AWS Security Best Practices

Kaung Thant Lwin @ AWSUGMM

mgkaungthant15@gmail.com

Agenda

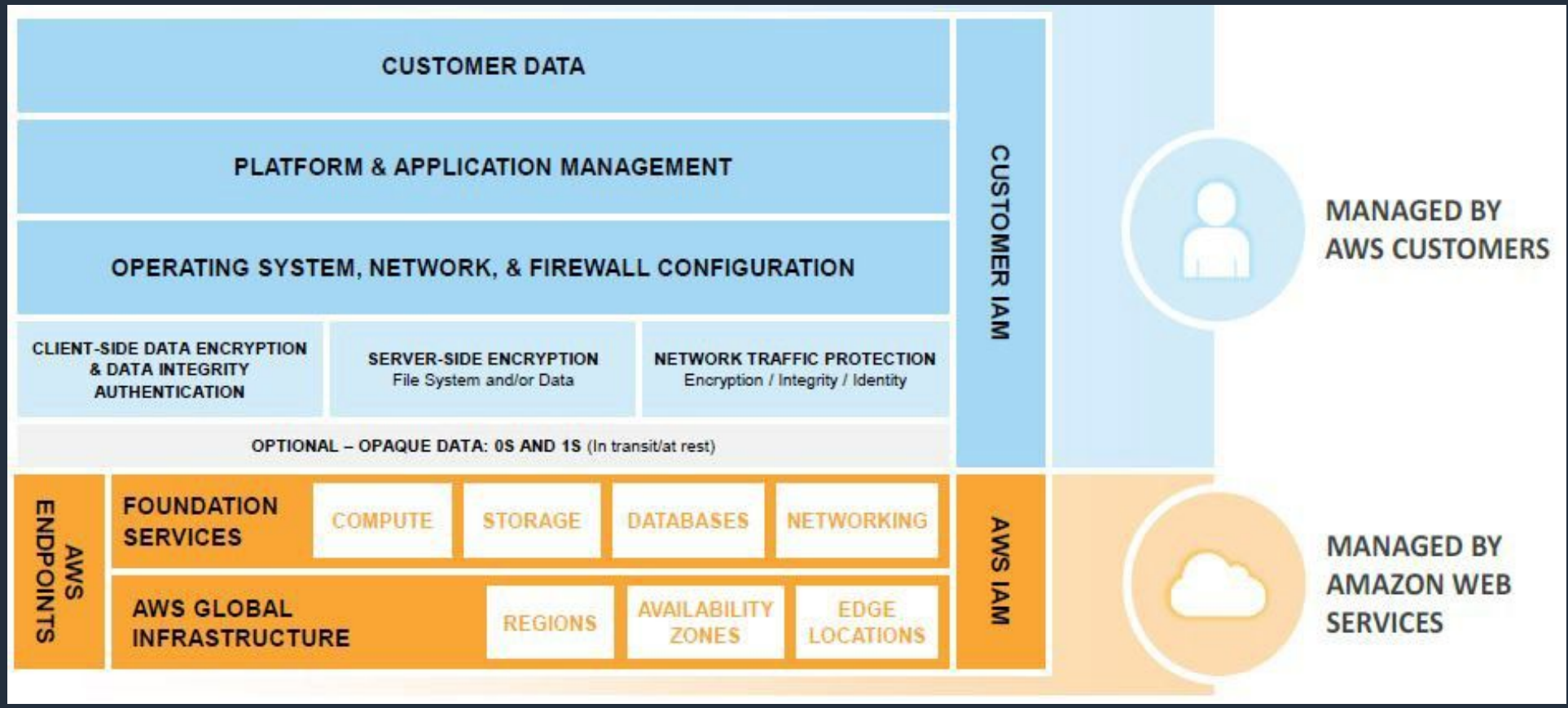
- ❑ Understand the Shared Responsibility
- ❑ Manage users and permissions
- ❑ Encrypt Everything
- ❑ Log Everything
- ❑ Automated security checks

