/awslabs/aws-serverless-workshops

awslabs / aws-serverless-workshops

Code and walkthrough labs to set up serverless applications for Wild Rydes workshops http://wildrydes.com

serverless tutorial aws lambda

153 commits | 2 branches | 2 releases | 22 contributors | Apache-2.0

mikedeck Updating instructions and screenshots to reflect new console UI — Latest commit 65e744a 4 days ago

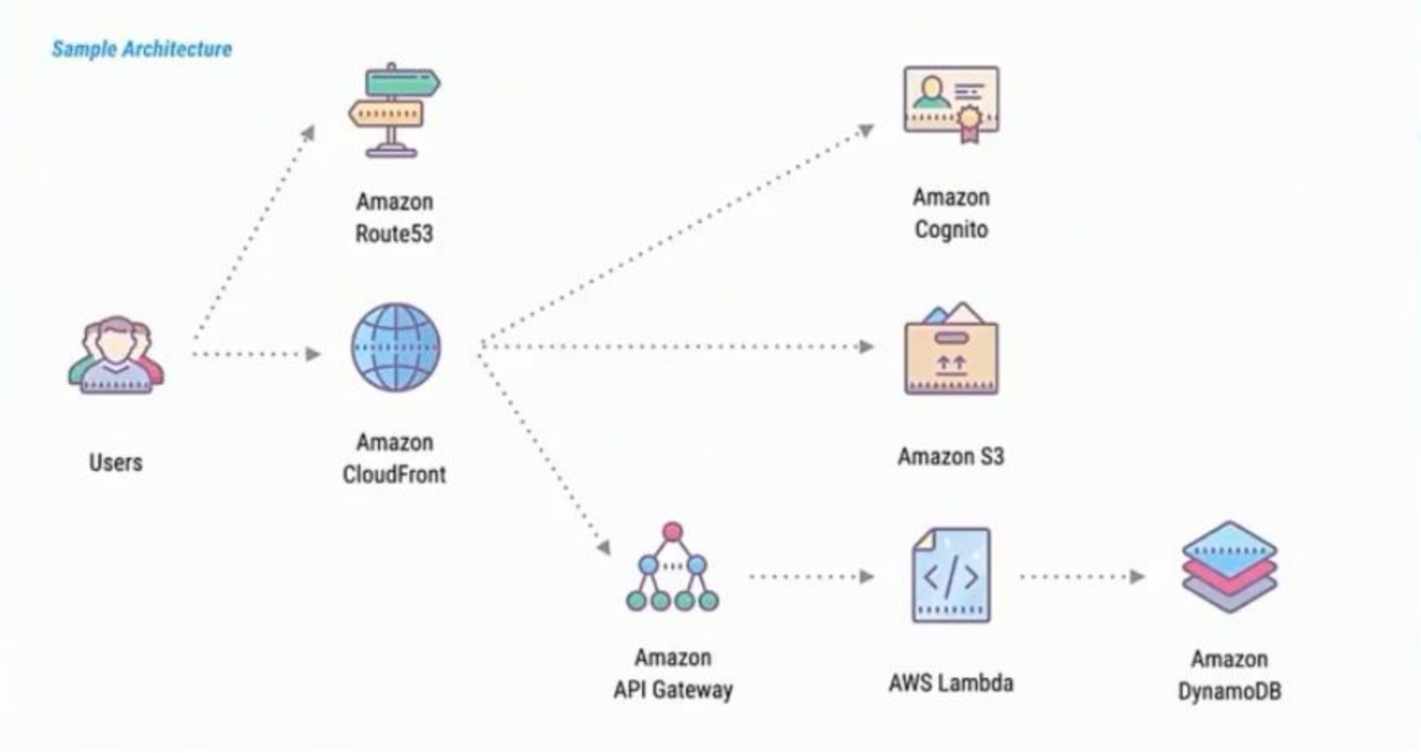
DataProcessing	Fix Dynamo permission in DataProcessing readme (#63)	2 months ago
DevOps	grammar fix	
ImageProcessing	add optional module on image processing workflow using	
MultiRegion	Update environment.ts	
WebApplication	Updating instructions and screenshots to reflect new cons	
WorkshopTemplate	creating deploy scripts and updating CFN links	
.eslintignore	Data Processing Workshop (#16)	
.eslintrc	replacing original website workshop with new multi-works	
.gitignore	First draft of OAuth lab for web application. TODO: Fix uni	
LICENSE	Initial commit	
NOTICE	replacing original website workshop with new multi-works	
README.md	Multi-Region Failover Module (#69)	a month ago
gulpfile.js	Data Processing Workshop (#16)	8 months ago

MINGW64:/c/Users/Elite8300/Documents/DevBranch

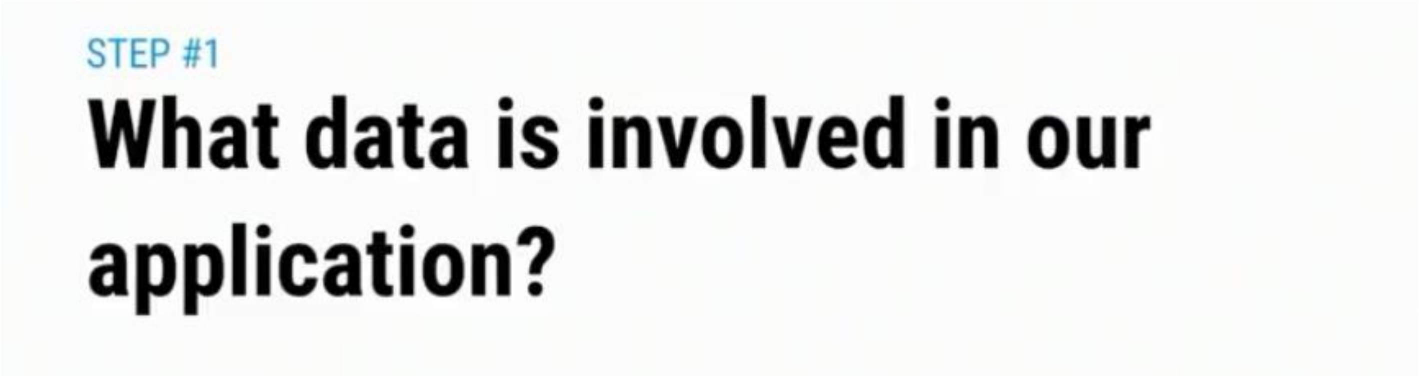
```
Elite8300@Elite8300-PC MINGW64 ~
$ cd 'C:\Users\Elite8300\Documents\DevBranch'

Elite8300@Elite8300-PC MINGW64 ~/Documents/DevBranch
$ git clone 'https://github.com/awslabs/aws-serverless-workshops.git'
Cloning into 'aws-serverless-workshops'...
remote: Counting objects: 1880, done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 1880 (delta 0), reused 19 (delta 0), pack-reused 1855
Receiving objects: 100% (1880/1880), 66.75 MiB | 2.54 MiB/s, done.
Resolving deltas: 100% (591/591), done.

Elite8300@Elite8300-PC MINGW64 ~/Documents/DevBranch
$
```

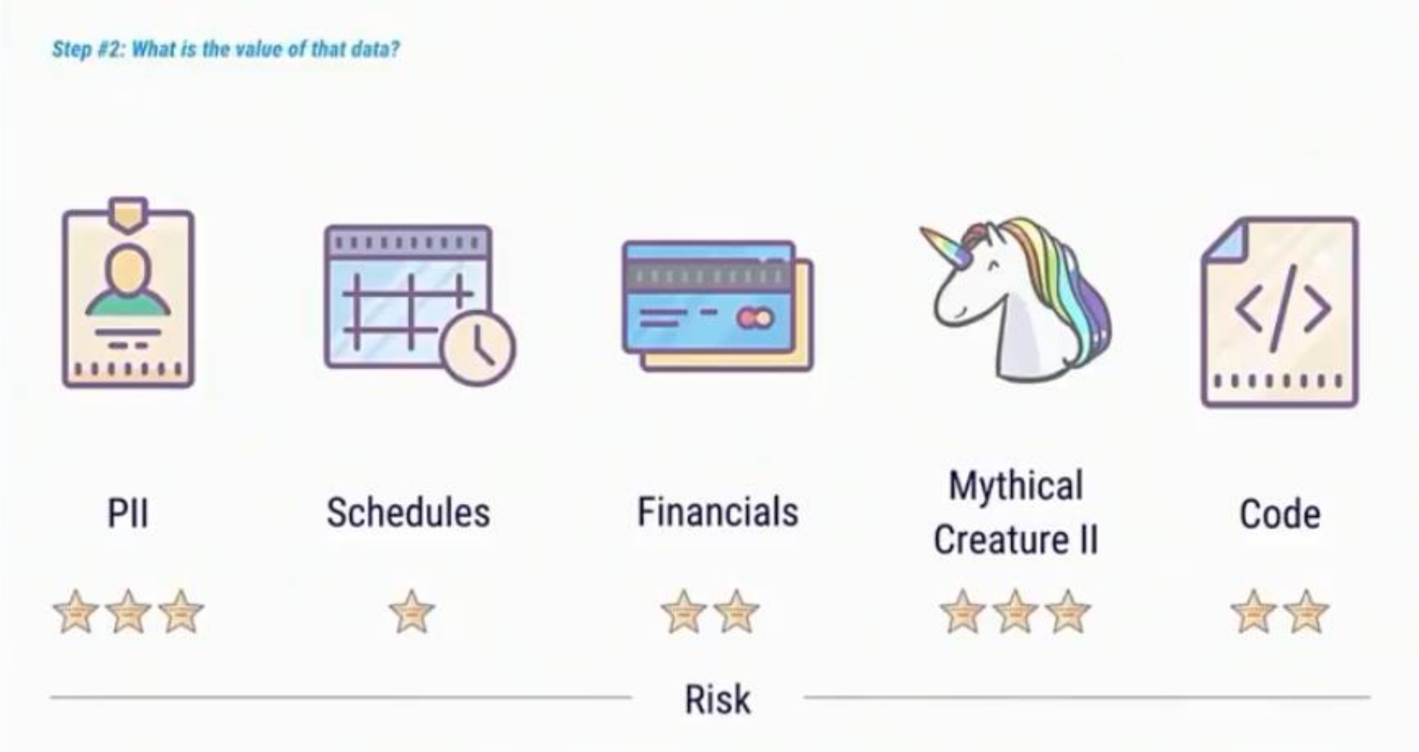


We are going to walk through this design and apply security features that will ensure that the app does only what we want it to do.



