AWS Security Series

Part 1: AWS Security Fundamentals & Audit Best Practices

Nitin Sharma
CyberSecurity and DevSecOps Engineer
LinkedIn: linkedin.com/in/nitins87
Quora: quora.com/profile/NitinS-1
Blog: 4hathacker.in

Contents

$ whoami

$ AWS Shared Responsibility Model (Diagram and Explanation)

$ AWS Well Architected Framework (Pillars and Understanding)

$ AWS Security Pillar (5 areas of AWS Security)

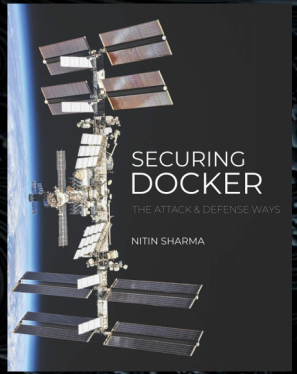
$ AWS Security - Perspective and Services

$ AWS Security Auditing

$ Demo - AWS Security Audit with Prowler

$ whoami

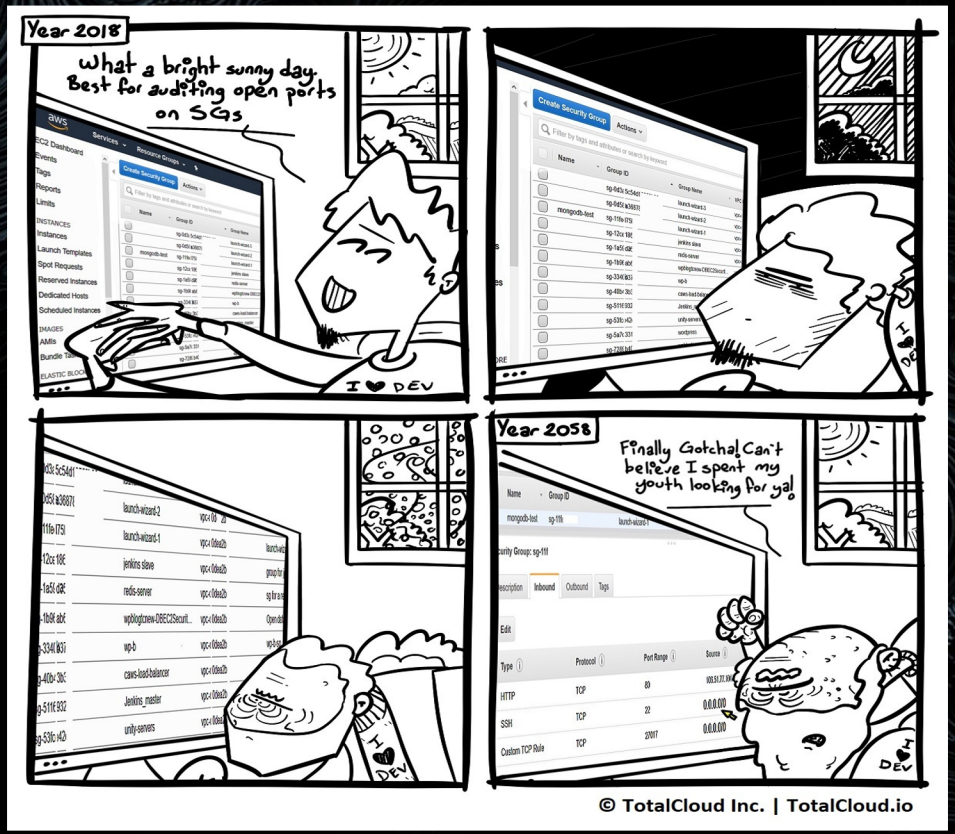
- Cybersecurity and DevSecOps professional experienced in Cloud Security, Container Security and DevOps Research
- Certifications:



