

오픈소스로 점검하는 AWS 인프라 보안

이지영

보안 엔지니어
백패커



Agenda

- AWS 보안 점검의 중요성
- 왜 오픈소스 보안 점검 툴에 관심을 가져야하는가?
- What is Prowler?
- What is AWS Service Screener v2
- Use Case

AWS 보안 점검의 중요성



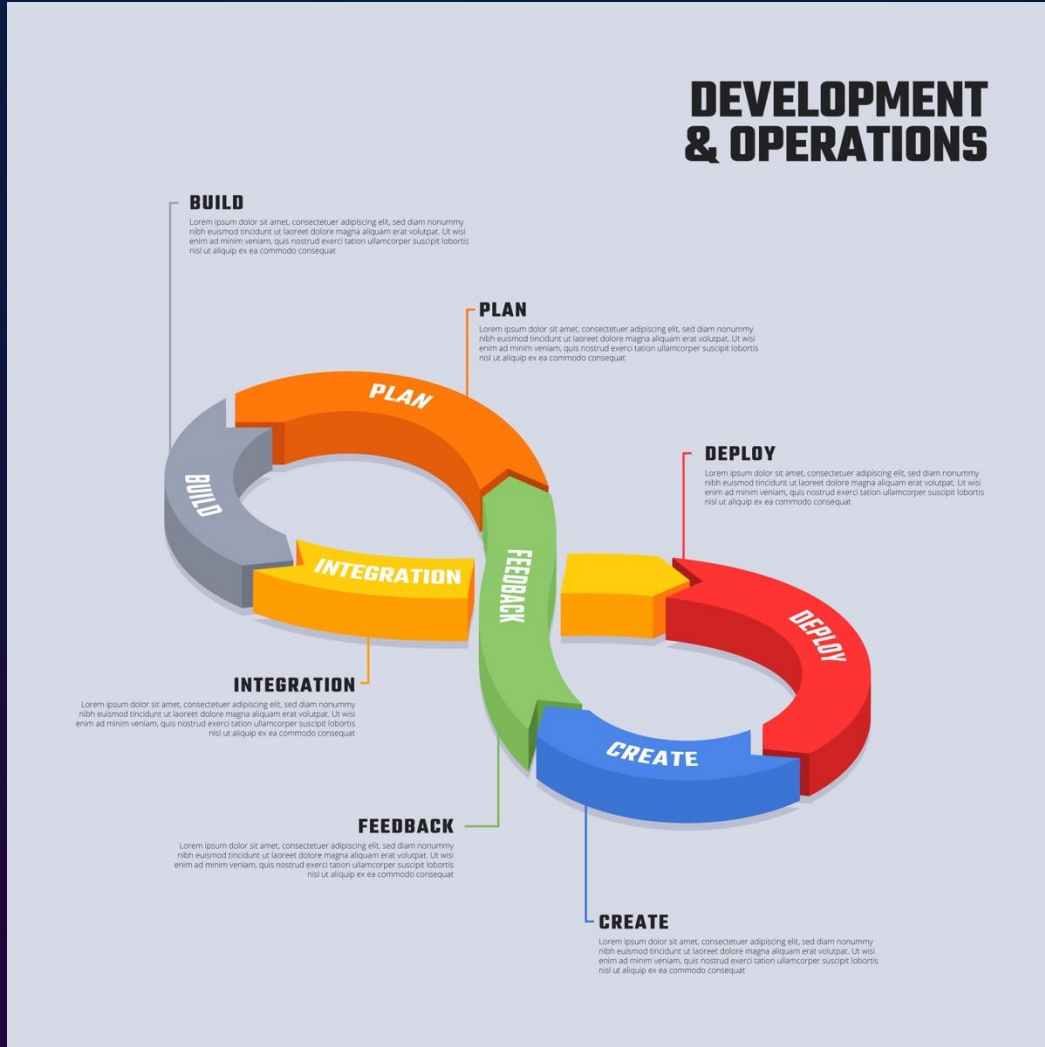
클라우드 보안설정 오류

=



보안 사고

AWS 보안 점검의 중요성



Software Development Lifecycle

SDLC는 계속해서 반복되어야 함



Security Optimization Cost

개발의 앞단계일수록 보안 개선
비용도 가장 낮아짐
배포 전/직후 클라우드 설정
점검을 파이프라인에
마이그레이션하는 것이 좋음

왜 오픈소스 보안 점검 툴에 관심을 가져야하는가?



