



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

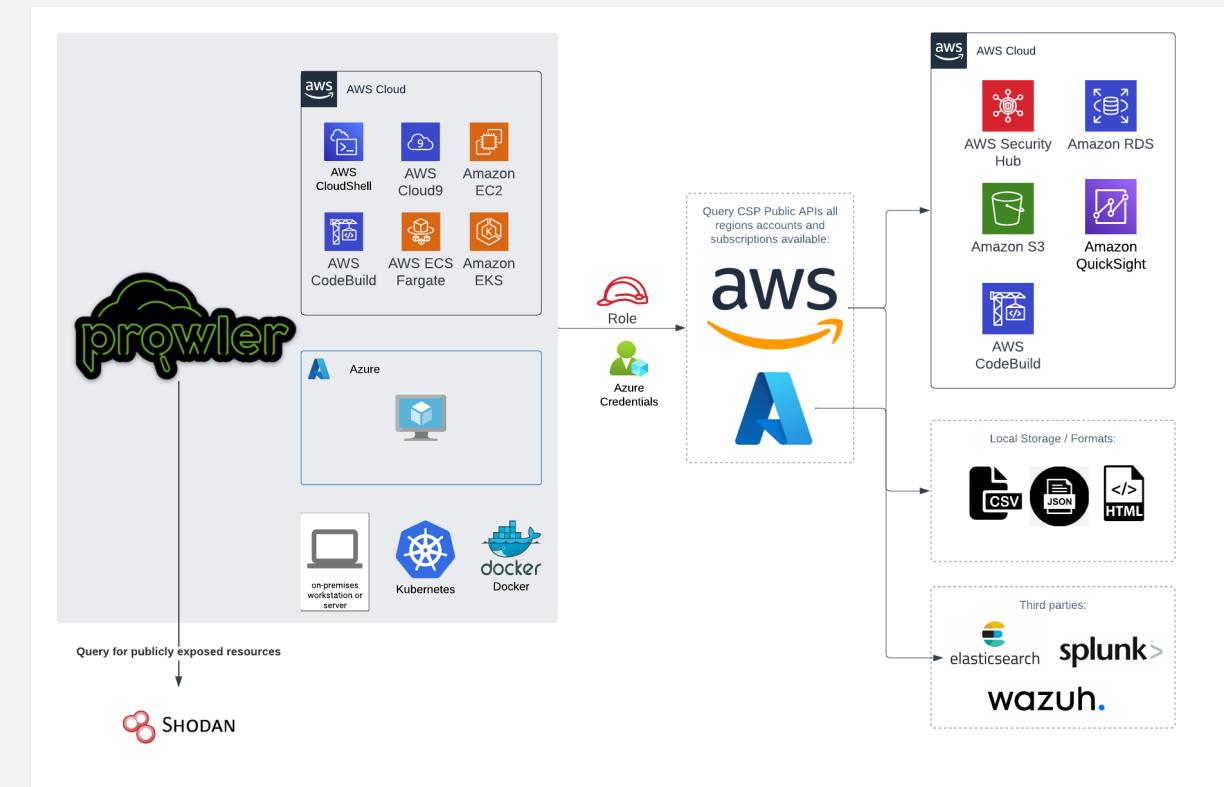
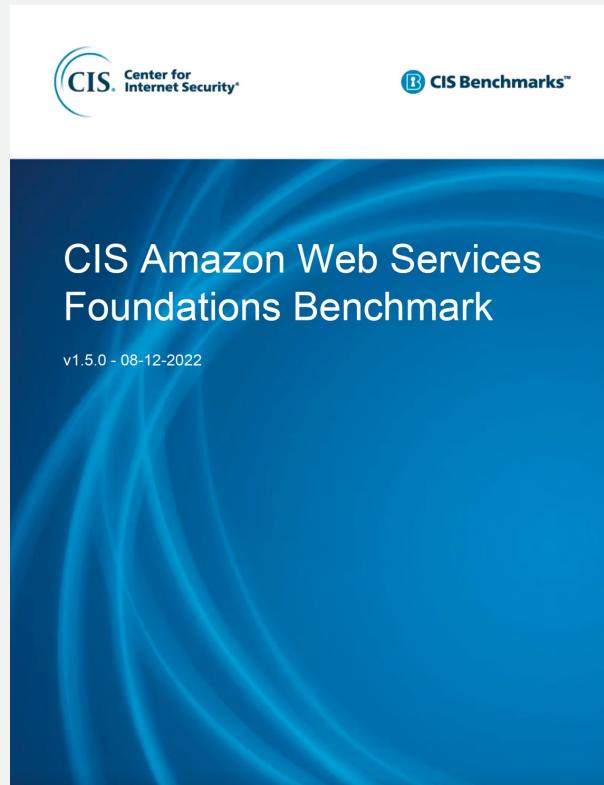
Prowler 소개



