



Prowler

Opensource Security Tool

AWS ProServe – Choi, Jaewook

2023.03.23



Disclaimer

Disclaimers. The following applies to this document and all other documents, information, data, and responses (written or verbal) provided by Amazon Web Services, Inc. or any of its affiliates (collectively, "AWS") in connection with responding to this request and other related requests (collectively, this "Response"): This Response is expressly (a) informational only and provided solely for discussion purposes, (b) non-binding and not an offer to contract that can be accepted by any party, (c) provided "as is" with no representations or warranties whatsoever, and (d) based on AWS's current knowledge and may change at any time due to a variety of factors such as changes to your requirements or changes to AWS's service offerings. All obligations must be set forth in a separate, definitive written agreement between the parties. Neither party will have any liability for any failure or refusal to enter into a definitive agreement. All use of AWS's service offerings will be governed by the AWS Customer Agreement available at <http://aws.amazon.com/agreement/> (or other definitive written agreement between the parties governing the use of AWS's service offerings) (as applicable, the "Agreement"). If the parties have an applicable Nondisclosure Agreement ("NDA"), then the NDA will apply to all Confidential Information (as defined in the NDA) disclosed in connection with this Response. AWS's pricing is publicly available and subject to change in accordance with the Agreement. Pricing information (if any) provided in this Response is only an estimate and is expressly not a binding quote. Fees and charges will be based on actual usage of AWS services, which may vary from the estimates provided. Nothing in this Response will modify or supplement the terms of the Agreement or the NDA. No part of this Response may be disclosed without AWS's prior written consent.

Contents

Prowler 소개

Prowler IAM Policies

Scanning to EC2

Scanning to CodeBuild

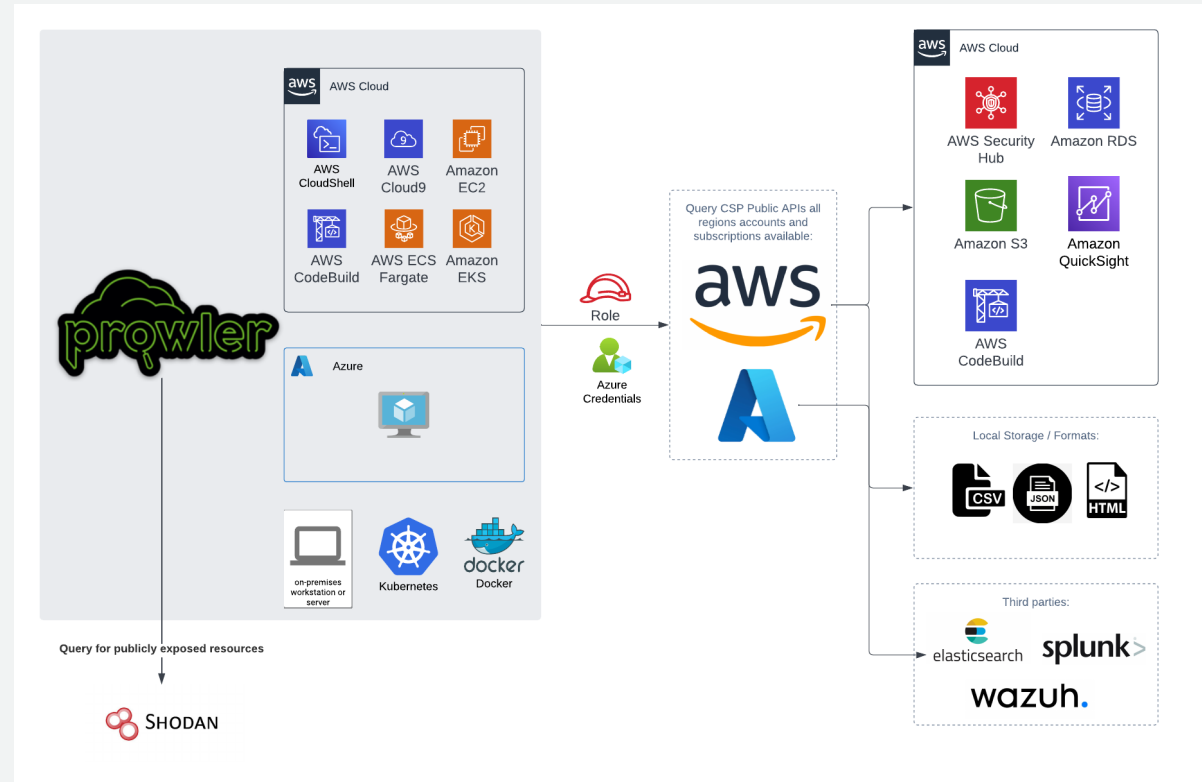
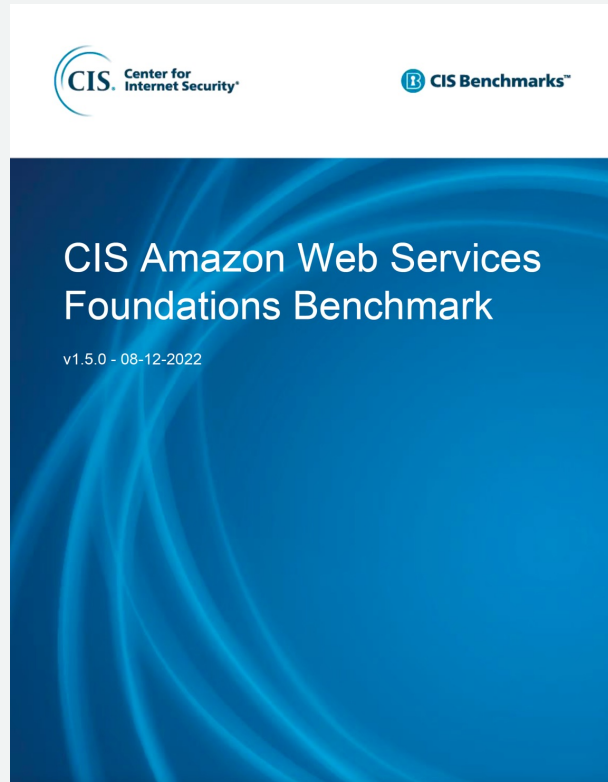
Visualization