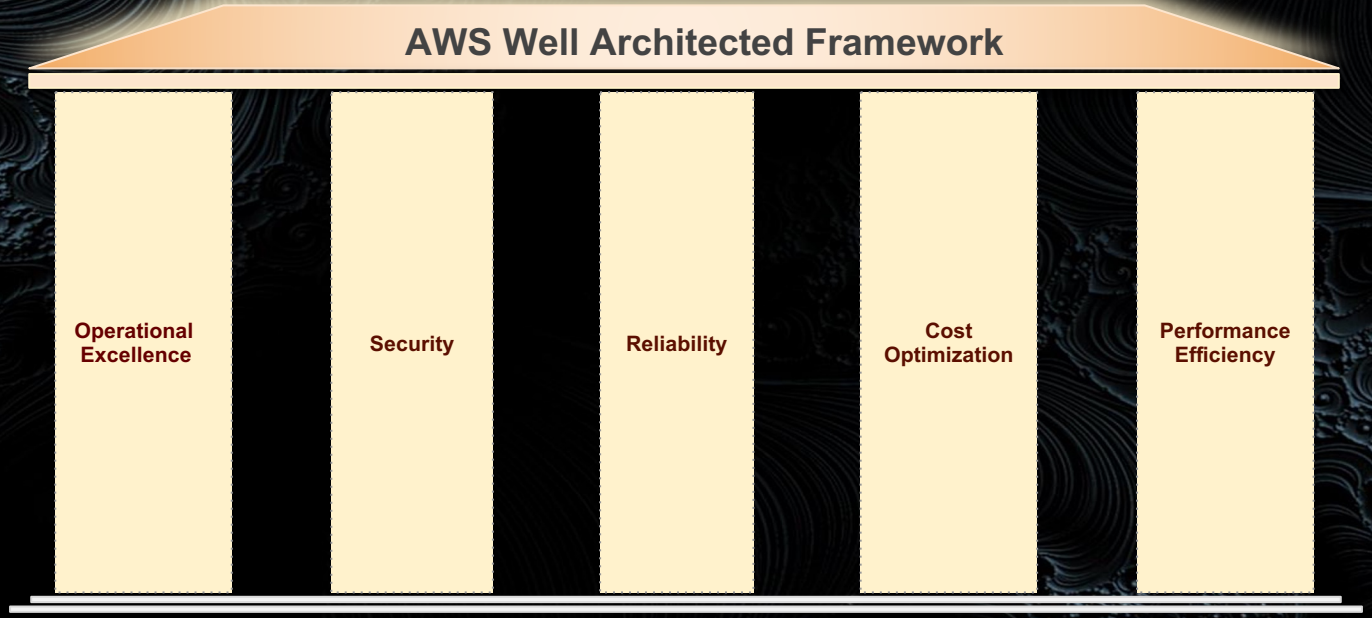
- Published author for "Securing Docker - The Attack & Defense Ways" book under CyberSecrets Publication
- Half Marathon runner, Cyclist and Fitness Enthusiast
- Helping out beginners in Cloud, DevOps and CyberSec at Quora

AWSUGNCR * AWS USER GROUP NCR *

$ whoami (in the past…)



