

Prowler MCP 개발 및 AWS 취약점 점검 / 조치 자동화 아키텍처 구성기 ↗

김서연

AWS BEGINNER

2025. 8. 21

Agenda ↴

1. INTRO

- 최근 규제 변화
- CSPM 도구의 필요성
- WHAT IS PROWLER?
- PROLWER V5

2. MCP 제작

- 기본 아이디어
- CLAUDE DESKTOP MCP 제작
- 시연영상

3. CLOSING

- 향후 계획

1. INTRO

1.1 최근 규제 변화

1.2 CSPM 도구의 필요성

1.3 what is prowl?

1.4 Prolwer v5



1.1 최근 규제 변화

: 금융 산업 내 AI 및 SaaS(클라우드) 사용 규제 완화

INTRO

MCP 제작

CLOSING

금융권 클라우드 전환 가속화

② 클라우드 이용 확대

(규제샌드박스)

	현 행	개 선
데이터	개인신용정보 금지	가명정보 허용
프로그램 유형	협업툴, 인사관리 등 비중요업무 허용	고객관리(CRM), 업무자동화 등 추가 허용
단말기	유선 PC만 허용	모바일단말 허용

2024년, 금융 산업 내 AI 및 SaaS(클라우드) 사용을 완화
(금융분야 망분리 개선 로드맵)



하나은행, 토스증권 등 시중 은행에서의 AWS(클라우드) 사용 증대

IV. 클라우드 활성화를 위한 제도개선 방안

< 기본 방향 >

1. 클라우드 서비스 이용범위 확대

- 금융회사, 펀테크기업이 클라우드를 활용하여 혁신적 상품과 서비스 개발이 가능하도록 이용범위를 확대
 - 개인신용정보 · 고유식별정보도 국내소재 클라우드를 이용할 수 있도록 개선
 - ※ 국외소재 클라우드 허용은 국내소재 클라우드 운영 이후 문제점 등을 고려하여 중·장기적으로 검토

2. 클라우드 서비스 이용 · 제공 기준 마련

- 중요정보 처리시스템의 안전성을 확보하기 위해 클라우드 이용(금융회사), 제공(제공자)시 기준을 도입하고 운영방안을 수립
 - (금융회사) 중요정보 클라우드 이용시 안전성 관리를 강화
 - (제공자) 금융의 특수성을 반영해 클라우드 서비스 제공자가 기본적으로 준수해야 할 기준을 마련
- * '중요정보'의 경우 기존 금융권 전산시스템에 준하는 보안수준을 충족하도록 함

3. 클라우드 서비스 감독 · 검사 강화

- 클라우드 활용 확대를 고려하여 금융권 클라우드 이용현황에 대한 모니터링을 강화하고, 적절한 감독·검사 체계 마련
 - 클라우드 서비스 이용 관련 금융회사의 보고의무 강화
 - 전자금융보조업자(클라우드 서비스 제공자)에 대한 감독당국의 직접 감독·조사권을 확보하는 방안을 검토(법개정 사항)

1.1 최근 규제 변화

: 금융 산업 내 AI 및 SaaS(클라우드) 사용 규제 완화

INTRO

MCP 제작

CLOSING

◆ 금융권 클라우드 도입률 92%…“전략적 자산으로 인식 변화”

조사 결과 국내 금융기관의 92%가 활용 수준과 관계없이 퍼블릭 클라우드를 도입한 상태다. 현재 사용하지 않으나 향후 3년 이내 도입을 계획 중인 기관까지 포함하면 96%에 달한다. 현재 사용하지도 않고 도입 계획도 없는 기관은 4%에 불과했다.

금융 및 핀테크 케이뱅크의 클라우드 도입 여정: 빅데이터, 채널, MSA, AI/ML

2021 2022 2023 2024

전사적 클라우드 확산

제품 출시속도를 가속합니다.

진화하는 요구사항에 대한 적응성, 확장성을 확보합니다.