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:GetFunctions",
        "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/*"
      ]
    }
  ]
}
```

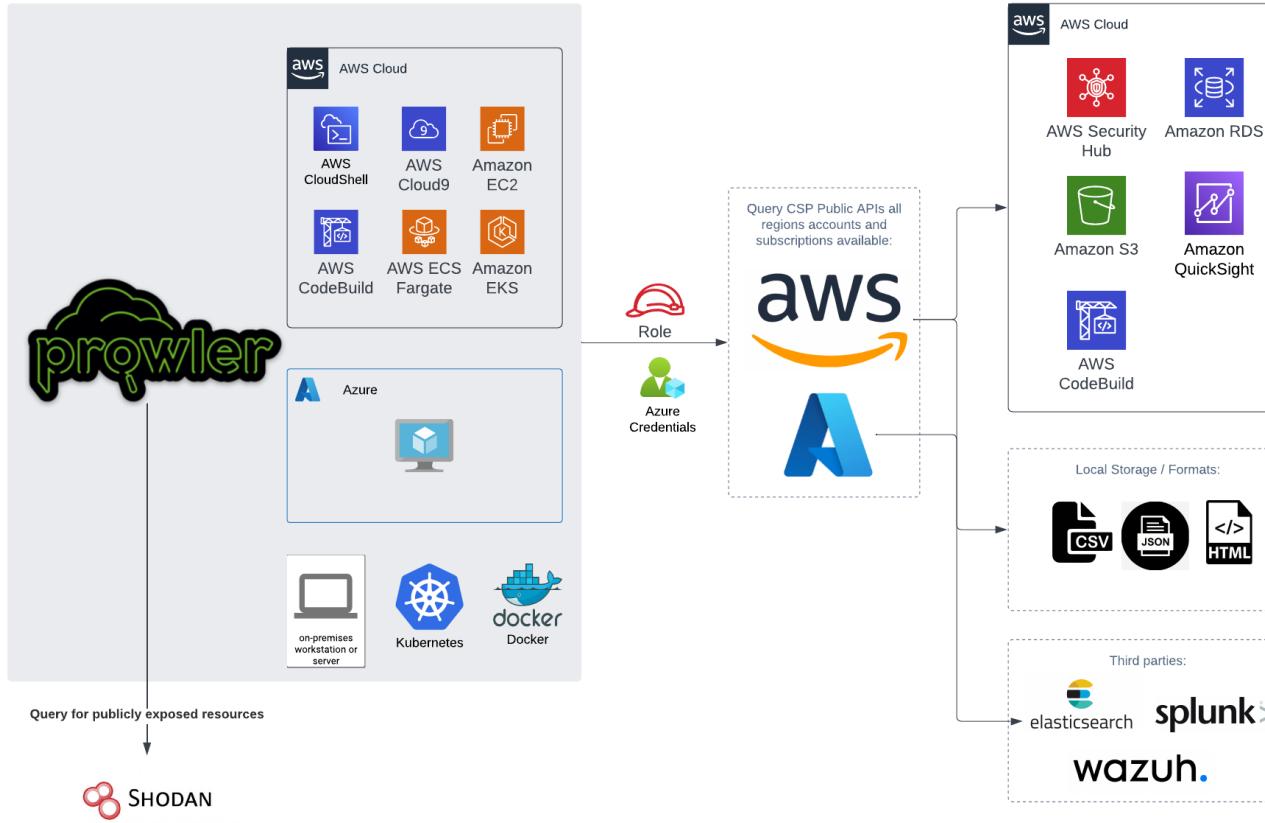
< prowler-additions-policy.json >

Prowler IAM Policies

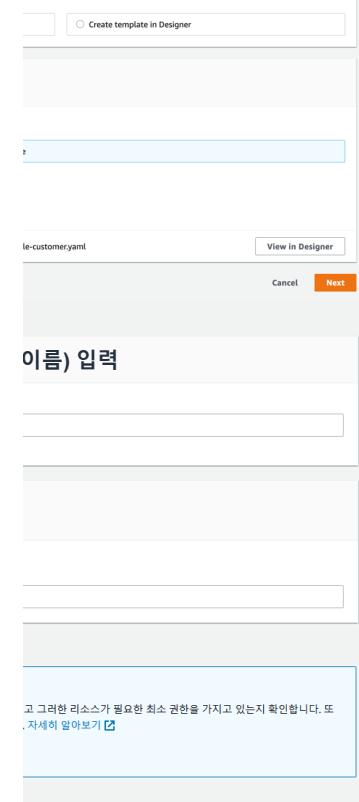
점검 대상에 IAM Role 생성

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
  managed policies attached for security assessment
Parameters:
  ProwlerRoleName:
    Description: |
      Name of the IAM role that will have these policies attached. Default:
      ECSProwlerRole
    Type: String
    Default: 'ECSProwlerRole'
Resources:
  ECSProwlerRole:
    Type: AWS::IAM::Role
    Properties:
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/SecurityAudit'
        - 'arn:aws:iam::aws:policy/JobFunctionViewOnlyAccess'
      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: '*'
```