AWS Shared Responsibility Models

1. Shared Responsibility Models for **Infrastructure Services**
2. Shared Responsibility Models for **Container Services**
3. Shared Responsibility Models for **Abstract Services**

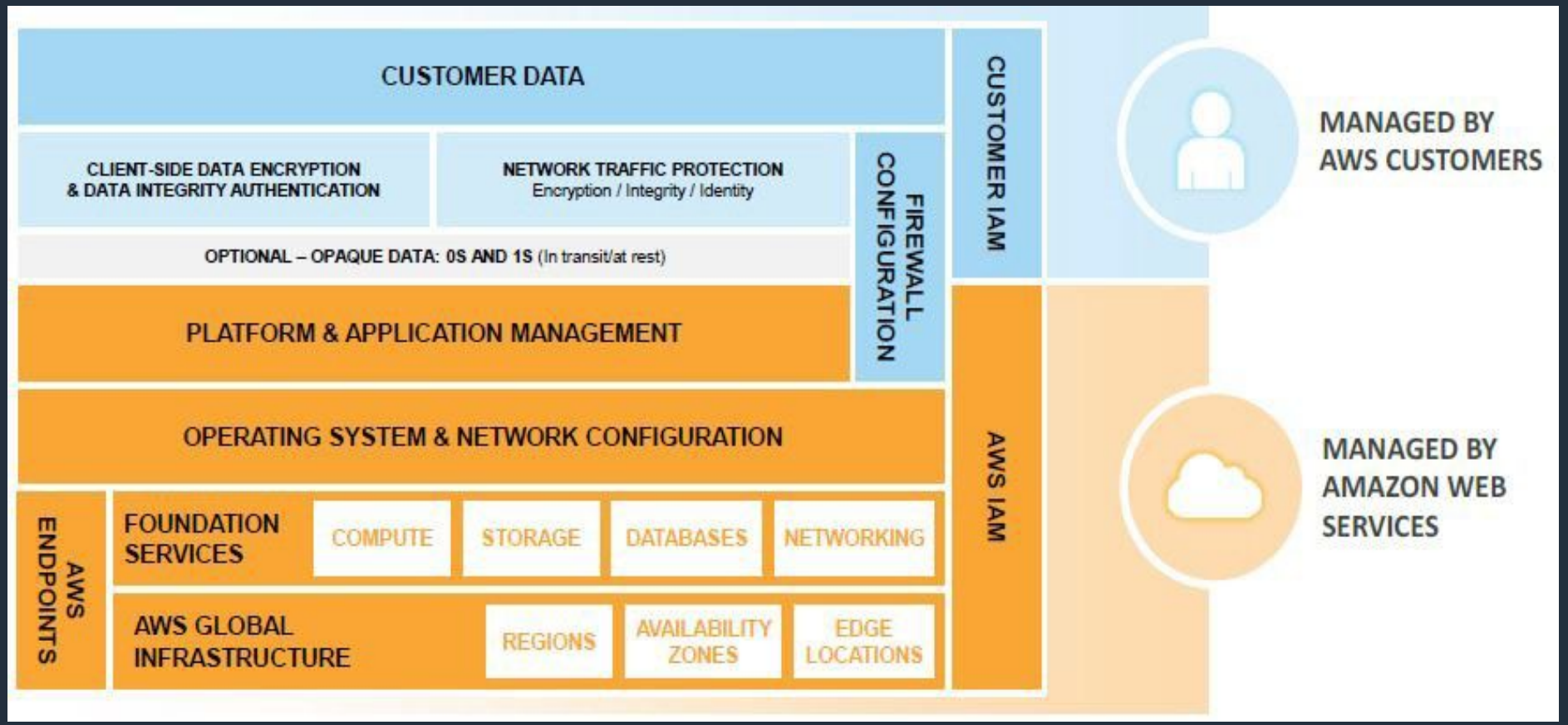
AWS Shared Responsibility Model-Infrastructure Services