신중훈, 솔루션즈 아키텍트 AWS

클라우드 네이티브 솔루션 채택

애팽킹 제3센터 구축 MSA 도입

데이터를 의사결정 프로세스와 통합

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Engineer (클라우드 보안/분석)

토스플레이스 소속 | 정규직 | 초기 멤버

합류하게 될 팀에 대해 알려드려요

- 토스플레이스의 보안팀은 Security Engineer, Information Security Manager, Privacy Manager, IT Manager로 구성되어 있어요.
- Security팀은 안전한 토스플레이스 서비스를 만들기 위해 Infra팀, 제품(서비스)을 만드는 사일로, Legal팀 그리고 Compliance팀과 협업하고 있어요.
- 이외에도 Security팀의 각 직무 담당자는 계열사의 동일 직군 동료들과 활발한 교류를 통해 전문분야에 대한 고민을 나누며 협업해요.
- 토스플레이스에서는 Security팀의 초기멤버로서 안정적인 서비스를 제공할 수 있도록 보안체계를 만들어 나가는 경험을 할 수 있어요.

합류하면 함께할 업무예요

- AWS 보안 서비스를 운영하고 보안 인프라를 구축 및 관리해요.(FW, WAF, Shield, GuardDuty, IAM 등)
- AWS 취약점 점검 및 모니터링을 수행해요.(CSPM)
- AWS 인프라 취약점 점검(Server, DBMS, Network 등) 활동을 수행해요.
- 침해사고 분석 및 대응 업무를 수행해요.
- 다양한 보안 이벤트 분석을 통해 위협을 실시간으로 식별하고 대응해요.

1.2 CSPM 도구의 필요성

: 클라우드 도입 시 주요 요건인 보안 문제를 해결하기 위해 자동화 된 보안 점검 대응 시스템이 필요

INTRO

MCP 제작

CLOSING

퍼블릭 클라우드 업체 선정 시 핵심 기능 요소



(산업별) Top 3

퍼블릭 클라우드 업체 선정 시 핵심 기능 요소

제조	금융	리테일	서비스
1 비용 효율성	비용 효율성	비용 효율성	비용 효율성
2 강력한 데이터 보안 체계	강력한 데이터 보안 체계	강력한 데이터 보안 체계	강력한 데이터 보안 체계
3 빠른 복구 대응력	법적 안정성	빠른 복구 대응력	안정적인 네트워크 성능

자동화된 보안 점검 대응 시스템 필요



1. 가상자원 관리	1
1.1. 가상환경 생성 시 최초 계정에 대한 비밀번호 규칙 수립	2
1.2. 이용자 가상환경 접속 시 코그언 규칙 적용	3
1.3. 가상자원 부여 계정 생성 시 추가 인증수단	4
1.4. 가상자원 생성 시 네트워크 설정 적용	8
1.5. 가상자원 접속 시 보안 방화 수립	12
1.6. 이용자 가상환경 관리 설정	14
1.7. 이용자 가상환경 내 협업모드 통제방안 수립	15
2. 네트워크 관리	18
2.1. 업무 목적에 따른 네트워크 구성	19
2.2. 내부망 대외망과의 보안 통제	33
2.3. 네트워크 보안 관제 수령	48
2.4. 공개망 대외망 네트워크 분리	65
2.5. 네트워크 사용 IP주소 할당 및 관리	68
2.6. 네트워크(인터넷) IP 주체 추가적 검토	70
3. 계정 및 권한 관리	71
3.1. 글로우드 계정 관리	72
3.2. 이용자 인증 수단 확장	83
3.3. 인증방법 사용 범위 확장	87
3.4. 글로우드 가상자원 관리시스템 관리 권한 추가인증 적용	92
3.5. 글로우드 가상자원 관리시스템 로그인 규칙 수립	96
3.6. 계정 비활성화 규칙 수립	103
3.7. 공개망 범위 접근 계정 제한	107
4. 암호화 관리	116
4.1. 암호화 적용 가능 여부 확인	117
4.2. 암호화 적용 범위 수립	126
4.3. 암호화 서비스 관리자 한정 통제	131
4.4. 암호화 적용 범위 확장	137
4.5. 한정한 암호화 알고리즘 적용	141
5. 로깅 및 모니터링 관리	144
5.1. 가상환경 이용여부, 사용, 변경 등에 관한 행위추적형 확보	145
5.2. 가상환경 이용 행위적 특징 추출 모니터링	155
5.3. 이용자 가상환경 모니터링 기능 확보	165
5.4. API 사용내용(내선, 헤더, 헤더 정보) 등에 관한 행위추적형 확보	177
5.5. 네트워크 관리 서비스(SVPC, 보안그룹, ACL 등)에 관한 행위추적형 확보	181
5.6. 계정 번동사행에 대한 행위추적형 확보	194
5.7. 계정 번동사행에 관한 모니터링 수행	206