생성 > 템플릿 파일 업로드 > 파일 업로드

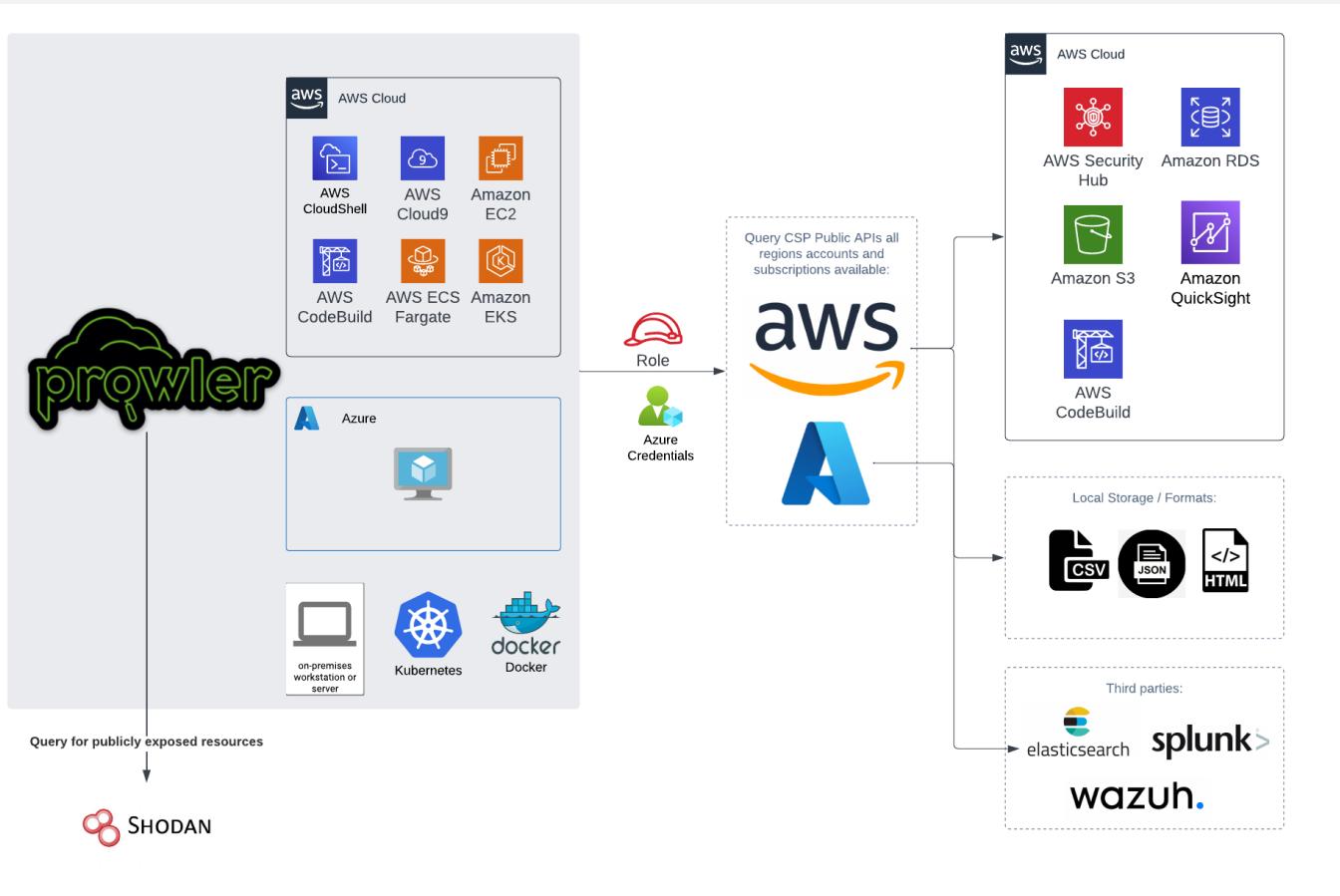


Prowler IAM Policies

점검 대상에 IAM Role 생성

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

```
AWS::TemplateFormatVersion: '2010-09-09'
Description: |
  This template creates an AWS IAM Role with an inline policy and two AWS managed policies attached for security assessment
Parameters:
  ProwlerRoleName:
    Description: |
      Name of the IAM role that will have these policies attached. Default: ECSAProwler
    Type: String
    Default: 'ECSAProwlerRole'
  Roles:
    ECSProwlerRole:
      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/JobFunctionViewOnlyAccess'
      RoleName: !Sub ${ProwlerRoleName}
    Policies:
      - PolicyName: ProwlerExecRoleAdditionalViewPrivileges
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
            - Effect: Allow
              Action:
                - 'account:Get*'
                - 'apstreamDescribeFleets'
                - 'codeartifact:listRepositories'
                - 'codebuild:BatchGetBuilds'
                - 'ds:Gets*'
                - 'ds:Describe*'