AWS Trusted Advisor

AWS Config

-
-
-

자체 서비스들로도 당연히 점검 가능

왜 오픈소스 보안 점검 툴에 관심을 가져야하는가?

Cost Effective



검증된 보안 진단 도구를
오픈 소스를 통해
비용 효율적으로 점검 가능

Community



커뮤니티에 의해 빠르게 업데이트
되고 있어서 최신의 트렌드가
원활하게 반영됨

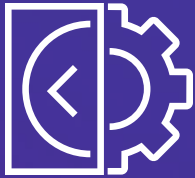
Customize



소스코드가 공개되어 있어,
필요한 경우 각 환경에 맞게
커스터마이징 가능

- What is Prowler?

01.
A



82개 AWS 서비스에
대한 560+의 점검항목
지원

02.
B



CIS, NIST, PCI-DSS,
SOC2 등 다수의
보안 프레임워크
준수 여부 점검

03.
C



커맨드라인 기반,
오픈소스 무료
(기업용 SaaS도
별도 제공)

- What is Prowler?

[illegible]

• What is Prowler?

PROWLER

Launch Scan +

Analytics

Overview

Compliance

Issues

Top failed issues

High-risk findings

Amazon Web Services

Microsoft Azure

Google Cloud

Kubernetes

Browse all findings

Settings

Configuration

Cloud Providers

Provider Groups

Sign out

Scans

Launch Scan

Choose a cloud provider

Show Filters

Provider	Started at	Status	Findings	Resources	Scheduled at	Completed at	Type	Scan name
199103129564	Mar 24, 2025 9:22 PM UTC	93% Executing	See Findings	0	Mar 24, 2025 9:22 PM UTC	--	SCHEDULED	Daily scheduled scan

1 entries in Total.

Page 1 of 1

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

• What is Prowler?

PROWLER

Launch Scan +

Analytics ^

Overview

Compliance

Issues

Top failed issues v

High-risk findings v

Browse all findings

Settings

Configuration ^

Cloud Providers

Provider Groups

Scan Jobs

Roles

Workspace

Memberships v

Sign out

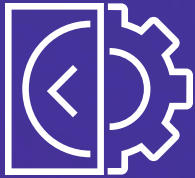
Overview

Details	Finding	Severity	Status	Last seen	Region	Service	Cloud provider
①	Find secrets in SSM Documents.	Critical ⚠	FAIL	Mar 24, 2025 9:34 PM UTC	us-east-1	ssm	aws No alias found in provider 199103129564
①	Ensure only hardware MFA is enabled for the root account	Critical ⚠	FAIL	Mar 24, 2025 9:32 PM UTC	us-east-1	iam	aws No alias found in provider 199103129564
①	Ensure no root account access key exists	Critical ⚠	FAIL	Mar 24, 2025 9:32 PM UTC	us-east-1	iam	aws No alias found in provider 199103129564
①	Ensure no security groups allow ingress from 0.0.0.0/0 or ::/0 to high risk ports.	Critical ⚠	FAIL	Mar 24, 2025 9:31 PM UTC	ap-northeast-2	ec2	aws No alias found in provider 199103129564
①	Ensure no EC2 instances allow ingress from the internet to TCP port 22 (SSH)	Critical ⚠	FAIL	Mar 24, 2025 9:31 PM UTC	ap-northeast-2	ec2	aws No alias found in provider 199103129564
①	Ensure there are no SNS Topics unencrypted	High	FAIL	Mar 24, 2025 9:34 PM UTC	us-east-1	sns	aws No alias found in provider 199103129564
①	Ensure there are no SNS Topics unencrypted	High	FAIL	Mar 24, 2025 9:34 PM UTC	us-east-1	sns	aws No alias found in provider 199103129564
①	Ensure there are no SNS Topics unencrypted	High	FAIL	Mar 24, 2025 9:34 PM UTC	us-east-1	sns	aws No alias found in provider 199103129564
①	Ensure there are no SNS Topics unencrypted	High	FAIL	Mar 24, 2025 9:34 PM UTC	us-east-1	sns	aws No alias found in provider 199103129564
①	Check S3 Account Level Public Access Block.	High	FAIL	Mar 24, 2025 9:34 PM UTC	us-east-1	s3	aws No alias found in provider 199103129564



- What is AWS Service Screener v2

01.
A



17+ AWS 주요
서비스에 대한
핵심 설정 점검 지원

02.
B



**AWS Well-
Architected
Framework** 보완

03.
C



CloudShell 기반 실행,
결과는 **대시보드 형태**
보고서로 출력

• What is AWS Service Screener v2

CloudShell

us-east-1 +

COMPLETED

--

LAM::us-east-1

(46.716s)