(금융)기업은 클라우드를 도입하면서 자산을 관리해야 하는데,
수작업으로 관리하면 시간과 인력이 과도하게 소요됨



자동화된 보안 점검 대응 시스템의 필요

1.2 CSPM 도구의 필요성

: 클라우드 도입 시 주요 요건인 보안 문제를 해결하기 위해 자동화 된 보안 점검 대응 시스템이 필요

INTRO

MCP 제작

CLOSING



1.3 WHAT IS PROWLER?

: 점유율이 가장 높은 오픈소스 CSPM 도구

INTRO

MCP 제작

CLOSING



프로젝트명	GitHub Stars	GitHub 기여자 수	GitHub 최근 커밋 날짜	지원 플랫폼	지원 컴플라이언스	주요 기능
Prowler-cloud	10.9k	259	2024-11-20	AWS, Azure, Google Cloud, Kubernetes	KISA-ISMS-PCIS, NIST 800-53, PCI-DSS, GDPR, FedRAM P, FFIEC, GXP, HIPAA, ISO 27001, SOC2, AWS Well-Architected Framework, ENS 등	클라우드보안 탐지 및 평가, 자산 식별, 컴플라이언스 준수 점검, Incident Response 지원, 하드닝 및 포렌식 준비, 보고서 생성, AWS 시큐리티 허브 통합