STEP #1

What data is involved in our application?



Step #2: What is the value of that data?

PII ★★★

Schedules ★

Financials ★★

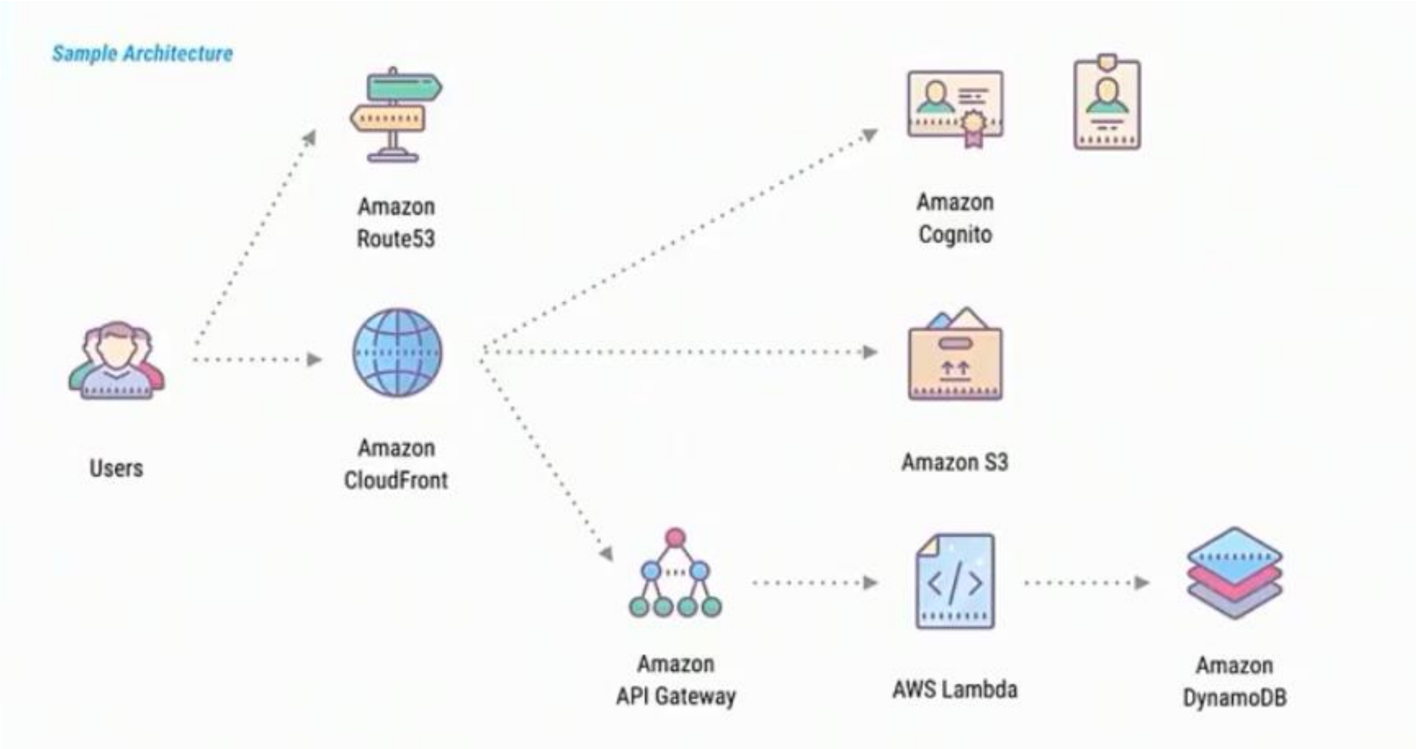
Mythical Creature II ★★★

Code ★★

Risk

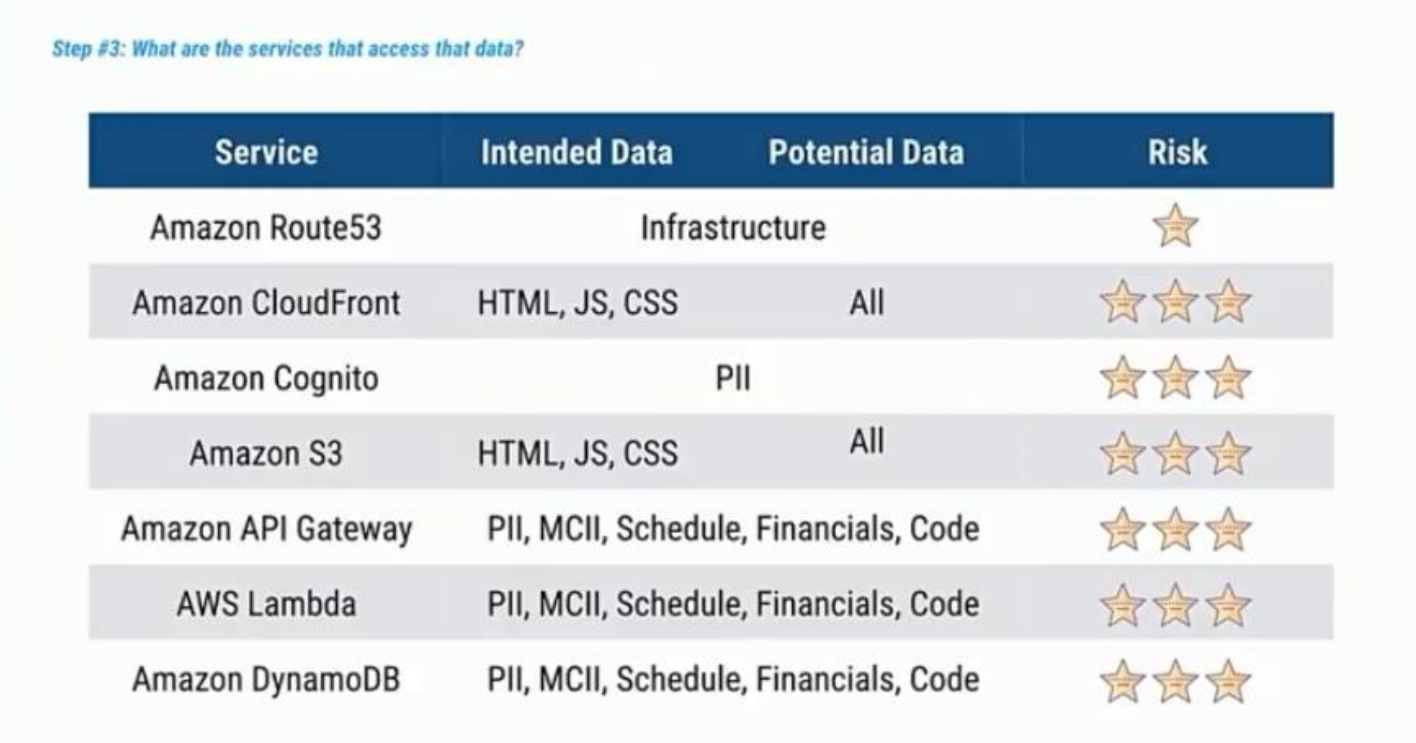
We can expose the scheduling data since it is not critical