Prowler 소개

Prowler 소개

Prowler는 AWS 및 Azure 보안 모범 사례 평가, 감사, 사고 대응, 지속적인 모니터링, 강화 및 포렌식 준비를 수행하는 오픈 소스 보안 도구입니다.

- Prowler는 CIS, PCI-DSS, ISO27001, GDPR, HIPAA, FFIEC, SOC2, AWS FTR, ENS 및 사용자 지정 보안 프레임워크를 다루는 수백 가지 컨트롤이 포함되어 있습니다.



Prowler 소개

버전 비교

	Version 2	Version 3
Compliance	CIS Level1, CIS Level2, FFIEC, HIPPA, PCI, SOC2, CIS Implementation Group2, ISO 27001	cis_1.4, cis_1.5, ens_rd2022, aws_audit_manager_control_tower_guardrails, aws_foundational_security_best_practices, cisa, fedramp_low_revision_4, fedramp_moderate_revision_4, ffiec, gdpr, gxp_eu_annex_11, gxp_21_cfr_part_11, hipaa, nist_800_53_revision_4, nist_800_53_revision_5, nist_800_171_revision_2, nist_csf_1.1, pci_3.2.1, rbi_cyber_security_framework, soc2
결과 지원 형식	text, mono, csv, json, json-asff, junit-xml, html	csv, json, json-asff, html
결과 저장소	Local, S3 Bucket, Security Hub, DB	Local, S3 Bucket, Security Hub, DB
Multi Account 지원	가능	가능
Inventory 출력	가능	가능
예외처리	가능	가능
Container	가능	가능

Prowler IAM Policies

Prowler IAM Policies

필수 & 추가 IAM Policies

Prowler를 실행하기 위해 아래의 2가지 AWS Managed IAM Policy가 필수적으로 필요합니다.

- **arn:aws:iam::aws:policy/SecurityAudit**
- **arn:aws:iam::aws:policy/job-function/ViewOnlyAccess**

정확한 점검을 위해 다음과 같은 추가 IAM Policy가 필요합니다.

- [prowler-additions-policy.json](#)

만약 점검 결과를 AWS Security Hub에 보내고자 한다면,
다음과 같은 IAM Policy가 필요합니다.

- [prowler-security-hub.json](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:GetFindings"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

< prowler-security-hub.json >

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "account:Get*",
        "appstream:Describe*",
        "appstream:List*",
        "codeartifact:List*",
        "codebuild:BatchGet*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ec2:GetEbsEncryptionByDefault",
        "ecr:Describe*",
        "elasticfilesystem:DescribeBackupPolicy",
        "glue:GetConnections",
        "glue:GetSecurityConfiguration*",
        "glue:SearchTables",
        "lambda:GetFunction*",
        "macie2:GetMacieSession",
        "s3:GetAccountPublicAccessBlock",
        "shield:DescribeProtection",
        "shield:GetSubscriptionState",
        "ssm:GetDocument",
        "support:Describe*",
        "tag:GetTagKeys"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowMoreReadForProwler"
    },
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET"
      ],
      "Resource": [
        "arn:aws:apigateway:*::/restapis/*"
      ]
    }
  ]
}
```

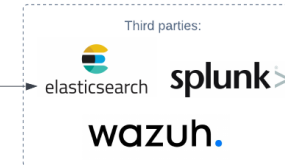
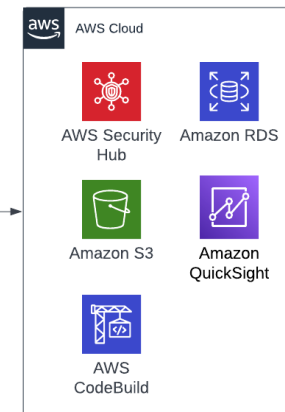
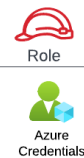
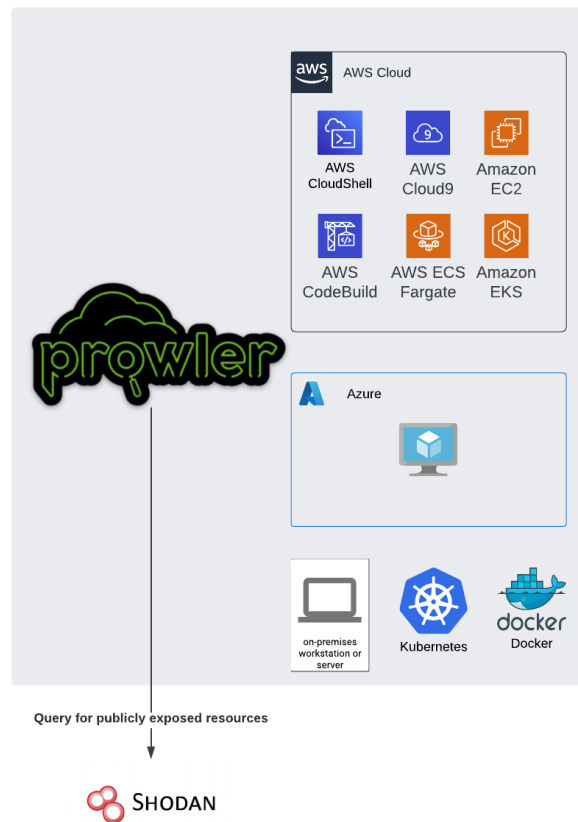
< prowler-additionas-policy.json >

Prowler IAM Policies

점검 대상에 IAM Role 생성

점검 수행 Account와 점검 대상 Account가 동일한 경우, 아래 Code로 CloudFormation 스택 생성