PREPARING

--

RDS::us-east-1

(1.637s)

COMPLETED

--

RDS::us-east-1

(1.637s)

PREPARING

--

RDS::ap-northeast-2

(2.921s)

COMPLETED

--

RDS::ap-northeast-2

(2.921s)

[info] Empty CF stacked deleted successfully, name:ssv2-9ae80d775375

Total Resources scanned: 290.00 | No. Rules executed: 837.00

Time consumed (seconds): 52.305

ElasticcachepageBuilder class not found, using default pageBuilder

RedshiftpageBuilder class not found, using default pageBuilder

CloudfrontpageBuilder class not found, using default pageBuilder

EfspaceBuilder class not found, using default pageBuilder

CloudwatchpageBuilder class not found, using default pageBuilder

OpensearchpageBuilder class not found, using default pageBuilder

RdspageBuilder class not found, using default pageBuilder

EkspageBuilder class not found, using default pageBuilder

DynamodbpageBuilder class not found, using default pageBuilder

Ec2pageBuilder class not found, using default pageBuilder

S3pageBuilder class not found, using default pageBuilder

CloudtrailpageBuilder class not found, using default pageBuilder

IampageBuilder class not found, using default pageBuilder

LambdapageBuilder class not found, using default pageBuilder

KmspageBuilder class not found, using default pageBuilder

ApigatewaypageBuilder class not found, using default pageBuilder

... Running CP - TA, it can takes up to 60 seconds

Error: TA unable to generate. Access denied due to support level

Pages generated, download **output.zip** to view

CloudShell user, you may use this path: **====>** /tmp/service-screener-v2/output.zip **<=====**