Services



Sample Architecture

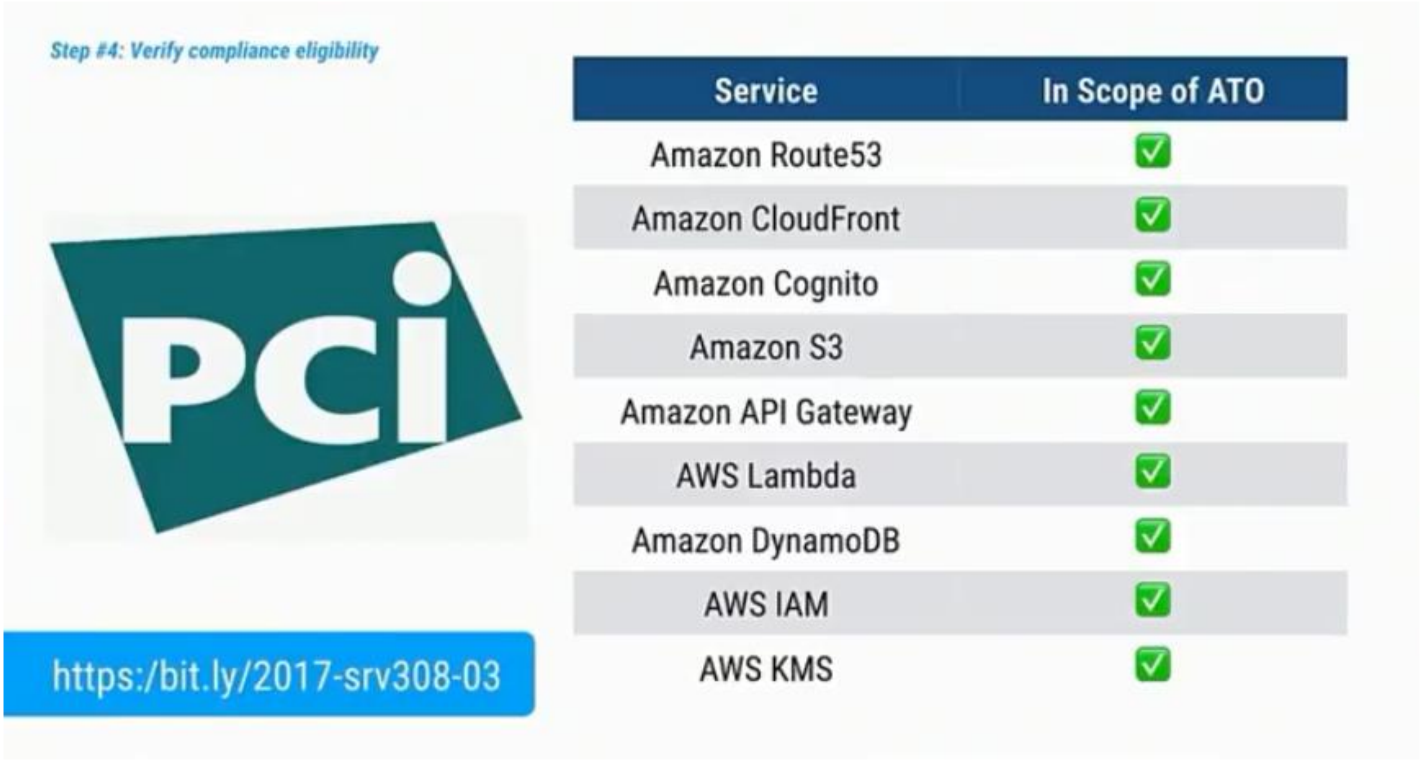
We can now go through each of these services to see how we can configure them to match our data security concerns



Step #3: What are the services that access that data?

Service	Intended Data	Potential Data	Risk
Amazon Route53	Infrastructure		☆
Amazon CloudFront	HTML, JS, CSS	All	☆☆☆
Amazon Cognito	PII		☆☆☆
Amazon S3	HTML, JS, CSS	All	☆☆☆
Amazon API Gateway	PII, MCII, Schedule, Financials, Code		☆☆☆
AWS Lambda	PII, MCII, Schedule, Financials, Code		☆☆☆
Amazon DynamoDB	PII, MCII, Schedule, Financials, Code		☆☆☆

What are the services that touch what piece of data? ***CloudFront*** is our cache and should only have our content code/data in it, HTML, JS and CSS only, it also has the potential to store sensitive data if our code is not secure enough. We need to put some mitigations and gates in place to prevent this.

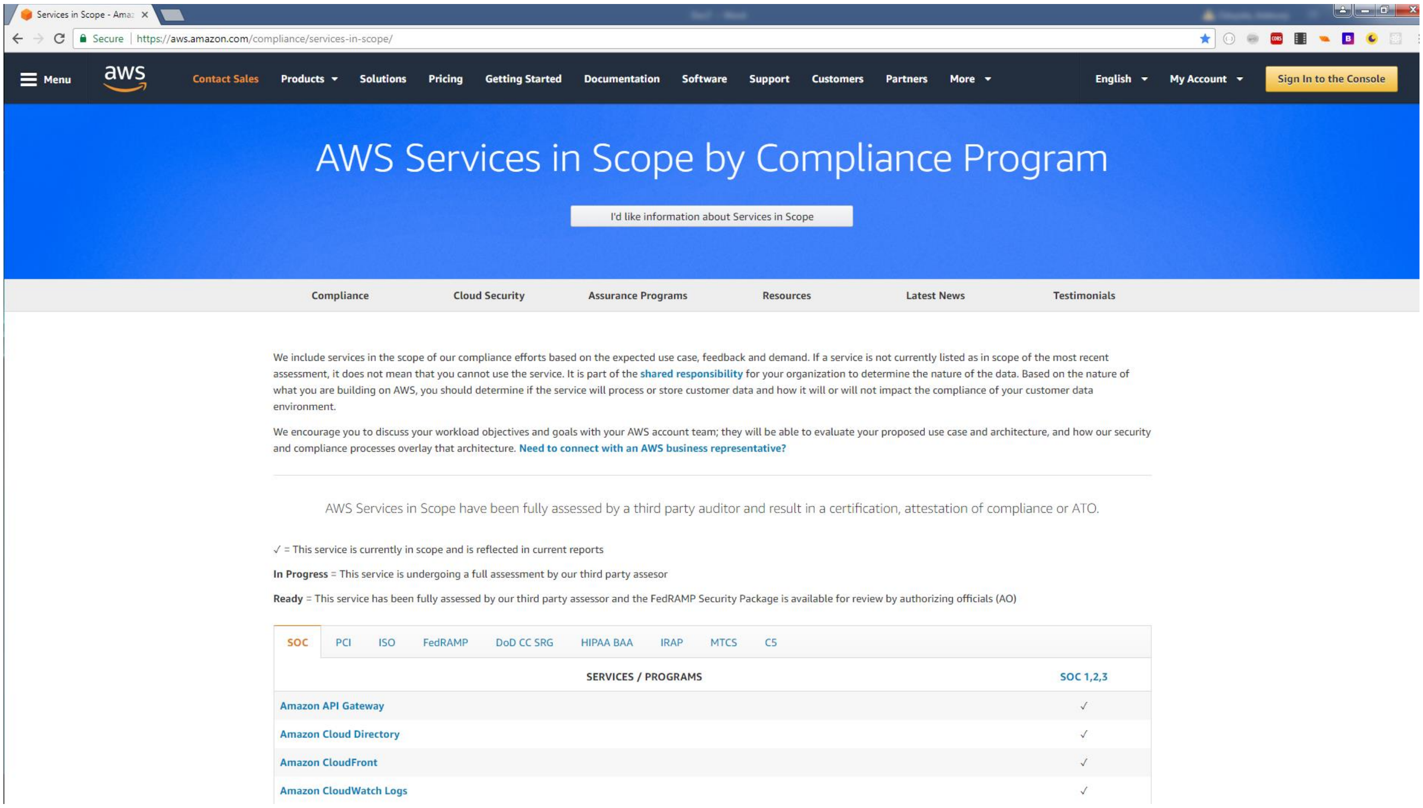


Step #4: Verify compliance eligibility

Service	In Scope of ATO
Amazon Route53	✓
Amazon CloudFront	✓
Amazon Cognito	✓
Amazon S3	✓
Amazon API Gateway	✓
AWS Lambda	✓
Amazon DynamoDB	✓
AWS IAM	✓
AWS KMS	✓

https:/bit.ly/2017-srv308-03

https://aws.amazon.com/compliance/services-in-scope/



AWS Services in Scope by Compliance Program

We include services in the scope of our compliance efforts based on the expected use case, feedback and demand. If a service is not currently listed as in scope of the most recent assessment, it does not mean that you cannot use the service. It is part of the shared responsibility for your organization to determine the nature of the data. Based on the nature of what you are building on AWS, you should determine if the service will process or store customer data and how it will or will not impact the compliance of your customer data environment.

We encourage you to discuss your workload objectives and goals with your AWS account team; they will be able to evaluate your proposed use case and architecture, and how our security and compliance processes overlay that architecture. Need to connect with an AWS business representative?

AWS Services in Scope have been fully assessed by a third party auditor and result in a certification, attestation of compliance or ATO.

✓ = This service is currently in scope and is reflected in current reports

In Progress = This service is undergoing a full assessment by our third party assesor

Ready = This service has been fully assessed by our third party assessor and the FedRAMP Security Package is available for review by authorizing officials (AO)

SERVICES / PROGRAMS	SOC 1,2,3
Amazon API Gateway	✓
Amazon Cloud Directory	✓
Amazon CloudFront	✓
Amazon CloudWatch Logs	✓

Payment Cards Industry PCI compliance is required since we are accepting credit cards for our rides. All the AWS services we are using are all certified to accept PCI data.