```
AWSTemplateFormatVersion: '2010-09-09'
Description: |
  This template creates an AWS IAM Role with an inline policy and two AWS
  attached for security assessment
Parameters:
  ProwlerRoleName:
    Description: |
      Name of the IAM role that will have these policies attached. Default
    Type: String
    Default: 'ECSAProwlerRole'
Resources:
  ECSProwlerRole:
    Type: AWS::IAM::Role
    Properties:
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/SecurityAudit'
        - 'arn:aws:iam::aws:policy/job-function/ViewOnlyAccess'
      RoleName: 'Sub ${ProwlerRoleName}'
      Policies:
        - PolicyName: ProwlerExecRoleAdditionalViewPrivileges
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
                  - 'account:Get*'
                  - 'appstream:DescribeFleets'
                  - 'codeartifact:ListRepositories'
                  - 'codebuild:BatchGetBuilds'
                  - 'ds:Get*'
                  - 'ds:Describe*'
                  - 'ds:List*'
                  - 'ec2:GetEbsEncryptionByDefault'
                  - 'ecr:Describe*'
                  - 'elasticfilesystem:DescribeBackupPolicy'
                  - 'glue:GetConnections'
                  - 'glue:GetSecurityConfiguration'
                  - 'glue:SearchTables'
                  - 'lambda:GetFunction'
                  - 'media2:GetMediaSession'
                  - 's3:GetAccountPublicAccessBlock'
                  - 's3:GetEncryptionConfiguration'
                  - 's3:GetBucketPublicAccessBlock'
                  - 'shield:DescribeProtection'
                  - 'shield:GetSubscriptionState'
                  - 'ssm:GetDocument'
                  - 'support:Describe*'
                  - 'tag:GetTagKeys'
                Resource: '*'
              - Effect: Allow
                Action:
                  - 'apigateway:GET'
                Resource: 'arn:aws:apigateway:*::/restapis/*'
              - Effect: Allow
                Action:
                  - 'securityhub:BatchImportFindings'
                  - 'securityhub:GetFindings'
                Resource: '*'
```



생성 > 템플릿 파일 업로드 > 파일 업로드

Create template in Designer

le-customer.yaml View In Designer

Cancel Next

이름) 입력

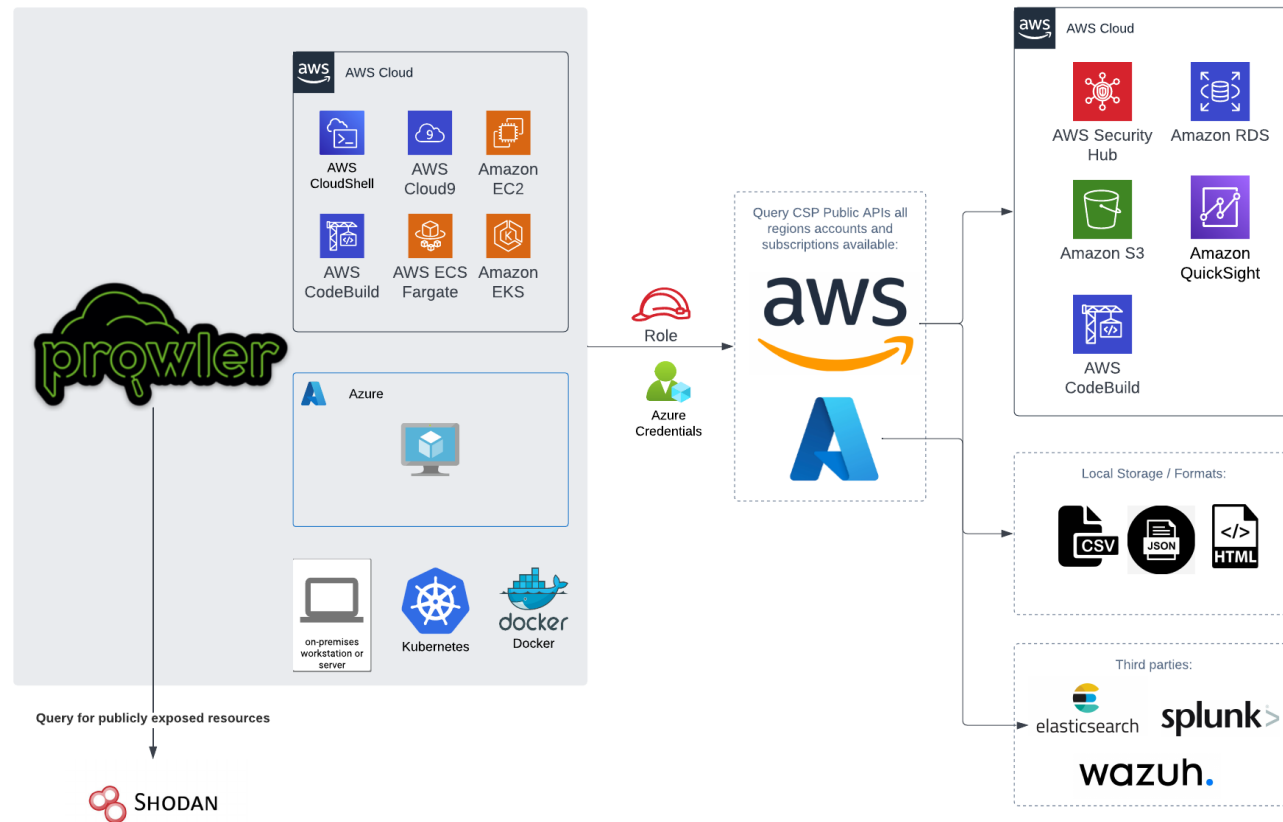
고 그러한 리소스가 필요한 최소 권한을 가지고 있는지 확인합니다. 또 자세히 알아보기

Prowler IAM Policies

점검 대상에 IAM Role 생성

점검 수행 Account와 점검 대상 Account가 다른 경우, 점검 대상 Account에 아래 Code로 CloudFormation 스택 생성