                - 'ds:Lists*'
                - 'ec2:GetTlsEncryptionByDefault'
                - 'ecr:Describes*'
                - 'elasticfilesystem:DescribeBackupPolicy'
                - 'glue:GetConnections'
                - 'glue:GetSecurityConfiguration'
                - 'glue:SearchTables'
                - 'lambda:GetFunction'
                - 'macie2:GetMapping'
                - 's3:GetAccountPublicAccessBlock'
                - 'ssm:GetEncryptionConfiguration'
                - 'ssm:PutPublicAccessBlock'
                - 'shield:DescribeProtection'
                - 'shield:GetSubscriptionState'
                - 'smi: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",
"ProwlerRole"

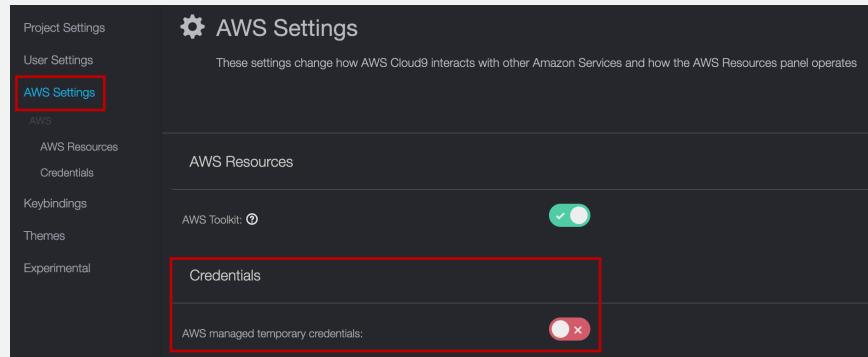
↑ Account ID

Scanning to EC2

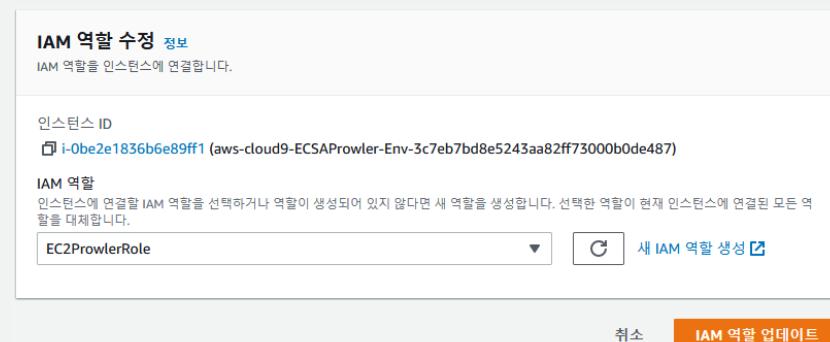
Scanning to EC2

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 설정



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} &
```



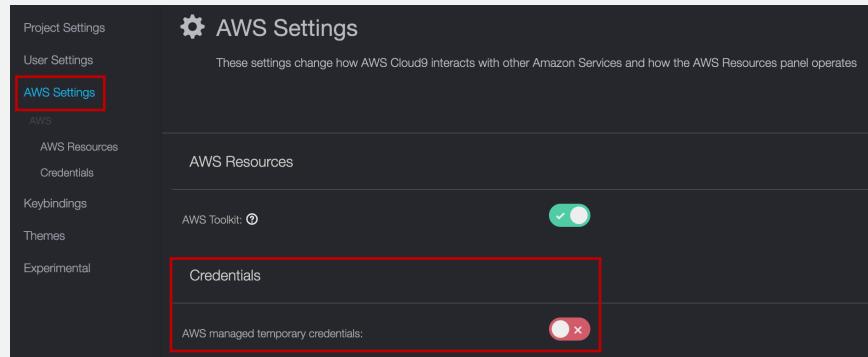
주요 옵션

-A : 점검 대상 Account ID	-B : S3 Bucket 저장
-R : 사용할 Role	-I : 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