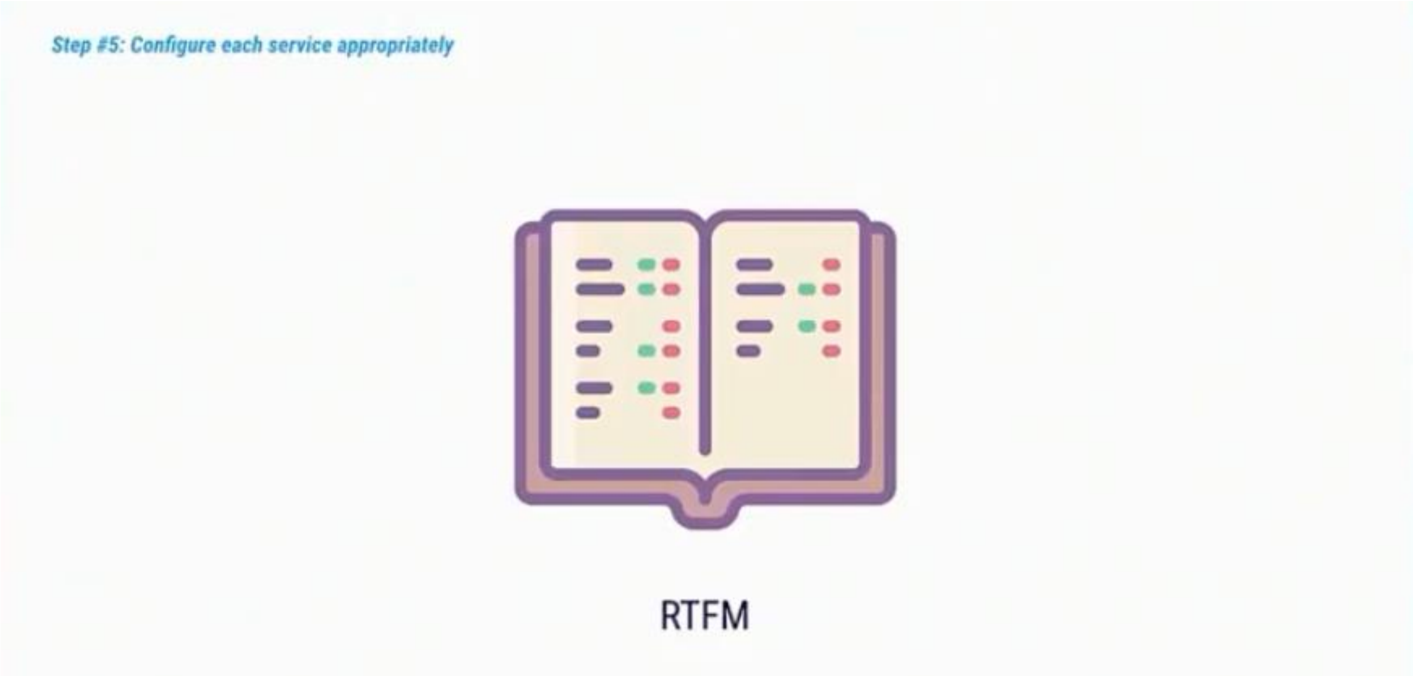
Amazon Web Services – Overview of Security Processes

Amazon Web Services: Overview of Security Processes

August 2016

https:/bit.ly/2017-srv308-04

(Please consult **http://aws.amazon.com/security/** for the latest version of this paper)



Step #5: Configure each service appropriately

RTFM

You need to read up on each service so that we know what access we have. S3 bucket creation is secured and locked down to only the specific user that created the bucket, you have to take explicit actions to make the bucket public. We need to know how to configure each service appropriately. IAM also denys all access by default, you need to allow access using specific IAM policies.

Step #6: Add tests for service configuration to CI/CD & PROD

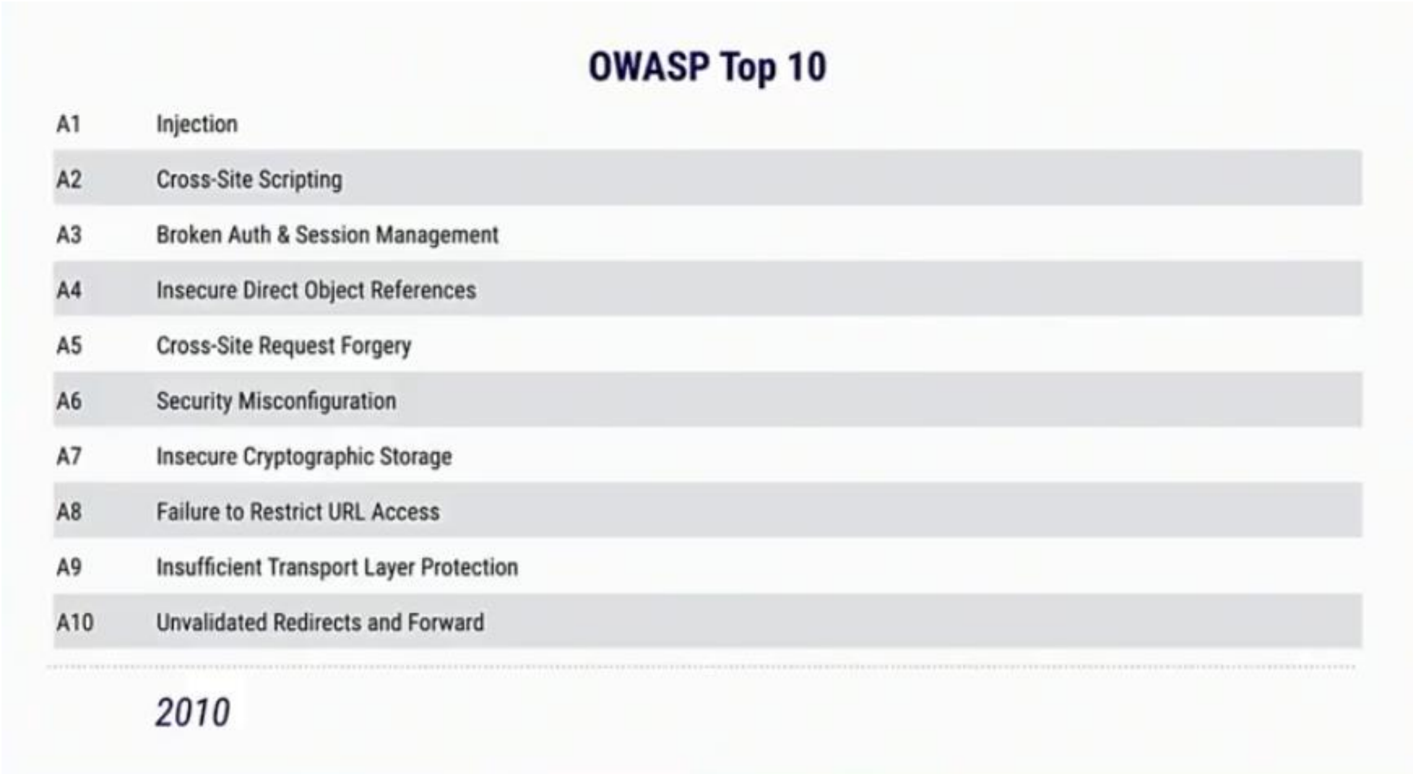
Test

You need to continue to test that what you intended to happen actually is true, you can set up lambdas to test our services.

Code

Ugh...

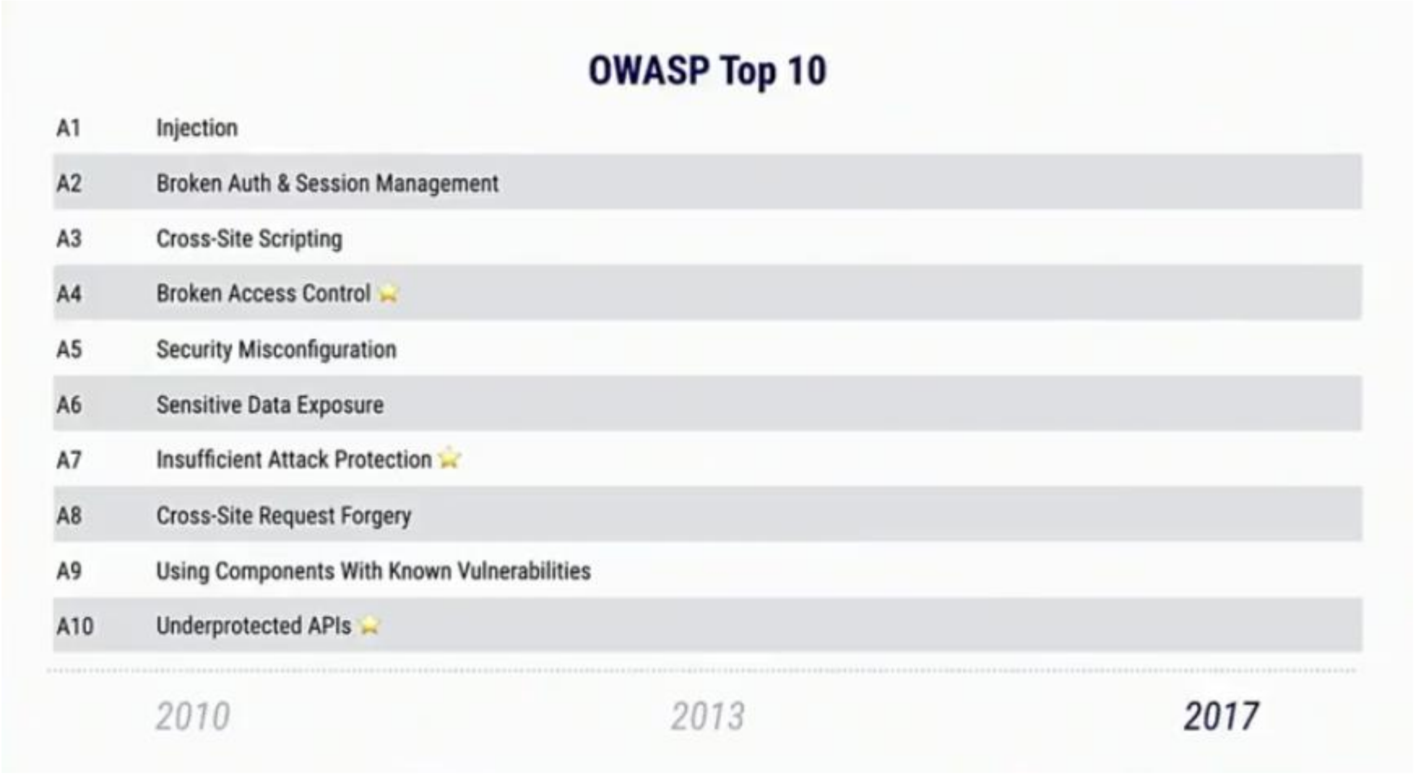
Code quality is ~~a~~ the problem



OWASP Top 10

A1	Injection
A2	Cross-Site Scripting
A3	Broken Auth & Session Management
A4	Insecure Direct Object References
A5	Cross-Site Request Forgery
A6	Security Misconfiguration
A7	Insecure Cryptographic Storage
A8	Failure to Restrict URL Access
A9	Insufficient Transport Layer Protection
A10	Unvalidated Redirects and Forward