```
AWSTemplateFormatVersion: '2010-09-09'
Description: |
  This template creates an AWS IAM Role with an inline policy and two AWS managed pol
  attached for security assessment
Parameters:
  ProwlerRoleName:
    Description: |
      Name of the IAM role that will have these policies attached. Default: ECSAProwler
    Type: String
    Default: 'ECSAProwlerRole'
Resources:
  ECSAProwlerRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              AWS: arn:aws:iam::{{account_id}}:root
            Action: 'sts:AssumeRole'
      MaxSessionDuration: 43200
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/SecurityAudit'
        - 'arn:aws:iam::aws:policy/job-function/ViewOnlyAccess'
      RoleName: !Sub ${ProwlerRoleName}
    Policies:
      - PolicyName: ProwlerExecRoleAdditionalViewPrivileges
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
            - Effect: Allow
              Action:
                - 'account:Get*'
                - 'appstream:DescribeFleets'
                - 'codeartifact:ListRepositories'
                - 'codebuild:BatchGetBuilds'
                - 'ds:Get*'
                - 'ds:Describe*'
                - 'ds:List*'
                - 'ec2:GetEbsEncryptionByDefault'
                - 'ecr:Describe*'
                - 'elasticfilesystem:DescribeBackupPolicy'
                - 'glue:GetConnections'
                - 'glue:GetSecurityConfiguration'
                - 'glue:SearchTables'
                - 'lambda:GetFunction'
                - 'macie2:GetMacieSession'
                - 's3:GetAccountPublicAccessBlock'
                - 's3:GetEncryptionConfiguration'
                - 's3:GetBucketPublicAccessBlock'
                - 'shield:DescribeProtection'
                - 'shield:GetSubscriptionState'
                - 'ssm:GetDocument'
                - 'support:Describe*'
                - 'tag:GetTagKeys'
              Resource: '*'
            - Effect: Allow
              Action:
                - 'apigateway:GET'
              Resource: 'arn:aws:apigateway:*::/restapis/*'
            - Effect: Allow
              Action:
                - 'securityhub:BatchImportFindings'
                - 'securityhub:GetFindings'
              Resource: '*'
```



Role을 생성

"ProwlerRole",
"ProwlerRole",
"ProwlerRole",
"ProwlerRole"

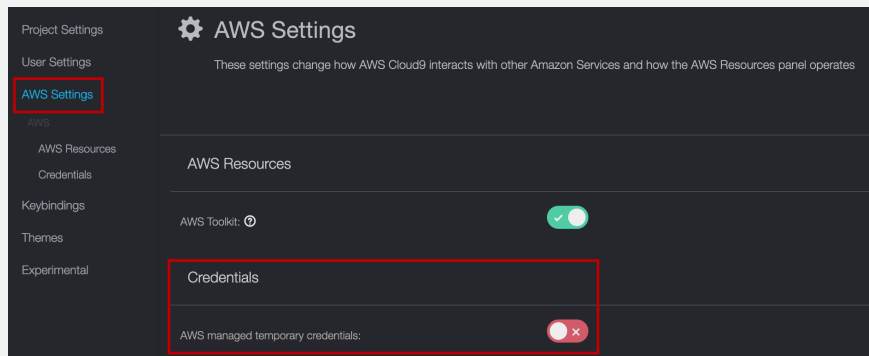
Account ID

Scanning to EC2

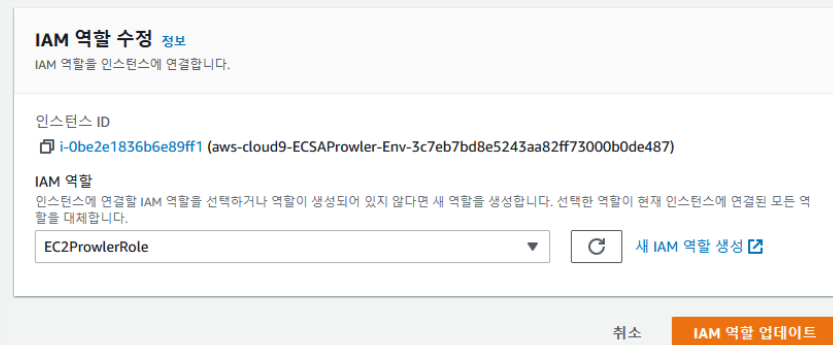
Scanning to EC2

Version 2 - 점검 환경 생성 및 점검 실행

1. Cloud9 생성 및 임시 자격증명 비활성화



2. EC2 > Cloud9 인스턴스 우클릭 > 보안 > IAM 역할 수정 > 생성한 IAM Role로 수정



3. Cloud9 접속 후, 아래 Command로 Prowler v2.12.1 설치

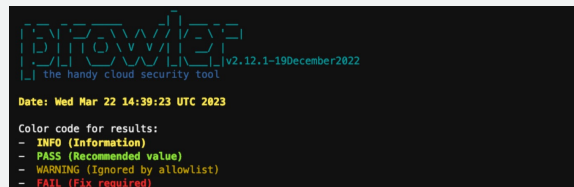
```
sudo yum install -y python3 jq git
sudo pip3 install detect-secrets==1.0.3
sudo curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
sudo unzip awscliv2.zip
sudo ./aws/install -b /bin --update
sudo git clone https://github.com/prowler-cloud/prowler
cd prowler
sudo git checkout 2.12.1
```

4. 점검 수행