$ AWS Well Architected Framework



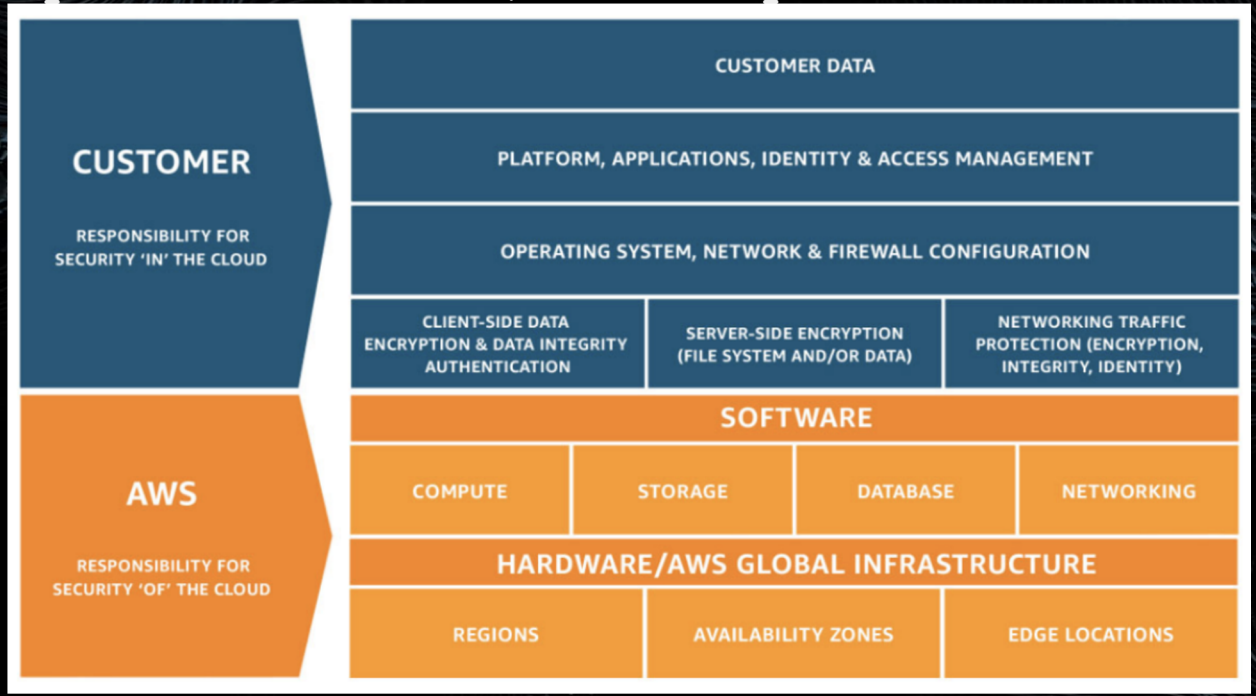
(Source: https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf)

$ AWS Shared Responsibility Model

- Security 'IN' the Cloud v/s Security 'OF' the Cloud

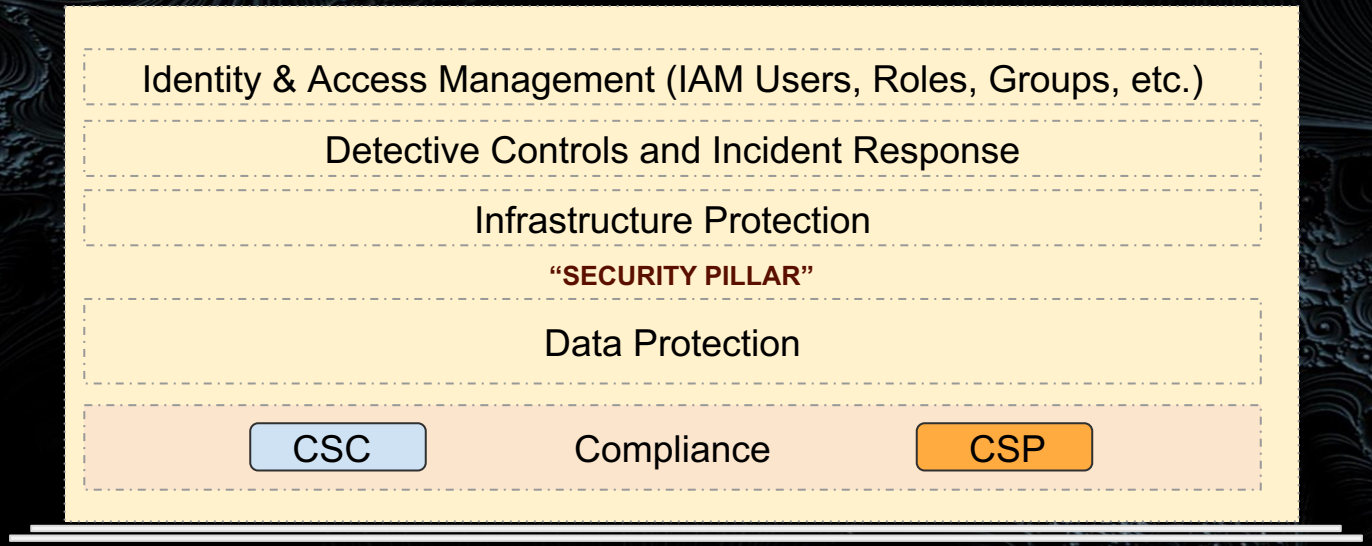
C S C

C S P



(Source: https://aws.amazon.com/compliance/shared-responsibility-model/)