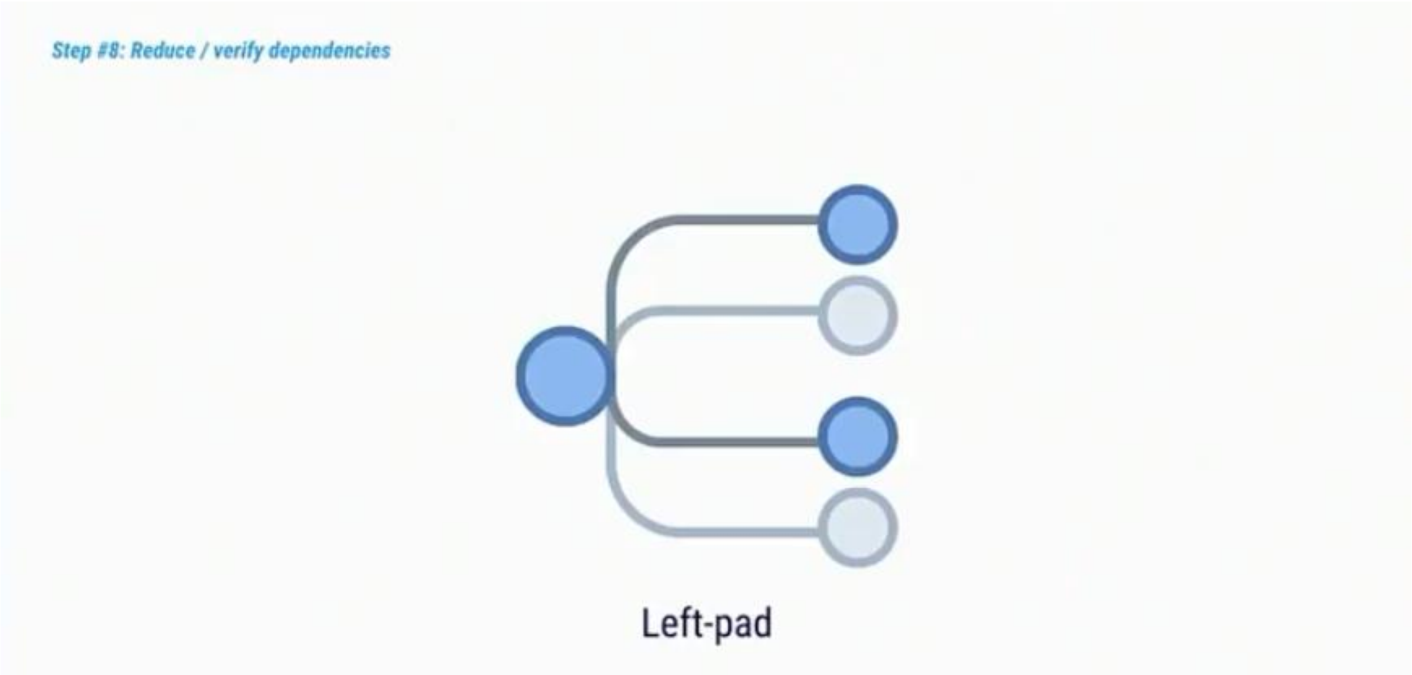
2010



OWASP Top 10

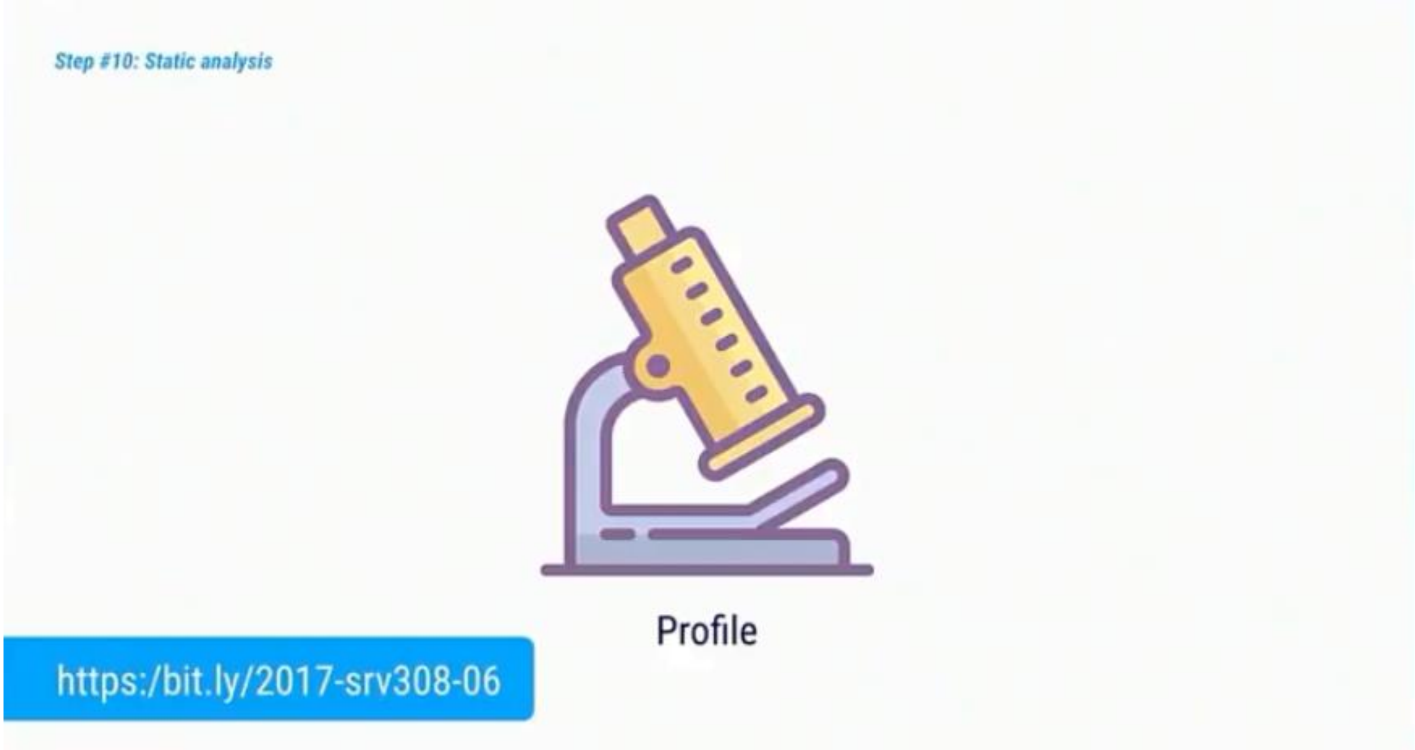
A1	Injection
A2	Broken Auth & Session Management
A3	Cross-Site Scripting
A4	Broken Access Control ⭐
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Insufficient Attack Protection ⭐
A8	Cross-Site Request Forgery
A9	Using Components With Known Vulnerabilities
A10	Underprotected APIs ⭐