```
sudo ./prowler -A {점검 대상 Account ID} -R {점검 대상 IAM Role 이름} -M {결과 형식 지정} &
```

주요 옵션

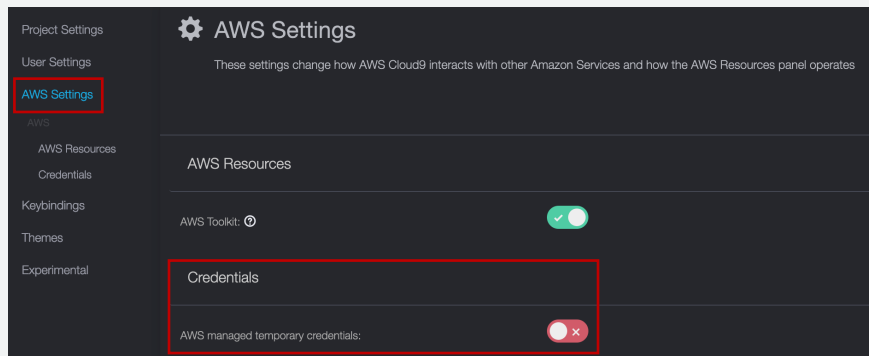
-A : 점검 대상 Account ID	-B : S3 Bucket 저장
-R : 사용할 Role	-l : 점검 항목 출력
-M : 출력 결과 형식	-f : 특정 리전 선택
-i : Inventory 스캔	-S : Security Hub에 결과 전송



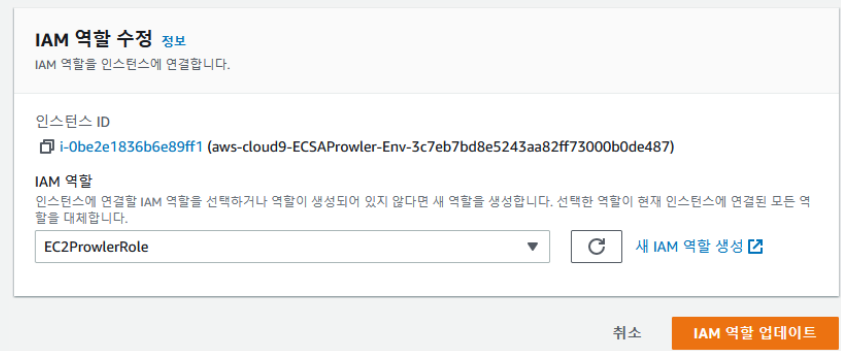
Scanning to EC2

Version 3 - 점검 환경 생성 및 점검 실행

1. Cloud9 생성 및 임시 자격증명 비활성화



2. EC2 > Cloud9 인스턴스 우클릭 > 보안 > IAM 역할 수정 > 생성한 IAM Role로 수정



3. Cloud9 접속 후, 아래 Command로 Prowler v3 설치

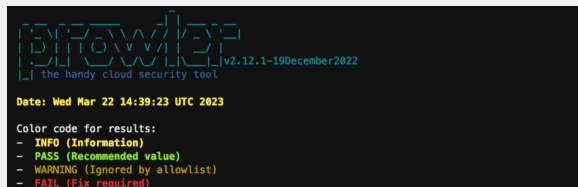
```
sudo yum install -y gcc openssl-devel bzip2-devel libffi-devel
wget https://www.python.org/ftp/python/3.9.16/Python-3.9.16.tgz
tar xf Python-3.9.16.tgz
cd Python-3.9.16
./configure --enable-optimizations
sudo make altinstall
pip3.9 install prowler
```

4. 점검 수행