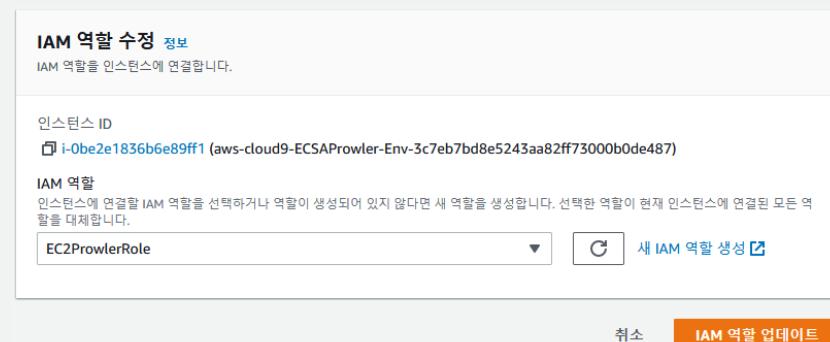
1. Cloud9 생성 및 임시 자격증명 비활성화



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
```

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



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	-I : 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 EC2

점검 결과물 샘플 (csv, html)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X								
1	PROFILE	ACCOUNT_ID	REGION	TITLE_ID	CHECK_RESU	ITEM_SCORE	ITEM_LEVEL	TITLE_TEXT	CHECK_RESU	CHECK_ASFF	CHECK_SERV	CHECK_ASFF	CHECK_ASFF	CHECK_RISK	CHECK_REME	CHECK_DOC	CHECK_CAF	CHECK_RESO	PROWLER_ST	ACCOUNT_DI	ACCOUNT_DI	ACCOUNT_DI	ACCOUNT_DI								
2	INSTANCE-PI	6.6157e+10	us-east-1	1.1 PASS	CIS Level 1	[check11] Av-us-east-1: Ro Software and High	iam	AwsAccount Software and The "root" ac: Follow the rei http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_root.html#root-access-to-a-specific-account	root	2023-03-20T15:55:20+0000																					
3	INSTANCE-PI	6.6157e+10	us-east-1	1.1 FAIL	CIS Level 1	[check110] Eu-us-east-1: Po Software and Medium	iam	AwsAccount Software and Password pol Ensure "Name":https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_password.html#password-policies-examples	password pol	2023-03-20T15:55:20+0000																					
4	INSTANCE-PI	6.6157e+10	us-east-1	1.1 FAIL	CIS Level 1	[check111] Eu-us-east-1: Po Software and Medium	iam	AwsAccount Software and Password pol Ensure "Path":https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_path.html#path-policies-examples	password pol	2023-03-20T15:55:20+0000																					
5	INSTANCE-PI	6.6157e+10	us-east-1	1.1 PASS	CIS Level 1	[check112] Eu-us-east-1: No Software and Critical	iam	AwsAccount Software and The root access Use the rei https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_root.html#root-access-to-a-specific-account	root access	2023-03-20T15:55:20+0000																					
6	INSTANCE-PI	6.6157e+10	us-east-1	1.1 PASS	CIS Level 1	[check113] Eu-us-east-1: No Software and Critical	iam	AwsAccount Software and The root access Use the rei https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_root.html#root-access-to-a-specific-account	root access	2023-03-20T15:55:20+0000																					
7	INSTANCE-PI	6.6157e+10	us-east-1	1.1 FAIL	CIS Level 2	[check114] Eu-us-east-1: Mi Software and Critical	iam	AwsAccount Software and The root accs Using IAM cc https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_root.html#root-access-to-a-specific-account	MFA	2023-03-20T15:55:20+0000																					
8	INSTANCE-PI	6.6157e+10	us-east-1	1.14 FAIL	CIS Level 2	[check114] Eu-us-east-1: Mi Software and Critical	iam	AwsAccount Software and The root accs Using IAM cc https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_root.html#root-access-to-a-specific-account	MFA	2023-03-20T15:55:20+0000																					
9	INSTANCE-PI	6.6157e+10	us-east-1	1.15 INFO	CIS Level 1	[check115] Eu-us-east-1: Ni Software and Medium	support	AwsAccount Software and The AWS sup L																							
10	INSTANCE-PI	6.6157e+10	us-east-1	1.16 PASS	CIS Level 1	[check116] Eu-us-east-1: Ni Software and Medium	support	AwsAccount Software and By default IAM	iam	AwsAccount User Software and By default IAM																					
11	INSTANCE-PI	6.6157e+10	us-east-1	1.17 PASS	CIS Level 1	[check117] Eu-us-east-1: No software or ac:3. Low	iam	AwsAccount User Software and By default IAM	iam	AwsAccount User Software and By default IAM																					
12	INSTANCE-PI	6.6157e+10	us-east-1	1.18 FAIL	CIS Level 1	[check118] Eu-us-east-1: Ac Software and Medium	support	AwsAccount Software and AWS provide C	ec2	AwsEc2Instan Software and AWS access f																					
13	INSTANCE-PI	6.6157e+10	ap-south-1	1.19 INFO	CIS Level 1	[check119] Eu-ap-south-1: S Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
14	INSTANCE-PI	6.6157e+10	eu-north-1	1.19 INFO	CIS Level 1	[check119] Eu-eu-north-1: S Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
15	INSTANCE-PI	6.6157e+10	eu-west-3	1.19 INFO	CIS Level 1	[check119] Eu-eu-west-3: S Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
16	INSTANCE-PI	6.6157e+10	eu-west-2	1.19 INFO	CIS Level 2	[check119] Eu-eu-west-2: N Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
17	INSTANCE-PI	6.6157e+10	eu-west-1	1.19 INFO	CIS Level 2	[check119] Eu-eu-west-1: N Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
18	INSTANCE-PI	6.6157e+10	ap-northeast-1	1.19 INFO	CIS Level 2	[check119] Eu-ap-northeast-1: Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
19	INSTANCE-PI	6.6157e+10	ap-northeast-1	1.19 PASS	CIS Level 2	[check119] Eu-ap-northeast-1: Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
20	INSTANCE-PI	6.6157e+10	ap-northeast-1	1.19 PASS	CIS Level 2	[check119] Eu-ap-northeast-1: Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
21	INSTANCE-PI	6.6157e+10	ca-central-1	1.19 INFO	CIS Level 2	[check119] Eu-ca-central-1: Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
22	INSTANCE-PI	6.6157e+10	ca-central-1	1.19 INFO	CIS Level 2	[check119] Eu-ca-central-1: Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
23	INSTANCE-PI	6.6157e+10	sa-east-1	1.19 INFO	CIS Level 2	[check119] Eu-sa-east-1: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
24	INSTANCE-PI	6.6157e+10	ap-southeast-1	1.19 INFO	CIS Level 2	[check119] Eu-ap-southeast-1: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
25	INSTANCE-PI	6.6157e+10	ap-southeast-1	1.19 INFO	CIS Level 2	[check119] Eu-ap-southeast-1: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