Such As Amazon EC2, Amazon EBS, & Amazon VPC



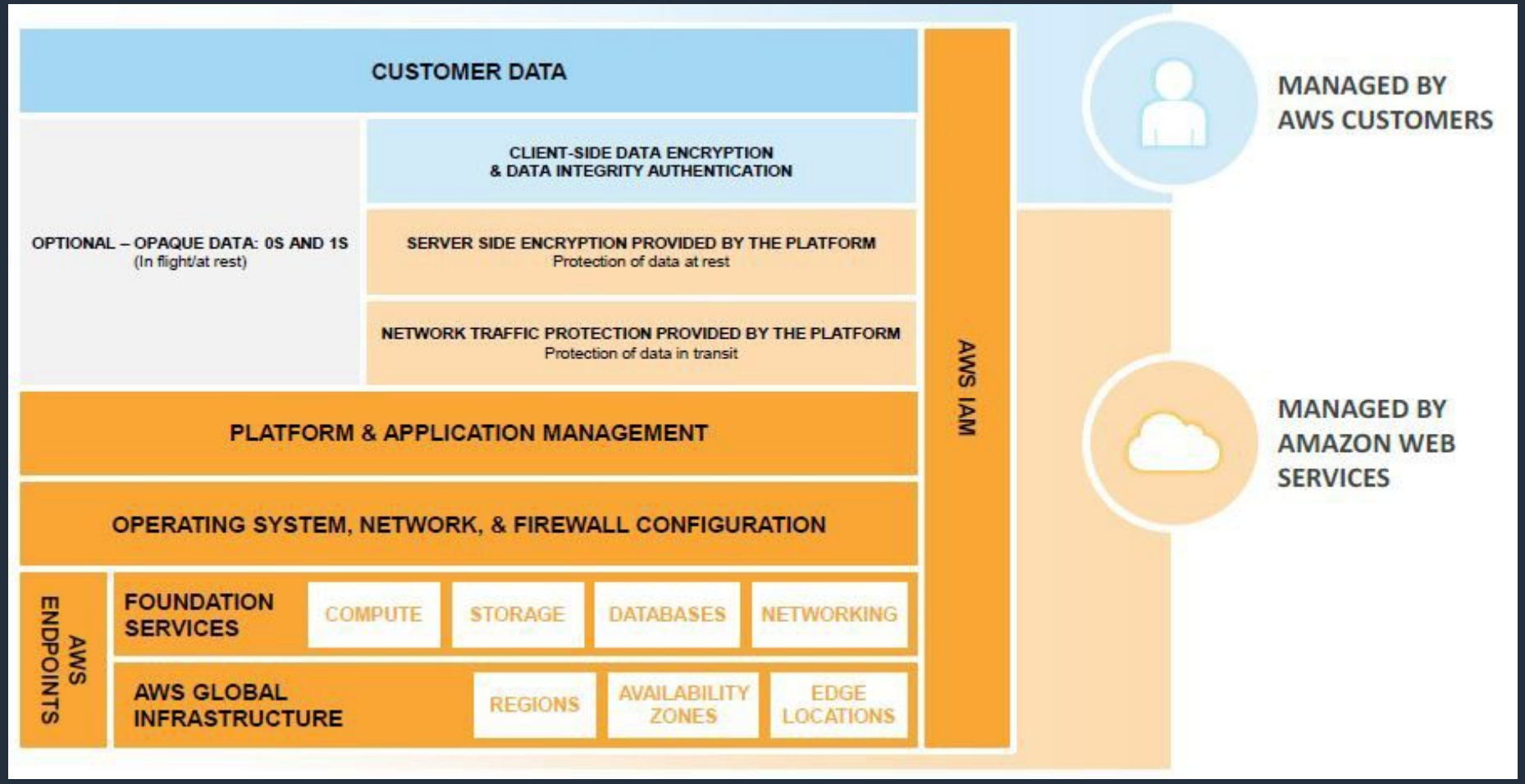
AWS Shared Responsibility Model-Container Services