```
prowler -R arn:aws:iam::<점검 대상 Account ID>:role/< 점검 대상 IAM Role 이름 > -M {결과 형식 지정}
```

주요 옵션

-R : 점검 대상 Role	-l : 점검 항목 출력
-M : 출력 결과 형식	-f : 특정 리전 선택
-i : Inventory 스캔	-S : Security Hub에 결과 전송
-B : S3 Bucket 저장	



Scanning to CodeBuild

Scanning to CodeBuild

점검 환경 생성 및 점검 실행

1. CodeBuild > 빌드 > 프로젝트 빌드 > 빌드 프로젝트 생성 > 프로젝트 이름 입력

빌드 프로젝트 생성

프로젝트 구성

프로젝트 이름

ProwlerCodeBuild

프로젝트 이름은 2~255자여야 합니다. 글자(A-Z 및 a-z), 숫자(0-9) 및 특수 문자(- 및 _)를 포함할 수 있습니다.

2. 소스 공급자 > 소스 없음

소스

소스 추가

소스 1 - 기본

소스 공급자

소스 없음

3. 환경 설정

운영 체제: Amazon Linux 2

런타임: Standard

이미지: aws/codebuild/amazonlinux2-x86_64-standard:3.0

이미지 버전: 이 런타임 버전에 항상 최신 이미지 사용

환경 유형: Linux

환경

환경 이미지

☒ 관리형 이미지
AWS CodeBuild에서 관리하는 이미지 사용

☐ 사용자 지정 이미지
도커 이미지 지정

운영 체제

Amazon Linux 2

이제 프로그래밍 언어 런타임은 Ubuntu 18.04의 표준 이미지에 포함됩니다. 이 이미지는 콘솔에서 생성된 새 CodeBuild 프로젝트에 대해 권장됩니다. 자세한 내용은 CodeBuild에서 제공하는 Docker 이미지 [을\(를\)](#) 참조하십시오.

런타임

Standard

이미지

aws/codebuild/amazonlinux2-x86_64-standard:3.0

이미지 버전

이 런타임 버전에 항상 최신 이미지 사용

환경 유형

Linux

Visualization

Visualization

Security Hub

Security Hub > 분석 결과

리전: 연결된 모든 리전

분석 결과 (20+)

보안 문제나 실패한 보안 검사가 분석 결과로 표시됩니다.

회사 이름 일치함 Prowler

워크플로 상태 일치함 NEW

워크플로 상태 일치함 NOTIFIED

레코드 상태 일치함 ACTIVE

필터 추가

☐	심각도	워크플로 상태	레코드 상태	리전	회사	제품	제목	리소스	규정 준수 상태	업데이트 시간
☐	MEDIUM	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find obsolete Lambda runtimes.	Lambda 함수 access-analyzer-list-iam-policy	PASSED	몇 초 전
☐	MEDIUM	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find obsolete Lambda runtimes.	Lambda 함수 LambdaFunctionEnableProwlerIntegration	PASSED	몇 초 전
☐	CRITICAL	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find secrets in Lambda functions variables.	Lambda 함수 LambdaFunctionKdfTransformation	PASSED	몇 초 전
☐	CRITICAL	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find secrets in Lambda functions variables.	Lambda 함수 LambdaFunctionEnableProwlerIntegration	PASSED	몇 초 전
☐	CRITICAL	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find secrets in Lambda functions code.	Lambda 함수 ProwlerCodeBuildQuickSigh-ProwlerScheduleLambdaFun-j5VrW41kP2jU	PASSED	몇 초 전
☐	LOW	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Check if Lambda functions invoke API operations are being recorded by CloudTrail.	Lambda 함수 ProwlerCodeBuildQuickSigh-LambdaFunctionExecuteQue-bo70ojIrmny	FAILED	몇 초 전
☐	LOW	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Check if Lambda functions invoke API operations are being recorded by CloudTrail.	Lambda 함수 ProwlerCodeBuildQuickSigh-ProwlerScheduleLambdaFun-j5VrW41kP2jU	FAILED	몇 초 전

Check if Lambda functions invoke API operations are being recorded by CloudTrail. ✕

Finding ID: prowler-awslambda_function_invoke_api_operations_cloudtrail_logging_enabled-066157043804-ap-northeast-2-186347295

■ LOW