2010 *2013* *2017*



Step #8: Reduce / verify dependencies

Left-pad



Step #10: Static analysis

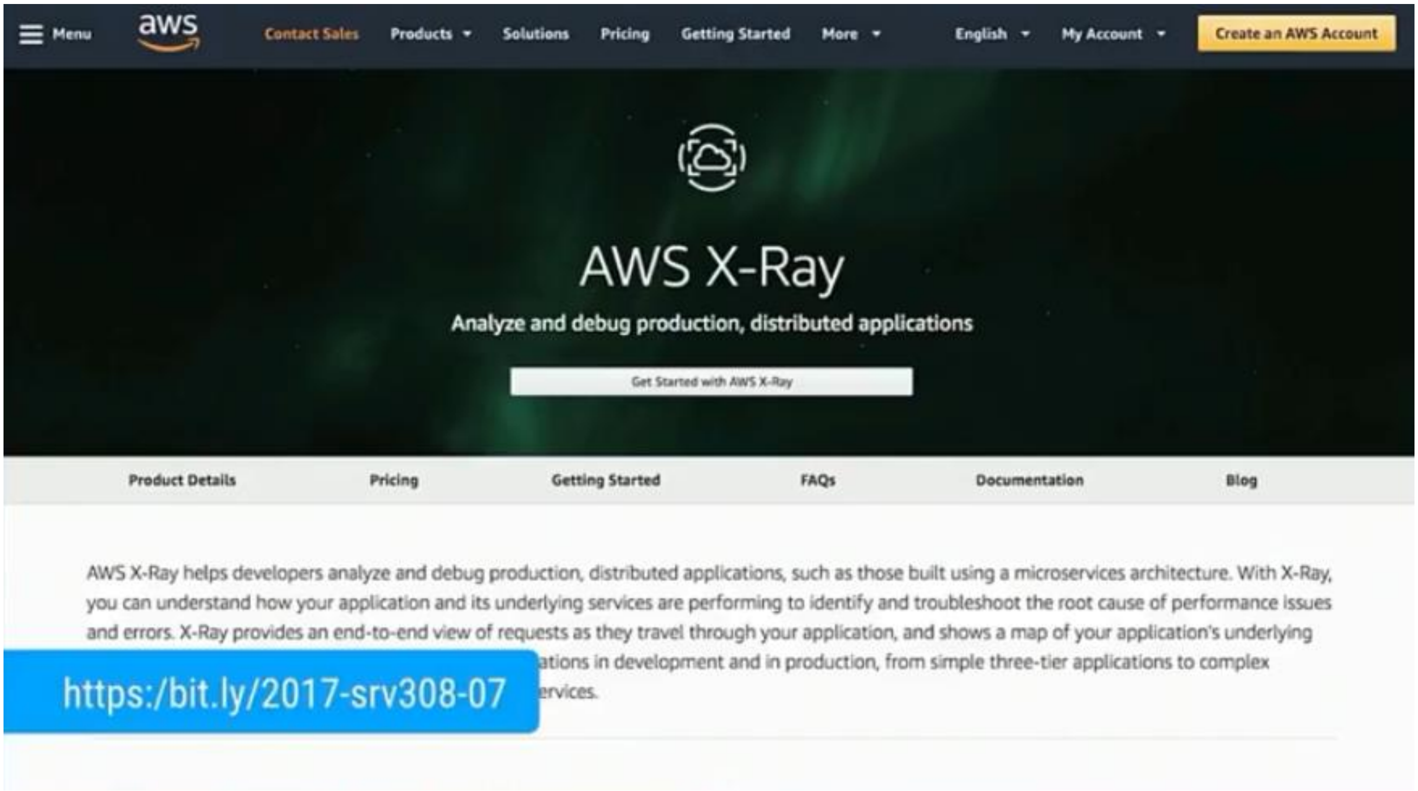
Profile

https:/bit.ly/2017-srv308-06

Data Flow

Step #11: Monitor the flow of information

Monitor



AWS X-Ray

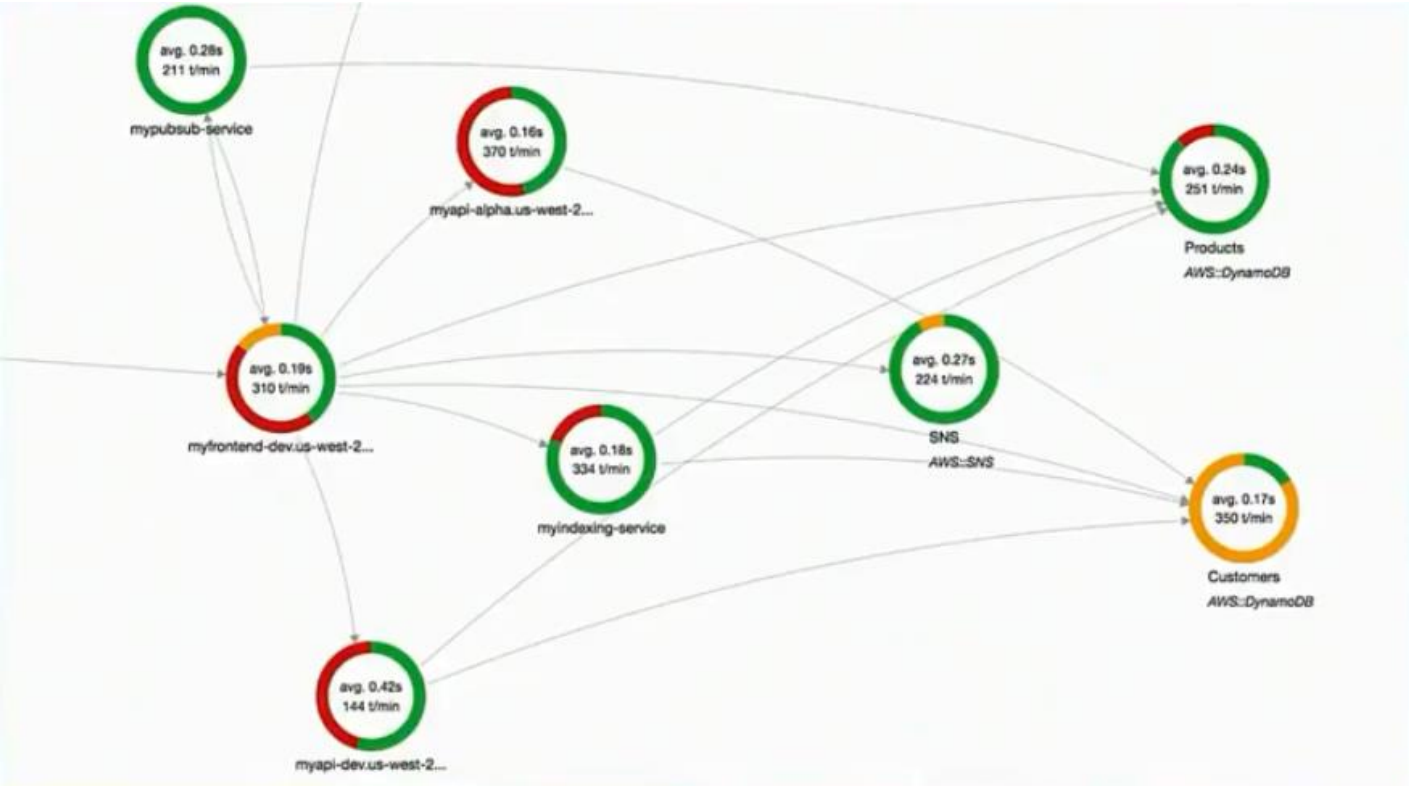
Analyze and debug production, distributed applications

AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying

ations in development and in production, from simple three-tier applications to complex

ervices.

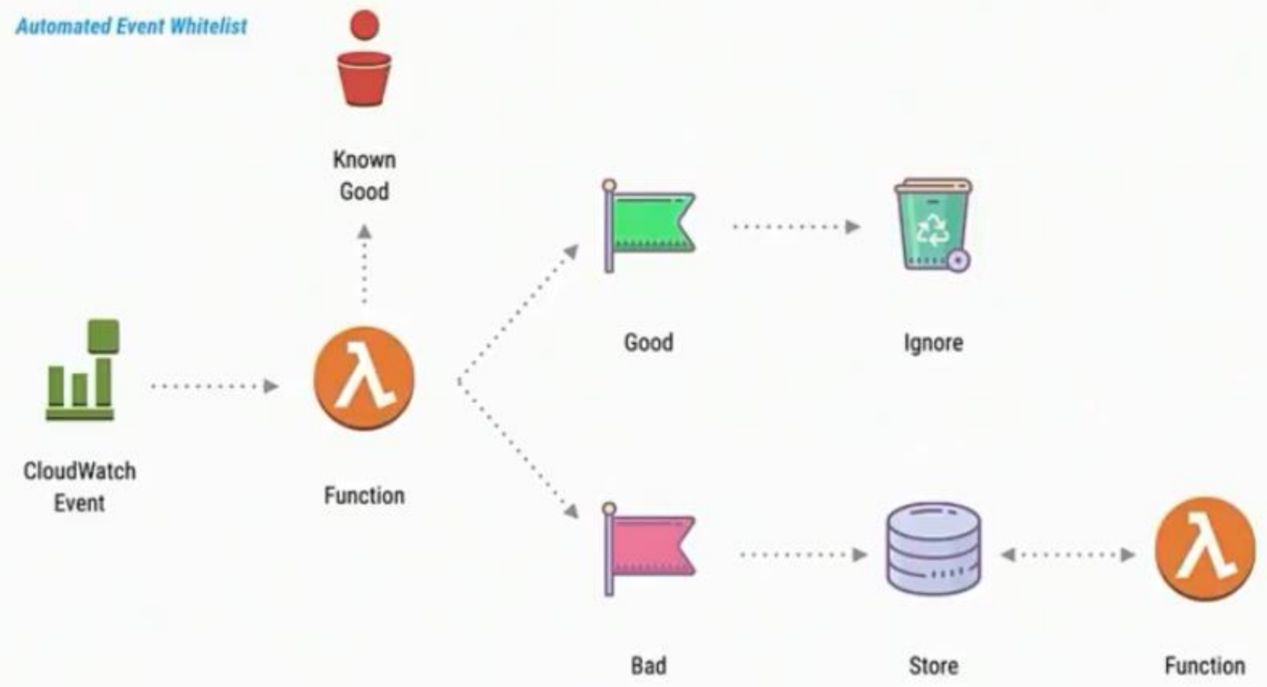
https:/bit.ly/2017-srv308-07



Amazon CloudWatch

https:/bit.ly/2017-srv308-08

Automated Event Whitelist



amazon macie

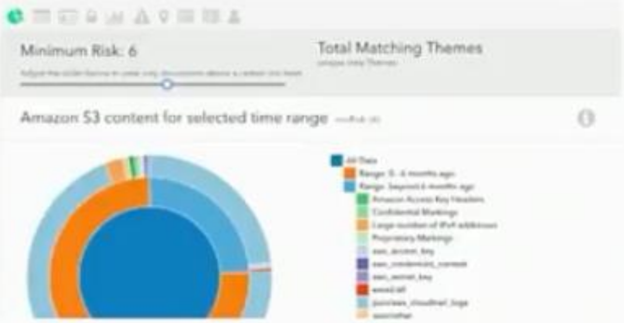
A machine learning-powered security service to discover, classify, and protect sensitive data.