@ Thank you for using Service Screener, script spent 54.117s to complete @

(tmp) [cloudshell-user@ip-10-132-51-72 service-screener-v2]\$

Actions ▲

us-east-1 environment actions

New tab

Split into rows

Split into columns

Upload file

Download file

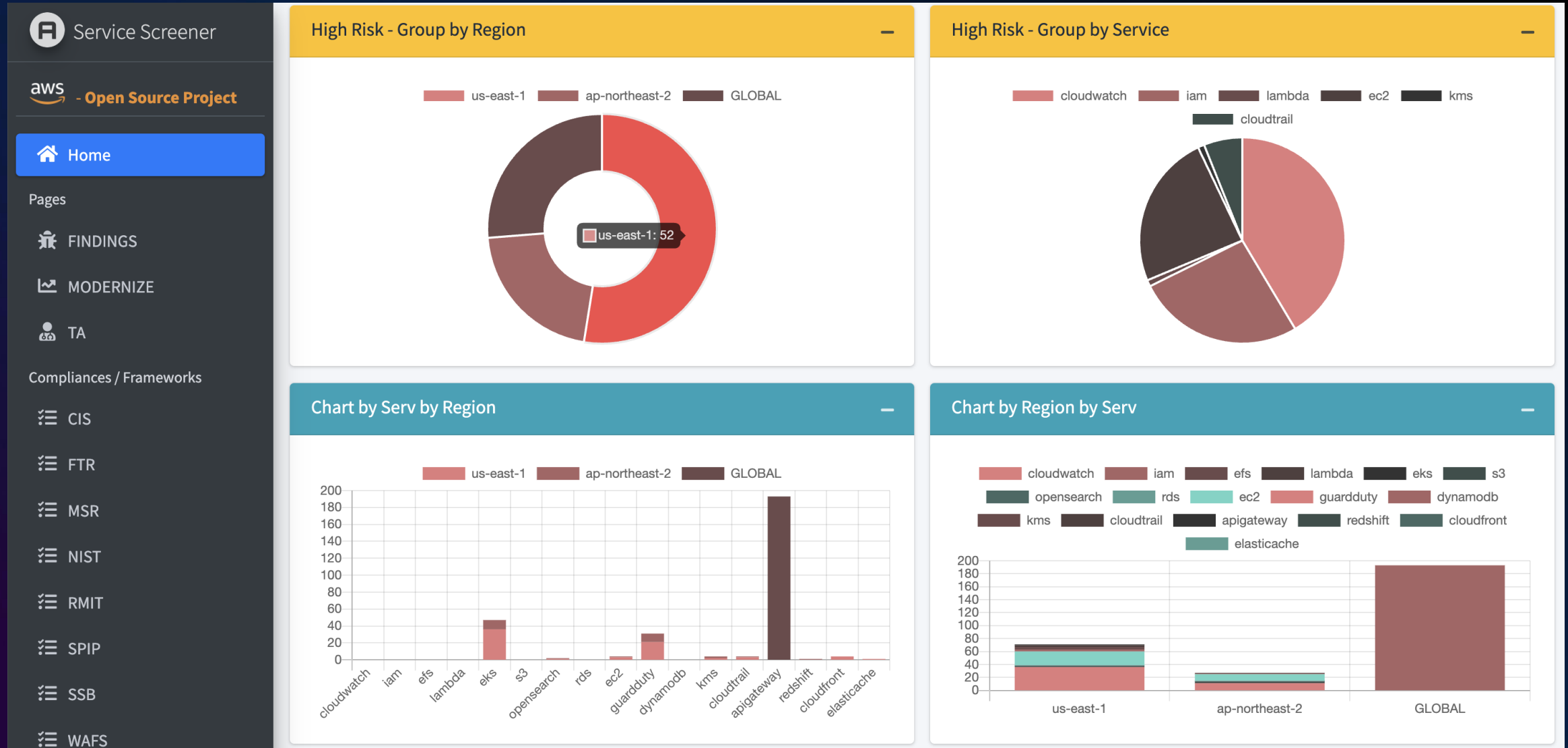
Restart

Delete


Global actions


Create VPC environment (max 2)

• What is AWS Service Screener v2



• What is AWS Service Screener v2

 Service Screener

 - Open Source Project

Home

Pages

FINDINGS

MODERNIZE

TA

Compliances / Frameworks

CIS

FTR

MSR

NIST

RMIT

SPIP

SSB

WAFS

CPFINDINGS

Findings


Show 50 entries


Search:

Copy CSV Column visibility

Service	Region	Check	Type	ResourceID	Severity
+ APIGATEWAY	us-east-1	EncryptionInTransit	Security	REST::serverless-app	Medium
+ APIGATEWAY	us-east-1	WAFWACL	Security	REST::serverless-app	Medium
+ APIGATEWAY	us-east-1	XRayTracing	Security	REST::serverless-app	Medium
+ CLOUDTRAIL	us-east-1	EnableTrailS3BucketMFADelete	Security	Cloudtrail::IAMAAPolGenTrail	High
+ CLOUDTRAIL	us-east-1	EnableTrailS3BucketVersioning	Reliability	Cloudtrail::IAMAAPolGenTrail	High
+ CLOUDTRAIL	us-east-1	EnableTrailS3BucketLogging	Reliability	Cloudtrail::IAMAAPolGenTrail	High
+ CLOUDTRAIL	us-east-1	EnableTrailS3BucketLifecycle	Cost Optimization	Cloudtrail::IAMAAPolGenTrail	Medium
+ CLOUDTRAIL	us-east-1	SetupSNSTopicForTrail	Operation Excellence	Cloudtrail::IAMAAPolGenTrail	Low


• What is AWS Service Screener v2


 Service Screener


 - Open Source Project

Home


Pages


 FINDINGS


 MODERNIZE


 TA


Compliances / Frameworks


 CIS


 FTR


 MSR

 NIST

 RMIT

 SPIP

 SSB






 WAFS

Framework: CIS Amazon Web Services Foundations Benchmark

Show entries

Search:

Copy CSV Column visibility

Category 	Rule ID 	Compliance Status 	Description 	Reference 
CloudTrail.	1	Compliant	✓ [NeedToEnableCloudTrail] ✓ [HasOneMultiRegionTrail]	
CloudTrail.	2	Need Attention	✗ [RequiresKmsKey] - Enable SSE • [us-east-1]Cloudtrail::management-events	Encrypt CloudTrail using AWS KMS CloudTrail Security Best Practices
CloudTrail.	4	Need Attention	✗ [LogFileValidationEnabled] - Enable CloudTrail log file integrity • [us-east-1]Cloudtrail::management-events	What is log file integrity Enable Log file integrity
CloudTrail.	5	Need Attention	✗ [CloudWatchLogsLogGroupArn] - CloudWatch for CloudTrail • [us-east-1]Cloudtrail::IAMAPolGenTrail	Using CloudWatch Logs with CloudTrail
CloudTrail.	6	Compliant	✓ [EnableS3PublicAccessBlock]	

• What is AWS Service Screener v2

Service Screener

References

APIGATEWAY

CLOUDFRONT

CLOUDTRAIL

CLOUDWATCH

DYNAMODB

EC2

EFS

EKS

ELASTICACHE

GUARDDUTY

IAM

KMS

LAMBDA

OPENSEARCH

RDS

Filter

Checks

Select checks...