Lambda function ProwlerCodeBuildQuickSigh-LambdaFunctionExecuteQue-bo70ojIrmny is not recorded by CloudTrail

워크플로 상태
신규

레코드 상태
ACTIVE
결과 공급자에 의해 설정됨

AWS 계정 ID
066157043804

규정 준수 상태
FAILED

생성 위치
2023-03-20T17:21:35Z

업데이트 시간
2023-03-22T16:01:23Z

제품 이름
Prowler

심각도 레이블
LOW

회사 이름
Prowler

▼ 리소스

리소스 detail
arn:aws:lambda:ap-northeast-2:066157043804:function:ProwlerCodeBuildQuickSigh-LambdaFunctionExecuteQue-bo70ojIrmny

리소스 유형
AwsLambdaFunction

리소스 리전
ap-northeast-2

리소스 ID
arn:aws:lambda:ap-northeast-2:066157043804:function:ProwlerCodeBuildQuickSigh-LambdaFunctionExecuteQue-bo70ojIrmny

▼ 수정

Make sure you are logging information about Lambda operations. Create a lifecycle and use cases for each trail.

▼ 분석 결과 공급자 필드

분석 결과 공급자 필드 detail
Finding Provider Field

공급자 심각도 레이블
LOW

Visualization

Athena Query – Data Catalog 생성하기 01

1. Glue > Data Catalog > Databases < Create database > database 이름 입력

[AWS Glue](#) > [Databases](#) > Add database

Create a database

Create a database in the AWS Glue Data Catalog.

Database details

Name

Enter a unique database name

Database name is required, in lowercase characters, and no longer than 255 characters.

Location - optional

Set the URI location for use by clients of the Data Catalog.

Description - optional

Enter text

Descriptions can be up to 2048 characters long.

Cancel

Create database

2. Glue > Data Catalog > Tables > Table 이름 입력

Set table properties

Table details

Name

Enter a unique name

If you plan to access the table from Amazon Athena, then the name should be under 256 characters and contain only lowercase letters (a-z), numbers (0-9), and underscore (_). For more information, see [Athena names](#).

Database

prowlerrresult

↺

Create database ↗

Description - optional

Enter a description

Descriptions can be up to 2048 characters long.

3. Data store: S3 선택 > 결과가 저장된 S3 선택

Data store

Select the type of source

☒ S3

☐ Kinesis

☐ Kafka

Data location is specified in

☒ my account

☐ another account

Include path

Q s3://bucket/prefix/

View ↗

Browse S3

Path must be in the form s3://bucket/prefix/. It must end with a slash (/) and not include any files.

4. Data format: CSV > Delimiter: Semicolon(;) 선택

Data format

Classification

Choose the format of the data in your table.

☐ Avro

☒ CSV

☐ JSON

☐ XML

☐ Parquet

☐ ORC

Delimiter

Semicolon (;)

Visualization

Athena Query – Data Catalog 생성하기 02

5. Edit schema as JSON 선택

Choose or define schema

Schema

☒ Define or upload schema
Manually define schema

☐ Choose from Glue Schema Registry
Select existing schema from your Glue Schema Registry.

Schema (0)

View and manage the table schema.

< 1 > ⚙

#	Column name	Data type	Partition key	Comment
No table schema				

Edit schema as JSON

Delete

Edit

Add

6. 아래 내용을 복사하고 Table 생성