26	INSTANCE-PI	6.6157e+10	eu-central-1	1.19 INFO	CIS Level 2	[check119] Eu-eu-central-1: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
27	INSTANCE-PI	6.6157e+10	eu-central-1	1.19 INFO	CIS Level 2	[check119] Eu-eu-central-1: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
28	INSTANCE-PI	6.6157e+10	eu-west-1	1.19 INFO	CIS Level 2	[check119] Eu-eu-west-1: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
29	INSTANCE-PI	6.6157e+10	eu-west-1	1.19 INFO	CIS Level 2	[check119] Eu-eu-west-1: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
30	INSTANCE-PI	6.6157e+10	eu-west-2	1.19 INFO	CIS Level 2	[check119] Eu-eu-west-2: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
31	INSTANCE-PI	6.6157e+10	eu-west-2	1.19 INFO	CIS Level 2	[check119] Eu-eu-west-2: No Software and Medium	ec2	AwsEc2Instan Software and AWS access f																							
32	INSTANCE-PI	6.6157e+10	eu-west-1	1.2 FAIL	CIS Level 1	[check120] Eu-eu-west-1: S users-op.ac:1. Medium	iam	AwsAccount Role Software and AWS provide C																							
33	INSTANCE-PI	6.6157e+10	eu-west-1	1.21 PASS	CIS Level 1	[check121] Dus-eu-west-1: No users-op.ac:1. Medium	iam	AwsAccount User Software and AWS console f																							
34	INSTANCE-PI	6.6157e+10	eu-west-1	1.21 PASS	CIS Level 1	[check121] Dus-eu-west-1: No users-op.ac:1. Medium	iam	AwsAccount User Software and AWS console f																							
35	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
36	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
37	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
38	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
39	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
40	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
41	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
42	INSTANCE-PI	6.6157e+10	eu-west-1	1.22 PASS	CIS Level 1	[check122] Dus-eu-west-1: Po Software and Medium	iam	AwsAccount Policy Software and IAM policies :i																							
43	INSTANCE-PI	6.6157e+10	eu-west-1	1.3 PASS	CIS Level 1	[check123] Enr-eu-west-1: Users-op.ac:1. Medium	iam	AwsAccount User Software and AWS IAM usl																							
44	INSTANCE-PI	6.6157e+10	eu-west-1	1.3 PASS	CIS Level 1	[check123] Enr-eu-west-1: Users-op.ac:1. Medium	iam	AwsAccount User Software and AWS IAM usl																							
45	INSTANCE-PI	6.6157e+10	eu-west-1	1.3 PASS	CIS Level 1	[check123] Enr-eu-west-1: Users-op.ac:1. Medium	iam	AwsAccount User Software and AWS IAM usl																							
46	INSTANCE-PI	6.6157e+10	eu-west-1	1.4 FAIL	CIS Level 1	[check124] Enr-eu-west-1: jae_ens-op.ac:1. Medium	iam	AwsAccount User Software and Access keys c l																							
47	INSTANCE-PI	6.6157e+10	eu-west-1	1.4 PASS	CIS Level 1	[check124] Enr-eu-west-1: jae_ens-op.ac:1. Medium	iam	AwsAccount User Software and Access keys c l																							
48	INSTANCE-PI	6.6157e+10	eu-west-1	1.5 FAIL	CIS Level 1	[check125] Enr-eu-west-1: Po Software and Medium	iam	AwsAccount Software and Password pol E																							
49	INSTANCE-PI	6.6157e+10	eu-west-1	1.6 FAIL	CIS Level 1	[check126] Enr-eu-west-1: Po Software and Medium	iam	AwsAccount Software and Password pol E																							
50	INSTANCE-PI	6.6157e+10	eu-west-1	1.7 FAIL	CIS Level 1	[check127] Enr-eu-west-1: Po Software and Medium	iam	AwsAccount Software and Password pol E																							

AWS Assessment Summary

Report Information

Version: 3.3.0

Parameters used: aws -M csv html

Date: 2023-03-20T15:18:20.30965

AWS Credentials

User Id: AROMQZ2EMB05NDVQL/jawook_admin

Caller Identity ARN: arn:aws:sts:066157043804:assumed-role/AWSReservedSSO_AdministratorAccess_ebdff1b898d0fe62 /jawook_admin

Audited Regions: All Regions

Assessment Overview

Total Findings: 1627

Passed: 919

Failed: 608

Total Resources: 272

Search:

CIS Level 1

Check for EC2 Instances older than specific days.

CIS Level 1

Check EC2 Instances older than specific days.

i-05161493f8bc6fbcc

Check EC2 Instances older than specific days.

i-03f455e75ce109ddd

Check exposed KMS keys.

b6ac247f-d110-48f1-9451-5ca91ce5d36a

KMS key b6ac247f-d110-48f1-9451-5ca91ce5d36a is not exposed to Public.

Exposed KMS Keys or wide polic read more...

To determine the full extent o

CIS Level 2

Check for EC2 Instances with Public IP.

CIS Level 2

Check for EC2 Instances with Public IP.

i-03f455e75ce109ddd

Check exposed KMS keys.

0b448be0-f0f2-48da-98cd-498cd0f9340f

KMS key 0b448be0-f0f2-48da-98cd-498cd0f9340f is not exposed to Public.

Exposed KMS Keys or wide polic read more...

To determine the full extent o

CIS Level 3

Check for EC2 Instances with Public IP.

CIS Level 3

Check for EC2 Instances with Public IP.

i-03f455e75ce109ddd

Check exposed KMS keys.

b531008a-e225-48c3-aea5-be7afe2ed1d

KMS key b531008a-e225-48c3-aea5-be7afe2

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](#)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

Scanning to CodeBuild

점검 환경 생성 및 점검 실행

4. 서비스 역할 > 새 서비스 역할 > 역할 수정 필수

<p>서비스 역할</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> 새 서비스 역할 계정에서 서비스 역할 생성 <input type="radio"/> 기존 서비스 역할 계정에서 기존 서비스 역할 선택 	<p>역할 이름</p> <input type="text" value="codebuild-ProwlerCodeBuild-service-role"/> <p>서비스 역할 이름 입력</p>
--	--

5. 추가 구성 > 환경 변수 추가

이름: \$PROWLER_OPTIONS

값: -M csv, json-asff

환경 변수	이름	값	유형	제거
PROWLER_OPTIONS		-M csv json-asff -S -z	일반 텍스트	▼
환경 변수 추가				
파라미터 생성				

6. 아래의 buildspec 작성