$ AWS - Security Pillar



(Source: Security, Identity And Compliance in AWS)

$ AWS Security - Perspective & Services

Identity and access management

AWS Identity and Access Management (IAM)

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

AWS Organizations

AWS Secrets Manager

AWS Resource Access Manager

Detective controls

AWS Security Hub

Amazon GuardDuty

AWS Config

AWS CloudTrail

Amazon CloudWatch

VPC flow logs

Infrastructure protection

AWS Systems Manager

AWS Shield

AWS WAF – Web application firewall

AWS Firewall Manager

Amazon Inspector

Amazon Virtual Private Cloud (Amazon VPC)

Data protection

AWS Key Management Service (AWS KMS)

AWS CloudHSM

AWS Certificate Manager (ACM)

Amazon Macie

Server-side encryption

Incident response

AWS Config rules

AWS Lambda

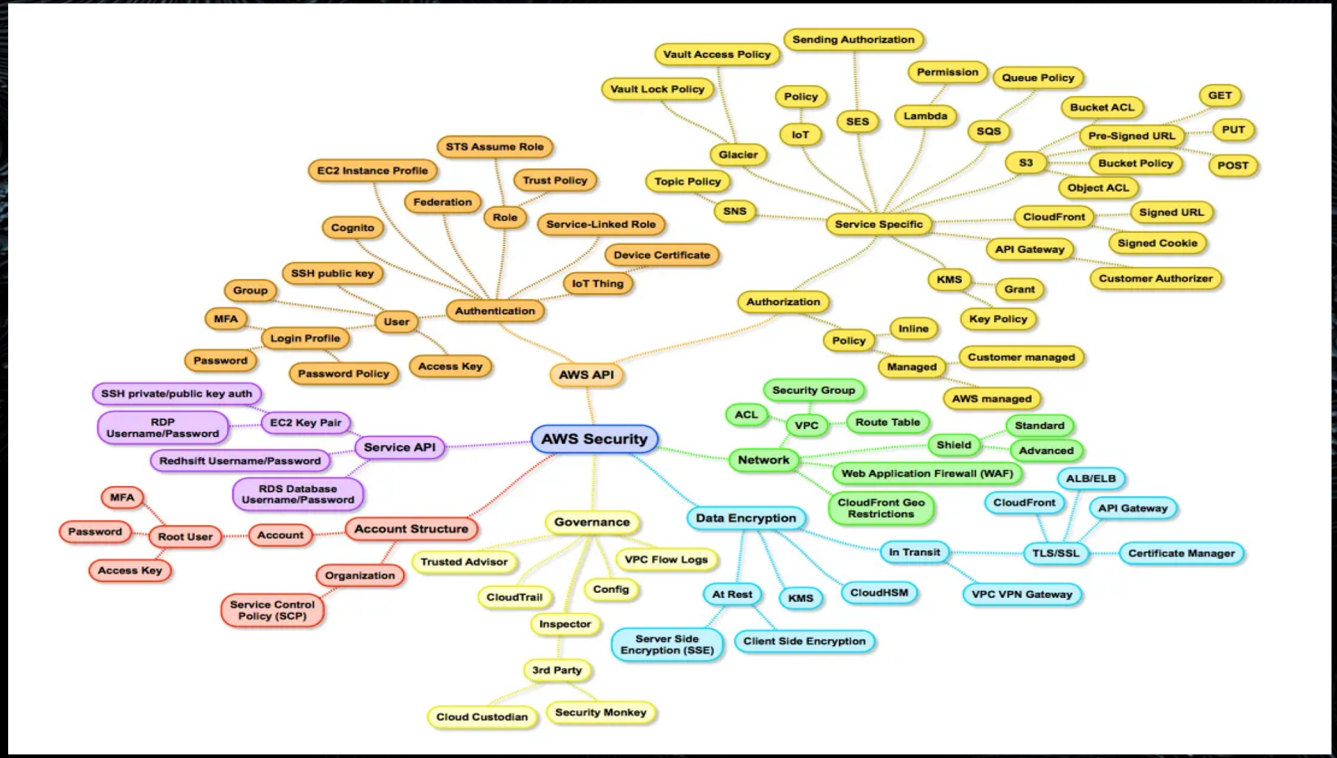
(Source: AWS CAF Security Perspective Capabilities)

$ AWS Security - Perspective & Services

- CSPs are responsible for their cloud based infrastructure to be COMPLIANT.
- CSCs are responsible for the COMPLIANCE of their own data, networks, applications, and operating systems that lives in the cloud.