Such As Amazon RDS, Amazon EMR & Amazon Elastic Beanstalk



AWS Shared Responsibility Model-Abstract Services

Such As Simple Storage Service(S3), DynamoDB, Amazon Glacier, SQS



Manage Users and Permissions

IAM Best Practices

- Create users
  - Unique credentials
  - Easier to rotate
  - Easier to track
- Factorize permissions with groups
  - Simplest way to manage permissions for similar users
- Use conditional permissions for privileged accounts (time, IP, etc)
  - Extra security
  - Possible for all APIs

Manage Users and Permissions

IAM Best Practices

- Enable Cloudtrail to log all API calls
  - Keep a log for ALL activity inside your AWS account
  - Useful for debugging and Vital for forensics
- Use a strong password policy

- Rotate security credentials regularly
  - Just in case one of your credentials leaked

- Enable MFA (Multi-factor Authentication) for privileged users
  - Protection against phishing attacks

Manage Users and Permissions
IAM Best Practices

- Use IAM roles to delegate permissions
  - No need to store or share security credentials
  - Use cases
    - Cross-account access
    - Federation

- Use IAM roles for EC2 instances
  - No need to store, share or rotate security credentials
  - Application is granted least-privilege
  - Integration with the AWS SDK and the AWS CLI

Encrypt Everything

- Native server-side encryption for most services
  - S3, EBS, RDS, Redshift, etc.

- Flexible key management
  - AWS Key Management Service (Only supports symmetric encryption)
  - AWS CloudHSM (Use both asymmetric and symmetric algorithms)

Log Everything

Infrastructure Logs

- AWS CloudTrail
- VPC Flow Logs

Service Logs

- Amazon S3
- Amazon CloudFront
- AWS Lambda
- AWS Elastic Load Balancing

Instance Logs

- Unix/Windows Logs
- Nginx/Apache/IIS
- Your own logs

Automated Security Check

- AWS Config Rules
  - Pre-defined rules: MFA On, CloudTrail On, EBS Encryption, etc.
  - Your own rules

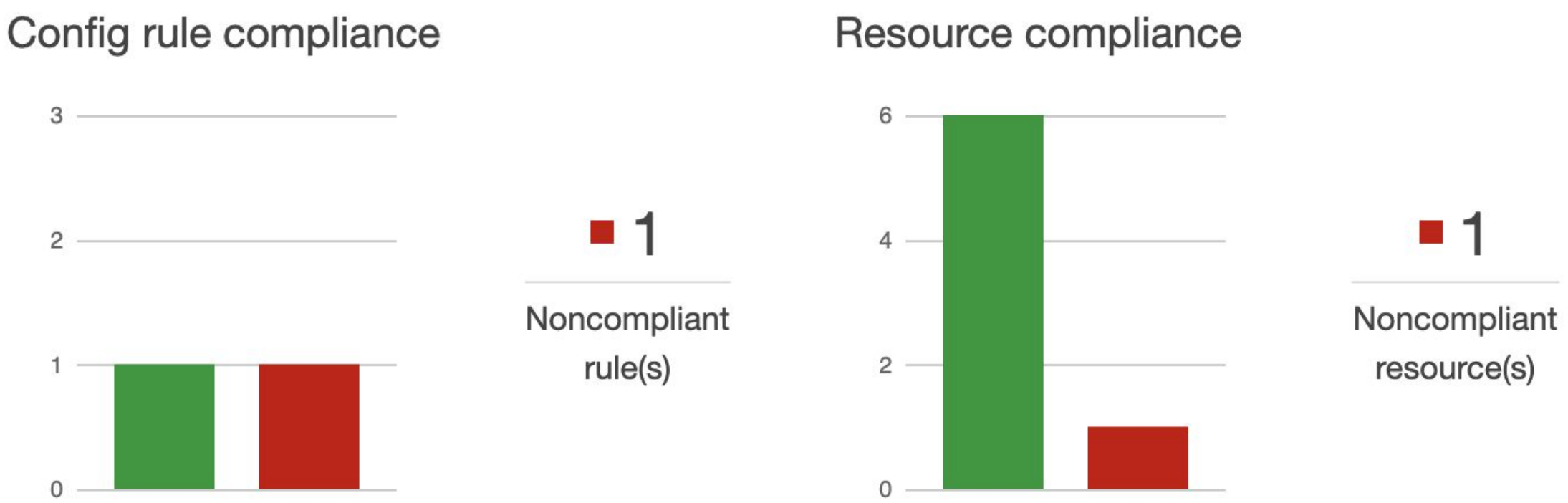
- Amazon Inspector
  - Check the configuration and the behavior of EC2 instances.
  - Agent-based
  - Can run from 15 mins to 24 hrs
  - Reports and advice on how to fix issues
  - Can be automated with the AWS API
  - Built-in rule packages