```
[
  {
    "Name": "assessment_start_time",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "finding_unique_id",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "provider",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "check_id",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "check_title",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "check_type",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "status",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "status_extended",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "service_name",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "subservice_name",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "severity",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "resource_type",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "resource_details",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "resource_tags",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "description",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "risk",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "related_url",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "remediation_recommendation_text",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "remediation_recommendation_url",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "remediation_recommendation_code_nativeiac",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "remediation_recommendation_code_terraform",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "remediation_recommendation_code_cli",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "remediation_recommendation_code_other",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "compliance",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "categories",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "depends_on",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "related_to",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "notes",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "profile",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "account_id",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "account_name",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "account_email",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "account_arn",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "account_org",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "account_tags",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "region",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "resource_id",
    "Type": "string",
    "Comment": ""
  },
  {
    "Name": "resource_arn",
    "Type": "string",
    "Comment": ""
  }
]
```

Visualization

Athena Query – 조회

7. Athena에서 다음과 같이 필요에 따라 Query문을 수정하여 결과를 조회

```
SELECT
account_id, region, check_title, status, severity, resource_id,
resource_arn, compliance, risk, description
FROM "{Database 이름}"."{Table이름}"
limit 10;
```

Amazon Athena > Query editor

EditorRecent queriesSaved queriesSettings

Workgroupprimary

Data

Data source
AwsDataCatalog

Database
prowlerv3result

Tables and views
CreateFilter tables and views

▼ Tables (1)
prowler_v3_result_table

► Views (0)

Query 2Query 3

1 SELECT
2 account_id, region, check_title, status, severity, resource_id, resource_arn, compliance, risk, description
3 FROM "prowlerv3result"."prowler_v3_result_table"
4 limit 10;

SQLLn 4, Col 10

Run againExplainCancelClearCreate

Reuse query results
up to 60 minutes ago

Query resultsQuery stats

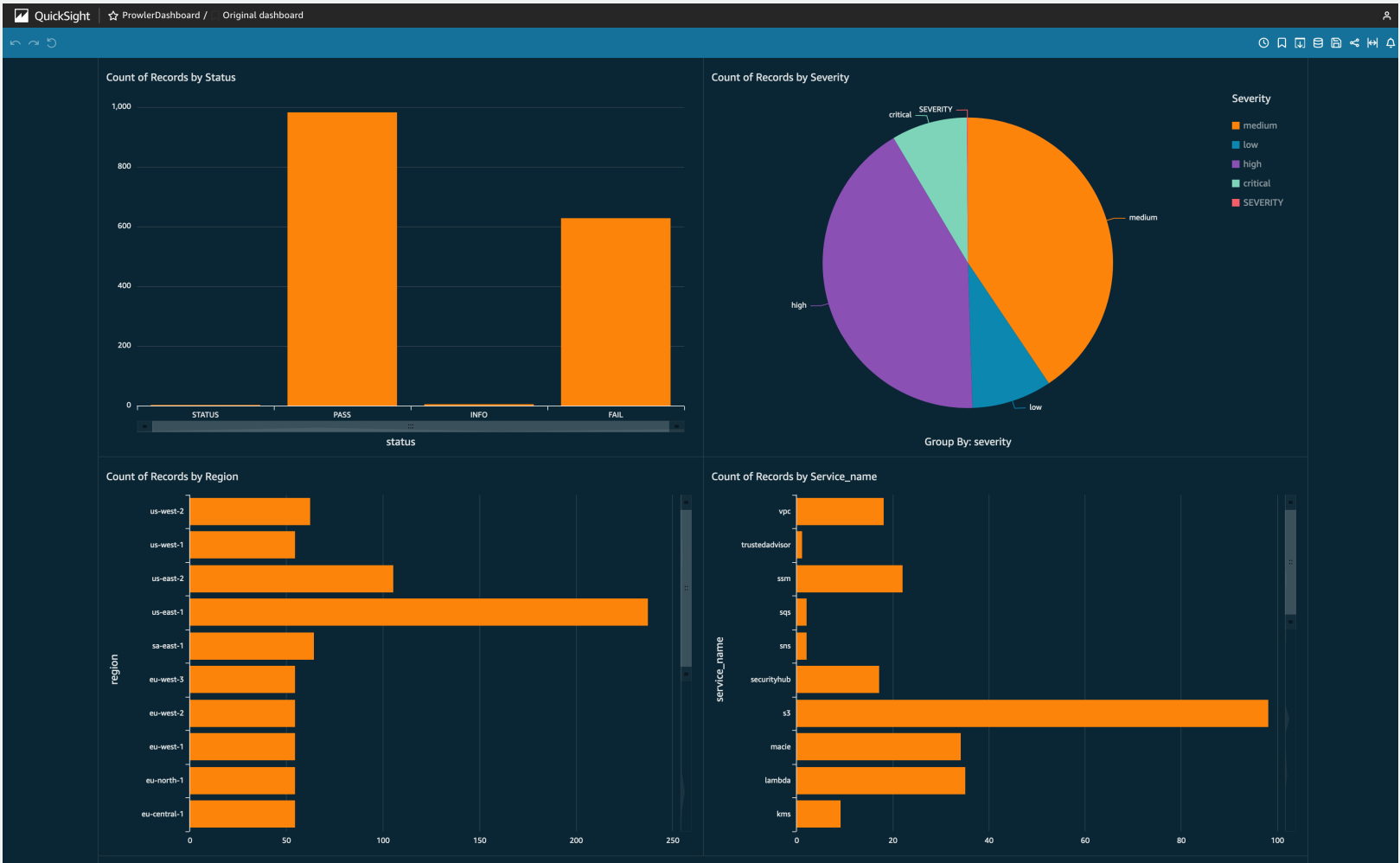
CompletedTime in queue: 104 msRun time: 567 msData scanned: 11.81 KB

Results (10)
Search rows

#	account_id	region	check_title	status	severity	resource_id	resource_arn	compliance	risk
1	ACCOUNT_ID	REGION	CHECK_TITLE	STATUS	SEVERITY	RESOURCE_ID	RESOURCE_ARN	COMPLIANCE	RISK
2	66157043804	ap-northeast-1	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
3	66157043804	ap-northeast-2	Check if Amazon Macie is enabled.	PASS	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
4	66157043804	ap-northeast-3	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
5	66157043804	ap-south-1	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
6	66157043804	ap-southeast-1	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
7	66157043804	ap-southeast-2	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
8	66157043804	ca-central-1	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
9	66157043804	eu-central-1	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz
10	66157043804	eu-north-1	Check if Amazon Macie is enabled.	FAIL	low	Macie		CIS-1.4: 2.1.4 CIS-1.5: 2.1.4	Amaz

Visualization

QuickSight Dashboard





Thank you!