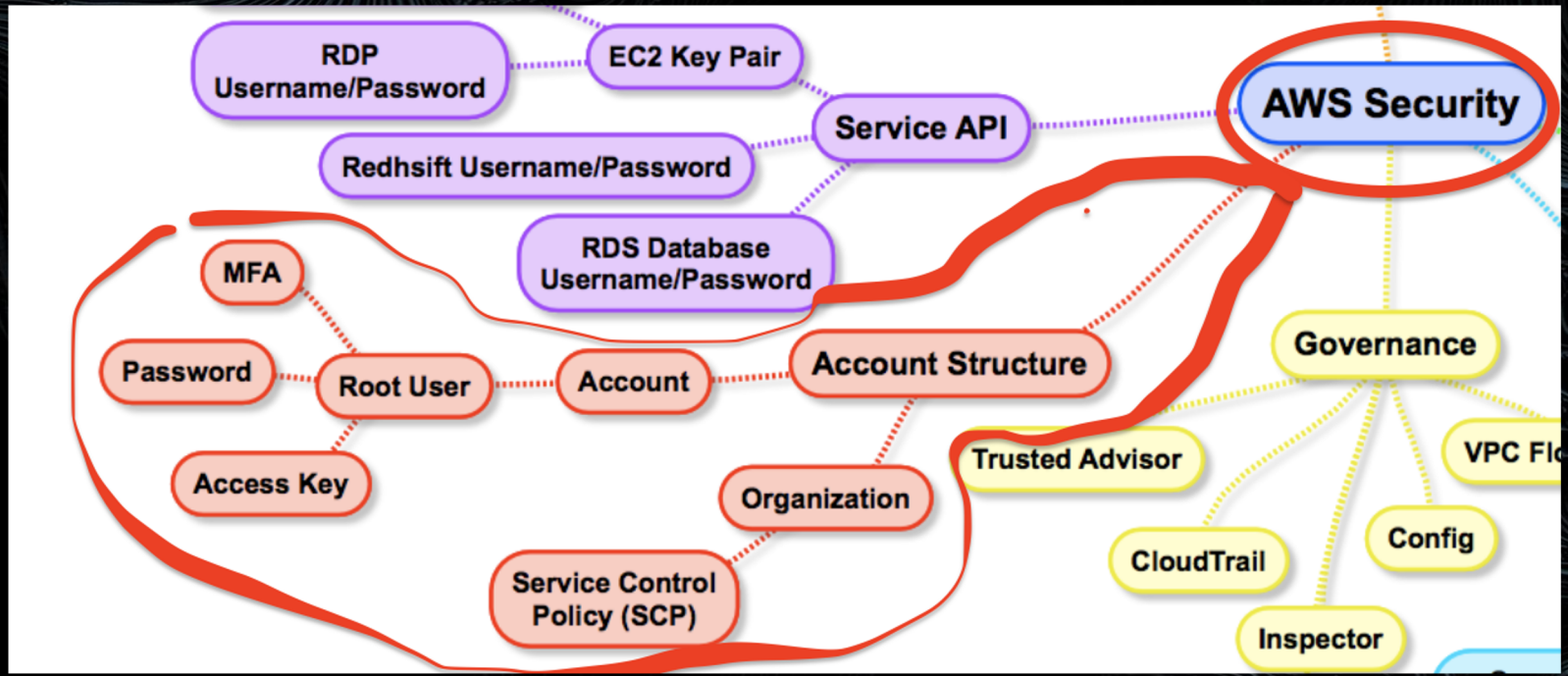
Important Note:
Compliance (Act) ≠ Security (Objective)

$ AWS Security - Perspective & Services



(Source: https://cloudonaut.io/images/2017/05/aws-security-surface.png)

$ AWS Security - Perspective & Services



(Source: https://cloudonaut.io/images/2017/05/aws-security-surface.png)

$ AWS Security Auditing

A *Cloud Security Audit* refers to an independent examination of internal and external (cloud) processes as per the scope defined by applicable regulatory requirements and organisational policies, performed by a qualified personnel/assessor. This could be either Internal or External based on the objectives and expectations.