Amazon Inspector Rules Package

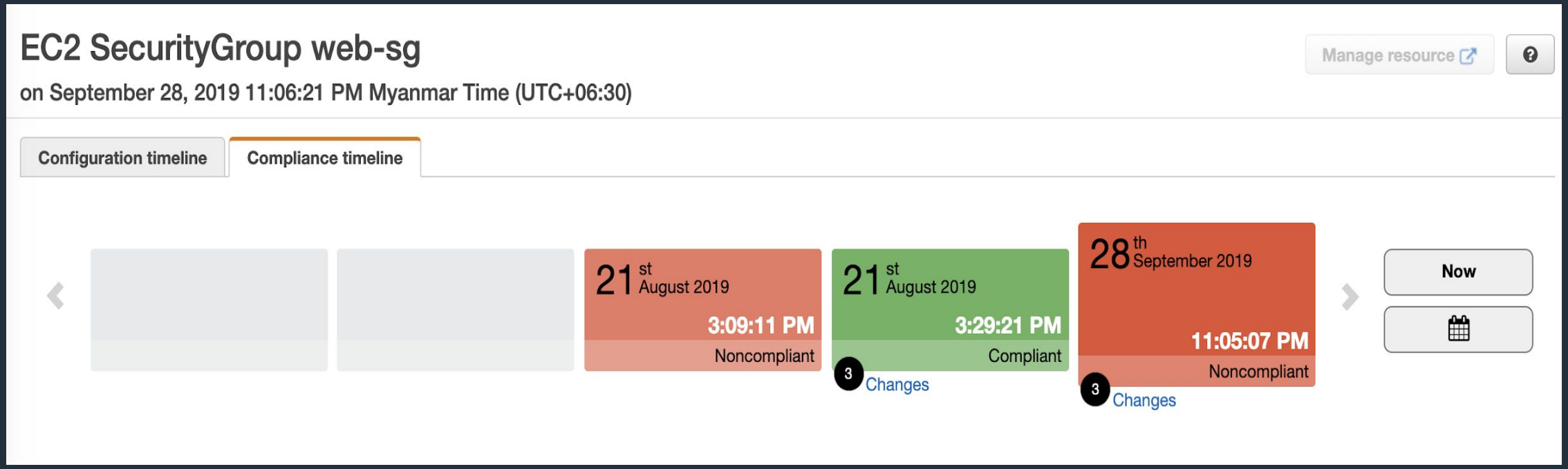
- Common Vulnerabilities and Exposures
  - http://cve.mitre.org
  - https://s3-us-west-2.amazonaws.com/rules-engine/CVEList.txt (47,050)

- CIS Security Benchmarks (Center for Internet Security)
  - https://www.cisecurity.org/benchmark/amazon_web_services/

AWS Config



AWS Config



Amazon Inspector

Name	Duration	Target name
AWSUGMM-Inspector-Demo	N/A	My Assessment Target

Assessment Template - AWSUGMM-Inspector-Demo

Name* AWSUGMM-Inspector-Demo

Target name* My Assessment Target

Rules packages* Security Best Practices-1.0

Common Vulnerabilities and Exposures-1.1

CIS Operating System Security Configuration Benchmarks-1.0

Select an Inspector rules package

Duration* 1 Hour (Recommended)