```
version: 0.2
phases:
  install:
    runtime-versions:
      python: 3.9
    commands:
      - echo "Installing Prowler and dependencies..."
      - curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
      - unzip awscliv2.zip
      - ./aws/install -b /bin --update
      - pip install prowler
  build:
    commands:
      - echo "Running Prowler as prowler aws \$PROWLER_OPTIONS"
      - prowler aws \$PROWLER_OPTIONS
```

7. 빌드 시작 > 빌드 로그 > 테일 로그에서 점검 상태 확인

Visualization

Visualization

Security Hub

Security Hub > 분석 결과

리전: 연결된 모든 리전

분석 결과 (20+)

보안 문제나 실패한 보안 검사가 분석 결과로 표시됩니다.

	상각도	워크플로 상태	레코드 상태	리전	회사	제품	제목	리소스	규정 준수 상태	업데이트 시간
<input type="checkbox"/>	■ MEDIUM	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find obsolete Lambda runtimes.	Lambda 함수 access-analyzer-list-iam-policy	PASSED	몇 초 전
<input type="checkbox"/>	■ MEDIUM	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find obsolete Lambda runtimes.	LambdaFunctionEnableProwlerIntegration	PASSED	몇 초 전
<input type="checkbox"/>	■ CRITICAL	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find secrets in Lambda functions variables.	Lambda 함수 LambdaFunctionKdfTransformation	PASSED	몇 초 전
<input type="checkbox"/>	■ CRITICAL	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find secrets in Lambda functions variables.	Lambda 함수 LambdaFunctionEnableProwlerIntegration	PASSED	몇 초 전
<input type="checkbox"/>	■ CRITICAL	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Find secrets in Lambda functions code.	ProwlerCodeBuildQuickSigh-ProwlerScheduleLambdaFun-j5VrW41kP2jU	PASSED	몇 초 전
<input type="checkbox"/>	■ LOW	NEW	ACTIVE	ap-northeast-2	Prowler	Prowler	Check if Lambda functions invoke API operations are being recorded by CloudTrail.	Lambda 함수 ProwlerCodeBuildQuickSigh-LambdaFunctionExecuteQue-bo70ojllrmny	FAILED	몇 초 전
<input type="checkbox"/>	■ 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-bo70ojllrmny is not recorded by CloudTrail.

워크플로 상태 레코드 상태
신규 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-bo70ojllrmny
리소스 유형 AwsLambdaFunction 리소스 리전 ap-northeast-2
리소스 ID arn:aws:lambda:ap-northeast-2:066157043804:function:ProwlerCodeBuildQuickSigh-LambdaFunctionExecuteQue-bo70ojllrmny
▼ 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.
[Input field]

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
prowlerresult

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
s3://bucket/prefix/

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

The screenshot shows the 'Schema' section of the AWS Glue Schema Registry. It has two options: 'Define or upload schema' (selected) and 'Choose from Glue Schema Registry'. Below is a table titled 'Schema (0)' with columns: #, Column name, Data type, Partition key, and Comment. A search bar and buttons for 'Edit schema as JSON', 'Delete', 'Edit', and 'Add' are at the top. The table body is empty, showing 'No table schema'.

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;
```

The screenshot shows the Amazon Athena Query editor interface. The top navigation bar includes 'Amazon Athena > Query editor' and tabs for 'Editor', 'Recent queries', 'Saved queries', and 'Settings'. A 'Workgroup' dropdown is set to 'primary'. The main area has two tabs: 'Query 2' and 'Query 3'. 'Query 3' is active, displaying the following SQL code:

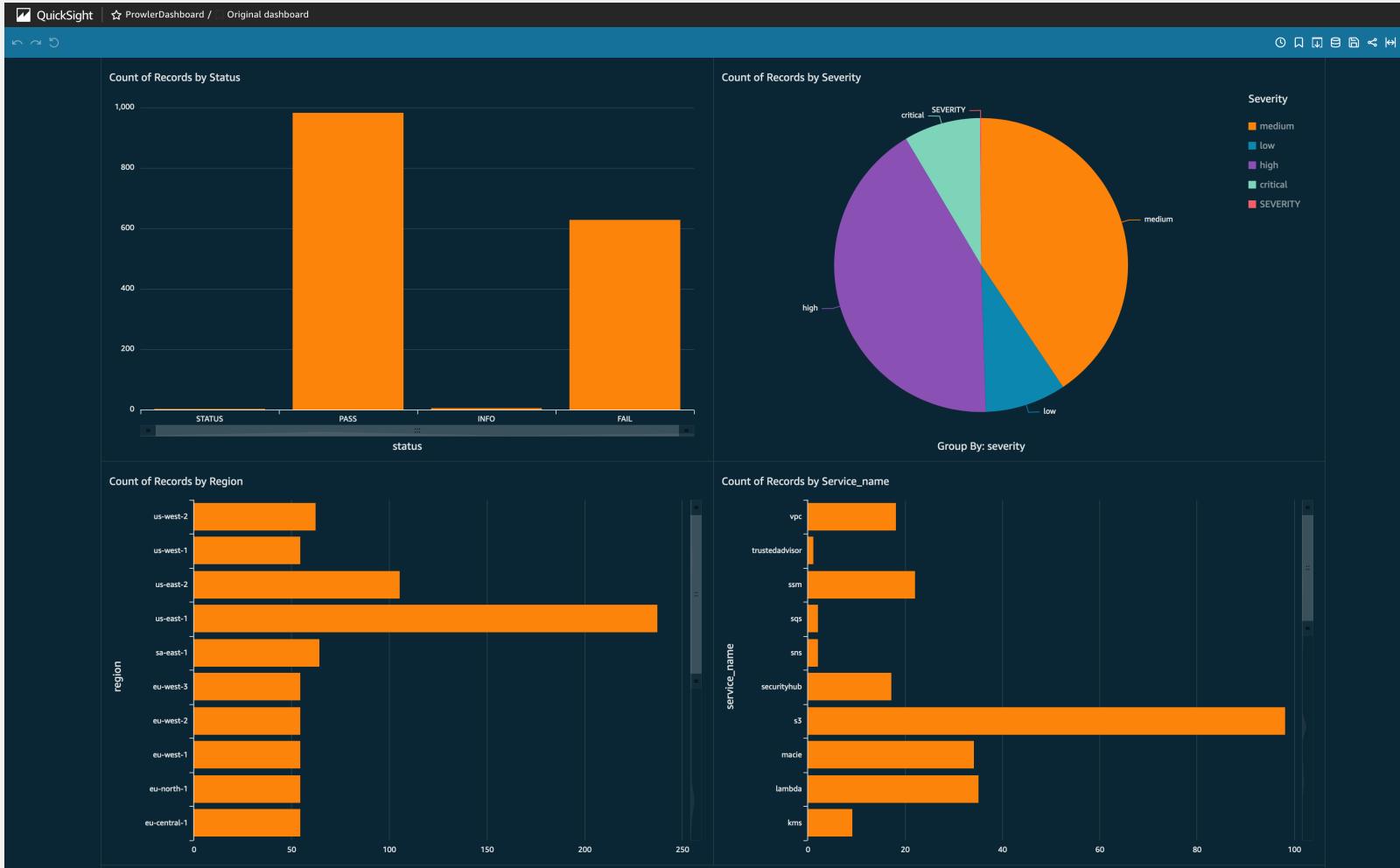
```
1 SELECT
2 account_id, region, check_title, status, severity, resource_id, resource_arn, compliance, risk, description
3 FROM "prowlerv3result"."prowler_v3_result_table"
4 limit 10;
```

The status bar indicates the query was completed with a run time of 567 ms and scanned 11.81 KB of data. Below the code, there are buttons for 'Run again', 'Explain', 'Cancel', 'Clear', and 'Create'. The left sidebar shows the 'Data' configuration with 'Data source' set to 'AwsDataCatalog' and 'Database' set to 'prowlerv3result'. It also lists 'Tables (1)' containing 'prowler_v3_result_table' and 'Views (0)'. The right side displays the 'Query results' tab with the heading 'Completed' and a table titled 'Results (10)'. The table columns are: #, account_id, region, check_title, status, severity, resource_id, resource_arn, compliance, and risk. The data rows are as follows:

#	account_id	region	check_title	status	severity	resource_id	resource_arn	compliance	risk
1	ACCOUNT_ID	REGION	CHECK_TITLE	STATUS	SEVERITY	RESOURCE_ID	RESOURCE_ARNS	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	Amazc
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	Amazc
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	Amazc
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	Amazc
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	Amazc
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	Amazc
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	Amazc
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	Amazc
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	Amazc

Visualization

QuickSight Dashboard





Thank you!