Important Note:
Audit = Proving (or Disproving) Compliance

$ AWS Security Auditing

- Usually the assessment/examination is based on some control requirements.
- E.g. Security Control XY(#N)
  - Ensure that there are no AWS IAM users with the administrator permissions (privileged users) in the AWS account while adhering to AWS IAM Security Best Practices.

$ AWS Security Auditing

- Understand when that rule is said to be COMPLIANT,
  - No IAM users assigned with AWS Managed Policies that give them Administrator, Power User or Full Access to permissions to any AWS Service.
  - No IAM user assigned permissions to Create, Update or Delete all kind of AWS resources.

$ AWS Security Auditing

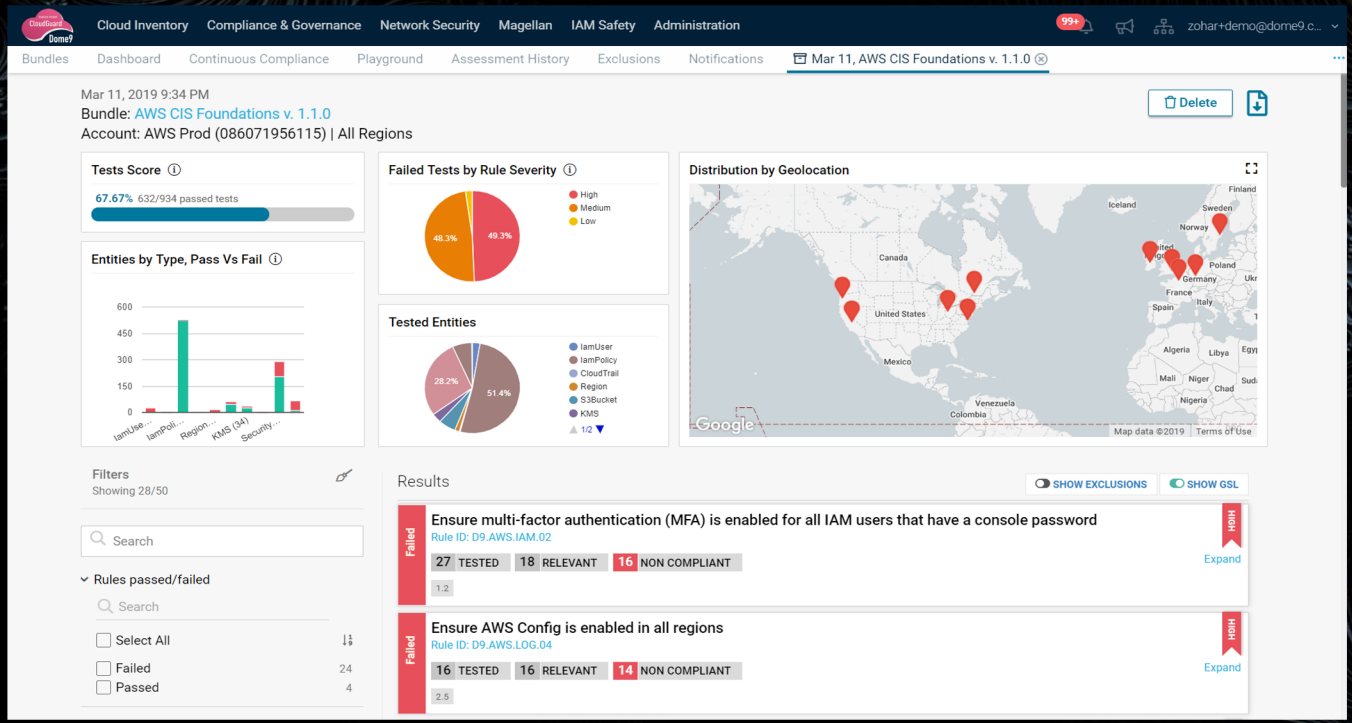
- CIS Amazon Foundations Standard
  - Control 1.13 - Ensure MFA is enabled for the “root” account.
- Payment Card Industry Data Security Standard (PCI DSS)
  - PCI.IAM.5 - Virtual MFA should be enabled for “root” user.