Amazon Inspector

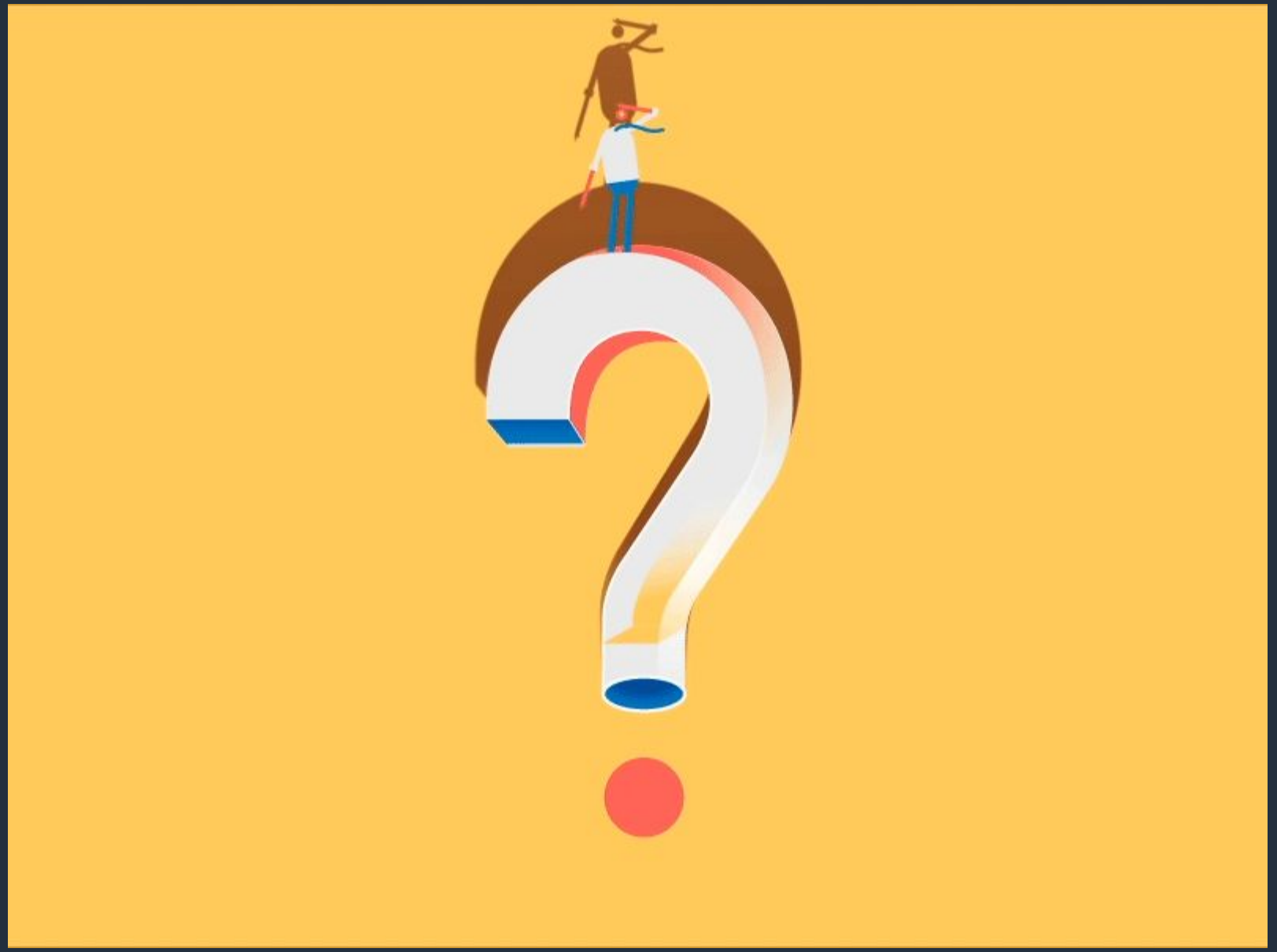
Amazon Inspector - Assessment Report

Findings Report

Report generated on 2019-09-28 at 18:39:08 UTC

Assessment Template: AWSUGMM-Inspector-Demo

Assessment Run start: 2019-09-28 at 16:31:37 UTC
Assessment Run end: 2019-09-28 at 17:33:03 UTC




THANK
YOU