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect
cie recognizes sensitive data such as personally identifiable information
ovides you with dashboards and alerts that give visibility into how this
he fully managed service continuously monitors data access activity for
anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data
leaks. Today Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS

https:/bit.ly/2017-srv308-09

Data Visibility

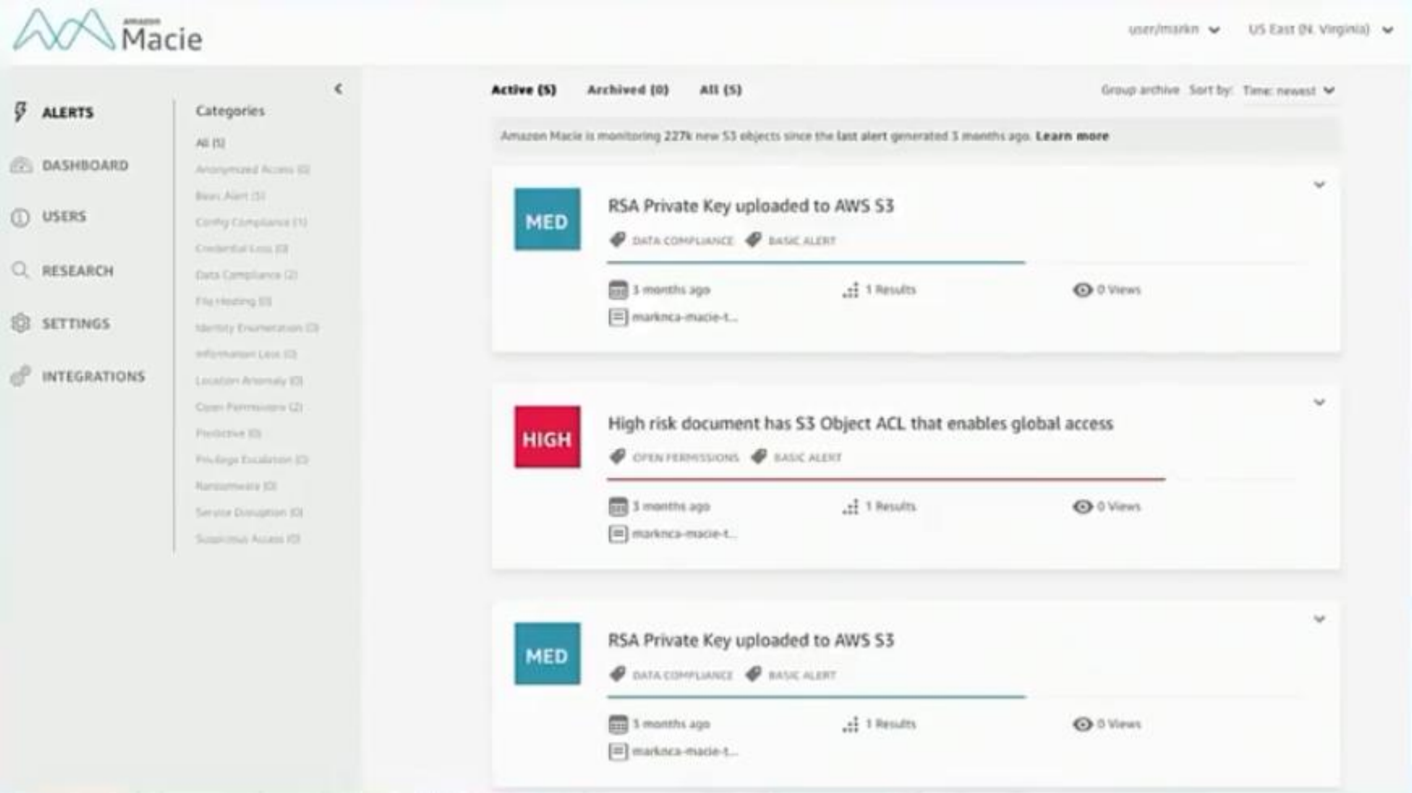
Amazon Macie uses machine learning-based classification of your Amazon S3 objects to provide visibility into your S3 environment. Macie can identify data with high business value including programming languages to detect source code, logging formats, database backup formats, credentials, and API key formats.



Minimum Risk: 6

Total Matching Themes

Amazon S3 content for selected time range



Amazon Macie

user/markn US East (N. Virginia)

ALERTS

DASHBOARD

USERS

RESEARCH

SETTINGS

INTEGRATIONS

Categories

All (5)
Anonymized Access (0)
Basic Alert (3)
Config Compliance (1)
Credential Loss (0)
Data Compliance (2)
File Hosting (0)
Identity Enumeration (0)
Information Loss (0)
Location Anomaly (0)
Open Permissions (2)
Predictive (0)
Privilege Escalation (0)
Ransomware (0)
Service Disruption (0)
Suspicious Access (0)

Active (5) Archived (0) All (5)

Group archive Sort by: Time: newest

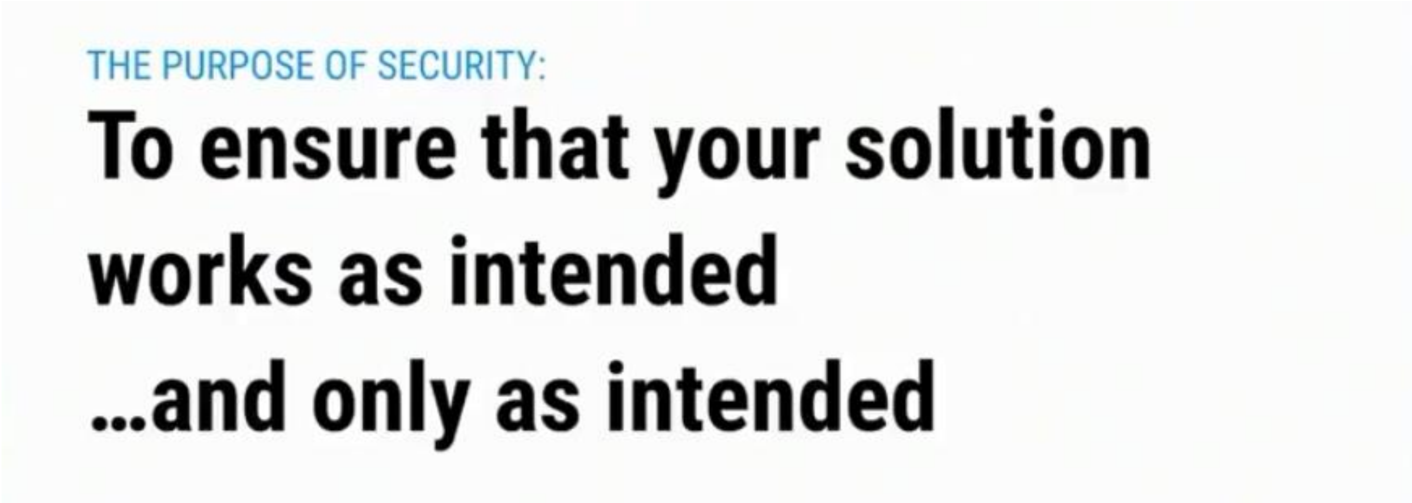
Amazon Macie is monitoring 227k new S3 objects since the last alert generated 3 months ago. **Learn more**

MED RSA Private Key uploaded to AWS S3
DATA COMPLIANCE BASIC ALERT
3 months ago 1 Results 0 Views
marknca-macie-t...

HIGH High risk document has S3 Object ACL that enables global access
OPEN PERMISSIONS BASIC ALERT
3 months ago 1 Results 0 Views
marknca-macie-t...