Pillar

All

Criticality

All

☐ Show low hanging fruit(s) only

☐ Expand / ☒ Hide all cards

disabledBackupReliability ⚠️ +

deleteTableProtectionReliability ⚠️ +

disabledPointInTimeRecoveryReliability ⚠️ +

resourcesWithoutTagsCost Optimization 👁️ +

disabledTTLCost Optimization 👁️ +

attributeNamesXLCost Optimization 👁️ +

Detail

us-east-1

1. GuardDuty-Example-Customer-DBDynamodb

Check	Current Value	Recommendation
⚠️ disabledBackup		Table does not have backup.
⚠️ deleteTableProtection		Delete table protection is disabled.

2. aws-security-hub-automated-response-and-remediation-admin-SchedulingTable1EC09B43-1HZ6UEPFWDTYCDynamodb

Check	Current Value	Recommendation
attributeNamesXL	AccountID-Region	Attributes name longer than 15 characters.



- Use Case - Prowler



배포된 **AWS 리소스 설정**을 신속 스캔하여
보안 취약 구성 식별

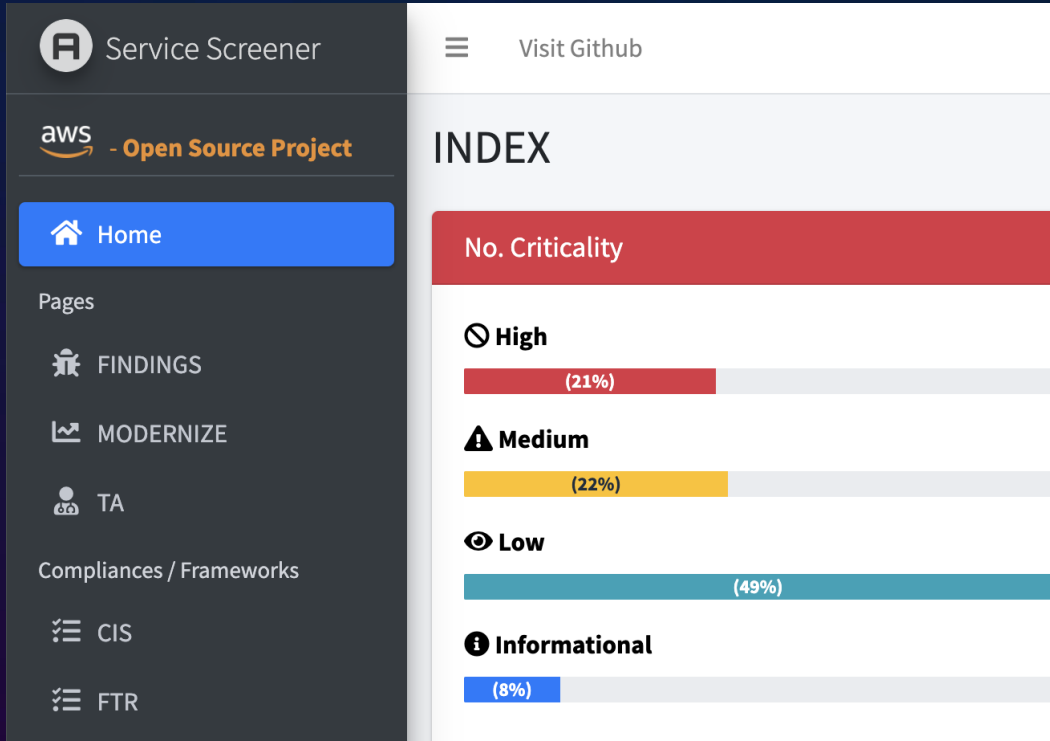
.....

CI/CD 파이프라인의 한 단계로 통합 가능
(예: 배포 후 스캔)

.....

지속적 활용: 일정 주기마다 **자동 재점검**
(예: 매일 또는 매주)

• Use Case – Service Screener V2



정기 진단: 전체 AWS 계정에 대해 종합 점검 실시

다각도 분석: 보안뿐 아니라 현대화 필요 영역,
비용 최적화, 운영 우수성도 점검

리포트 활용: 쉽게 만드는 대시보드/리포트로 보고 용이



보안의 수준은 관심의 수준과 동일하다.

Thank you!