$ AWS Security Auditing

- Tools of Trade,
  - Proprietary:
    - CheckPoint CloudGuard Dome9
    - CloudHealth by VMware
  - Open Source:
    - ScoutSuite
    - Prowler

$ AWS Security Auditing

- CheckPoint CloudGuard Dome9



$ AWS Security Auditing

- Prowler

```
prowler v2.1.0
  the handy cloud security tool

Date: Wed Nov 27 11:40:14 EST 2019

Colors code for results:
INFO (Information), PASS (Recommended value),  FAIL (Fix required),  Not Scored

This report is being generated using credentials below:

AWS-CLI Profile: [basc] AWS API Region: [us-east-1] AWS Filter Region: [all]

Caller Identity:
-----------------------------------------------------
|                  GetCallerIdentity                |
+----------+----------------------------------------+
|  Account |  XXXXXXXXXXXX                          |
|  Arn     |  arn:aws:iam::XXXXXXXXXXXX:user/rami   |
|  UserId  |  AIDAVYKGZEV6VVEJD6YPD                 |
+----------+----------------------------------------+


1.0 Identity and Access Management - [group1] **********************

0.1 Generating AWS IAM Credential Report...

1.1  [check11] Avoid the use of the root account (Scored)
      INFO! Root account last accessed (password key_1 key_2): 2019-11-26T18:27:54+00:00 N/A N/A

1.2  [check12] Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)
      FAIL! User jdow has Password enabled but MFA disabled
      FAIL! User student-10 has Password enabled but MFA disabled
      FAIL! User student-11 has Password enabled but MFA disabled
      FAIL! User student-12 has Password enabled but MFA disabled
      FAIL! User student-13 has Password enabled but MFA disabled
      FAIL! User student-14 has Password enabled but MFA disabled
      FAIL! User student-15 has Password enabled but MFA disabled
      FAIL! User student-16 has Password enabled but MFA disabled
      FAIL! User student-17 has Password enabled but MFA disabled
      FAIL! User student-18 has Password enabled but MFA disabled
      FAIL! User student-19 has Password enabled but MFA disabled
      FAIL! User student-2 has Password enabled but MFA disabled
      FAIL! User student-20 has Password enabled but MFA disabled
      FAIL! User student-21 has Password enabled but MFA disabled
      FAIL! User student-3 has Password enabled but MFA disabled
      FAIL! User student-4 has Password enabled but MFA disabled
      FAIL! User student-5 has Password enabled but MFA disabled
      FAIL! User student-6 has Password enabled but MFA disabled
      FAIL! User student-7 has Password enabled but MFA disabled
      FAIL! User student-8 has Password enabled but MFA disabled
      FAIL! User student-9 has Password enabled but MFA disabled
```

$ Demo - AWS Security Audit with Prowler

- Prowler (by Toni de la Fuente aka toniblyx) is a command line tool that helps you with AWS security assessment, auditing, hardening and incident response.
- It follows guidelines of the CIS Amazon Web Services Foundations Benchmark (49 checks) and has more than 100 additional checks including related to GDPR, HIPAA, PCI-DSS, ISO-27001, FFIEC, SOC2 and others.

$ Demo - AWS Security Audit with Prowler

Demo Time...

$ AWS Security Audit - Cloud Audit Academy

- Cloud Audit Academy (CAA) is an Amazon Web Services (AWS) Security Auditing Free Digital Training and Learning Path designed for those that are in auditing, risk, and compliance roles and are involved in assessing regulated workloads in the cloud. (Announced in June 2017)

  Link: https://aws.amazon.com/compliance/auditor-learning-path/

Thank You...

For queries feel free to connect with AWS Delhi User Group at:

1. AWS Delhi User Group (Meet-Up) - Learn Together, Grow Together
2. AWS User Group Delhi NCR (Follow us on LinkedIn Page)