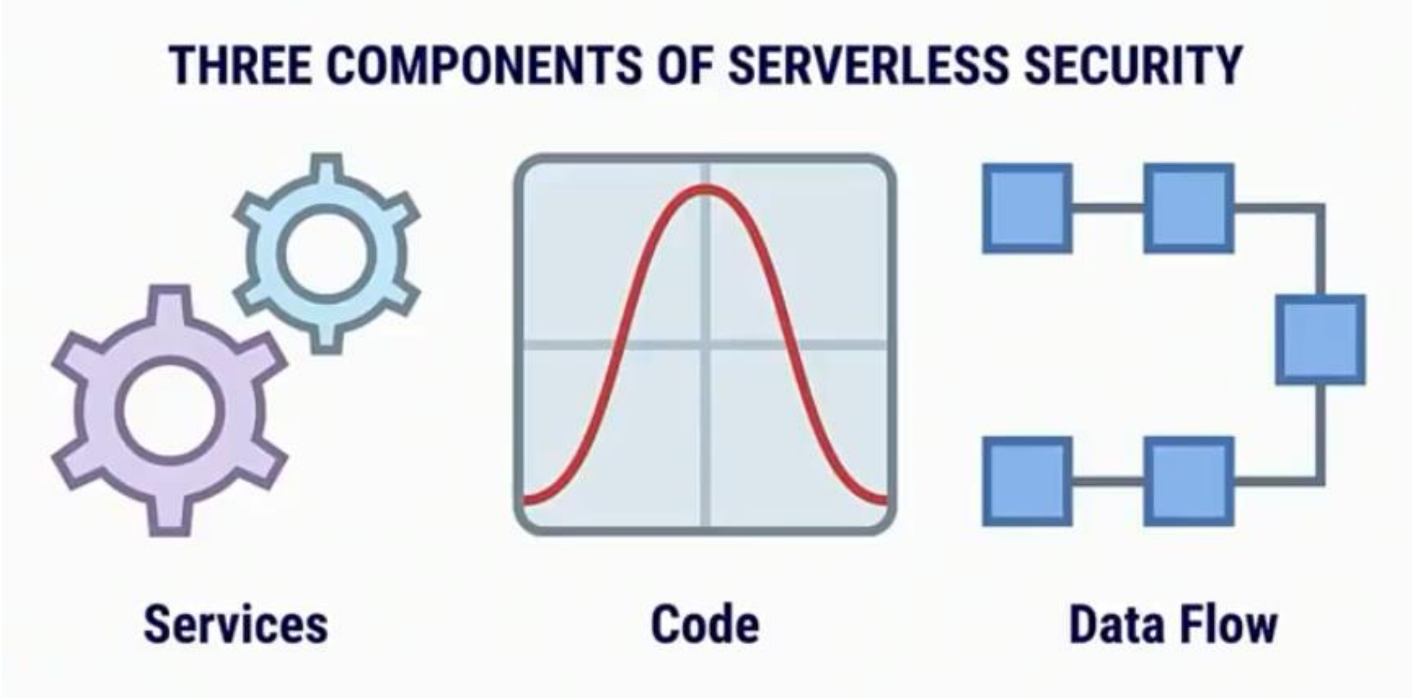
MED RSA Private Key uploaded to AWS S3
DATA COMPLIANCE BASIC ALERT
3 months ago 1 Results 0 Views
marknca-macie-t...

Take Aways



THE PURPOSE OF SECURITY:

To ensure that your solution works as intended …and only as intended

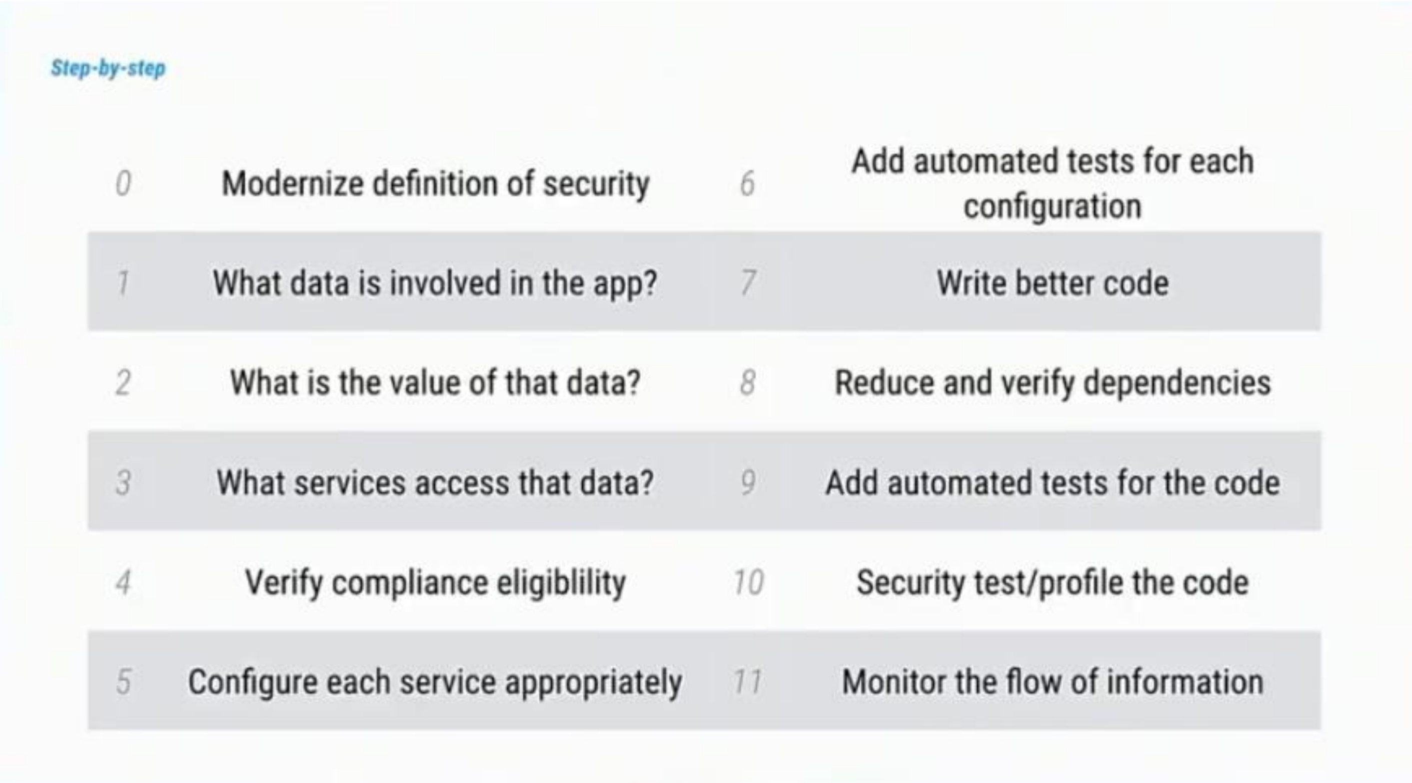


THREE COMPONENTS OF SERVERLESS SECURITY

Services

Code

Data Flow



Step-by-step

0 Modernize definition of security

1 What data is involved in the app?

2 What is the value of that data?

3 What services access that data?

4 Verify compliance eligiblility

5 Configure each service appropriately

6 Add automated tests for each configuration

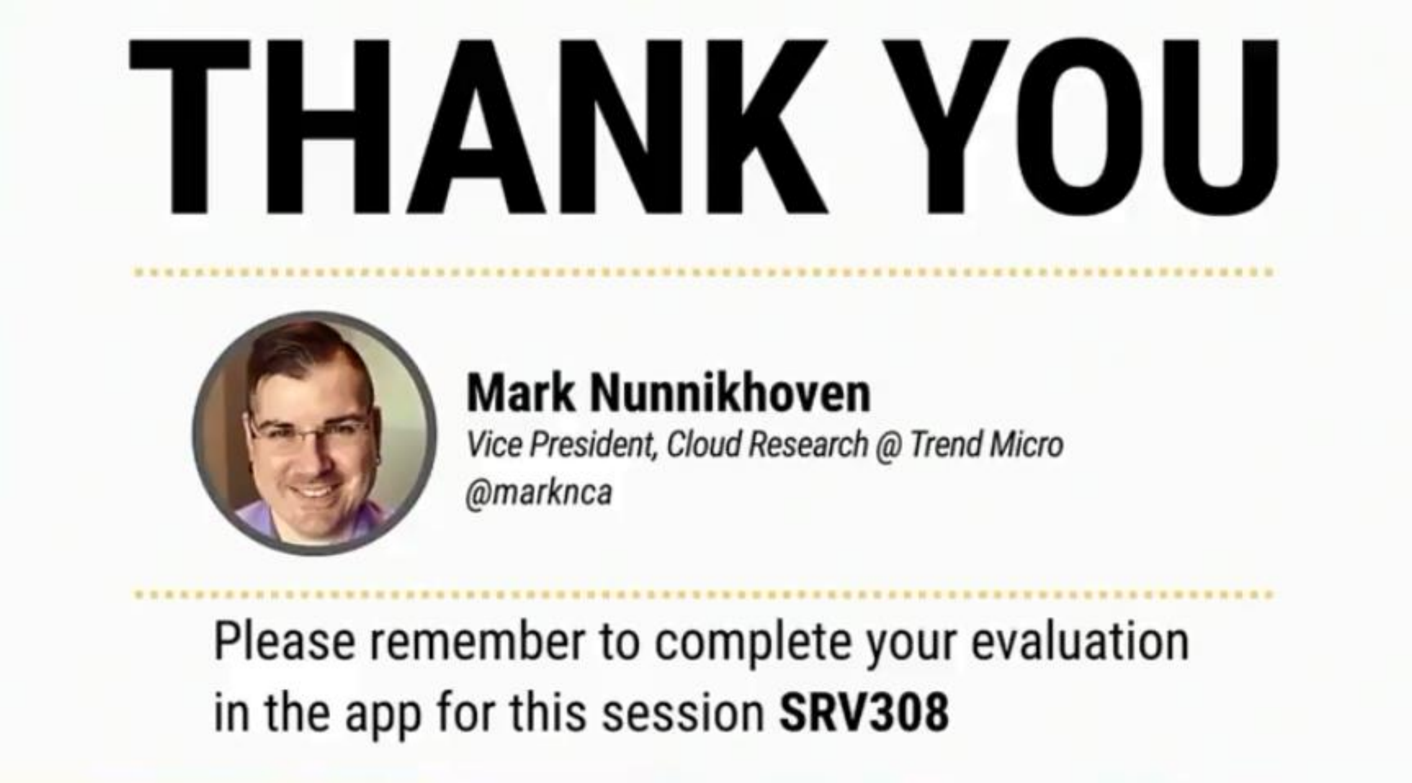
7 Write better code

8 Reduce and verify dependencies

9 Add automated tests for the code

10 Security test/profile the code

11 Monitor the flow of information



THANK YOU

Mark Nunnikhoven
Vice President, Cloud Research @ Trend Micro
@marknca

Please remember to complete your evaluation in the app for this session **SRV308**