그림1-2. 주요 오픈소스 CSPM 포지셔닝

1.3 WHAT IS PROWLER?

: 점유율이 가장 높은 오픈소스 CSPM 도구

```
v4.0.0
the handy multi-cloud security tool

Date: 2024-04-08 15:09:16

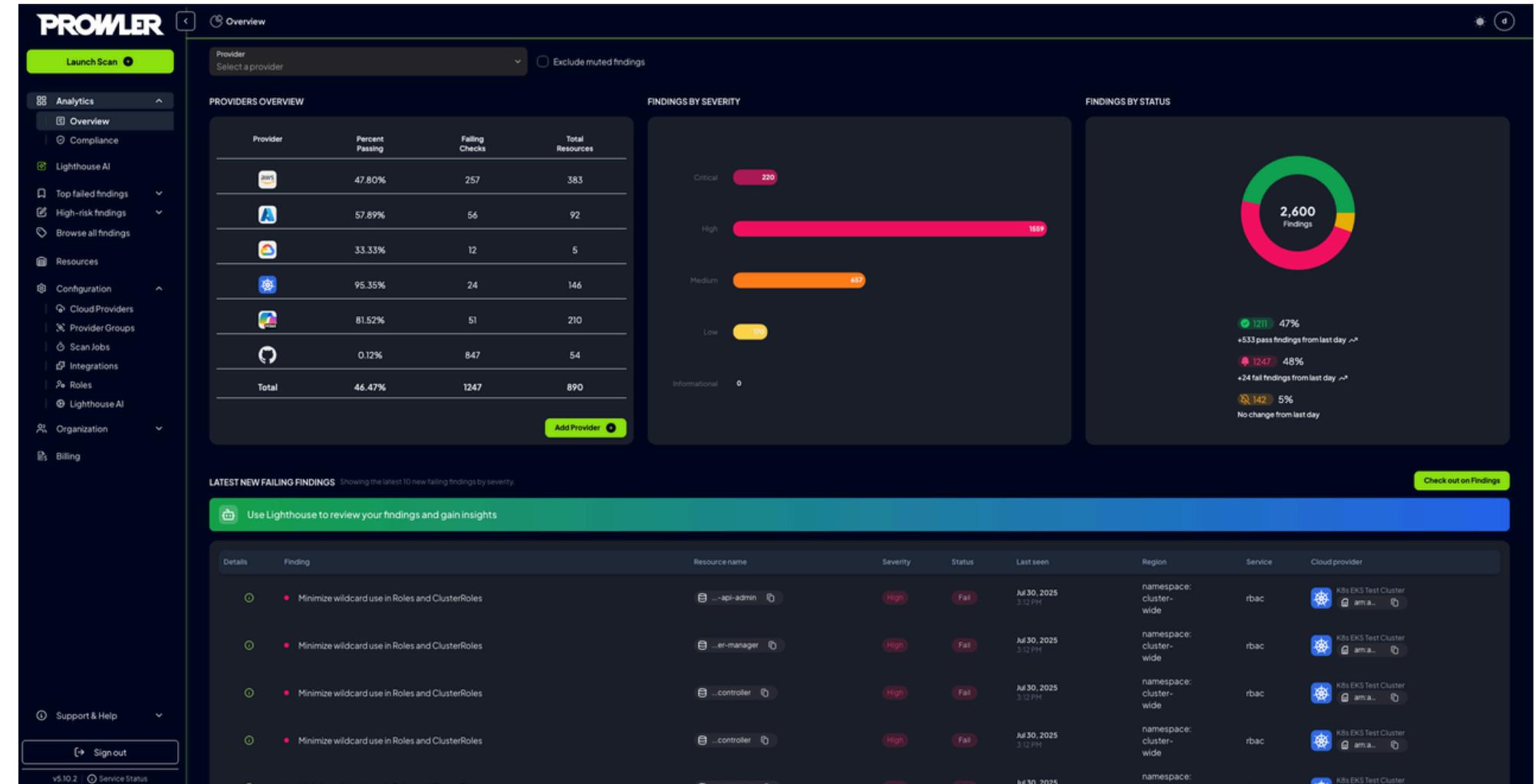
-> Using the AWS credentials below:
  • AWS-CLI Profile: default
  • AWS Regions: us-east-1
  • AWS Account: [REDACTED]
  • User Id: [REDACTED]:toni
  • Caller Identity ARN: arn:aws:sts:[REDACTED]:toni

-> Using the following configuration:
  • Config File: prowler/config/config.yaml
  • Mute List File: prowler/config/aws_mutelist.yaml
  • Scanning unused services and resources: False

Executing 305 checks, please wait...
-> Scan completed! | 305/305 [100%] in 1:56.7

Overview Results:
  41.8% (79) Failed | 54.5% (103) Passed | 19.05% (36) Muted

Account 552455647653 Scan Results (severity columns are for fails only):
+-----+-----+-----+-----+-----+-----+-----+-----+
| Provider | Service | Status | Critical | High | Medium | Low | Muted |
+-----+-----+-----+-----+-----+-----+-----+-----+
| aws     | accessanalyzer | FAIL (1) | 0 | 0 | 0 | 1 | 0 |
| aws     | account       | FAIL (1) | 0 | 0 | 1 | 0 | 0 |
| aws     | lambda         | FAIL (1) | 0 | 0 | 0 | 1 | 5 |
| aws     | backup          | FAIL (1) | 0 | 0 | 0 | 1 | 0 |
| aws     | cloudformation | FAIL (5) | 0 | 0 | 5 | 0 | 3 |
| aws     | cloudtrail      | FAIL (4) | 0 | 0 | 1 | 3 | 9 |
| aws     | cloudwatch      | FAIL (19) | 0 | 0 | 19 | 0 | 6 |
| aws     | config          | PASS (1) | 0 | 0 | 0 | 0 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
```



Prowler CLI

Prowler Cloud

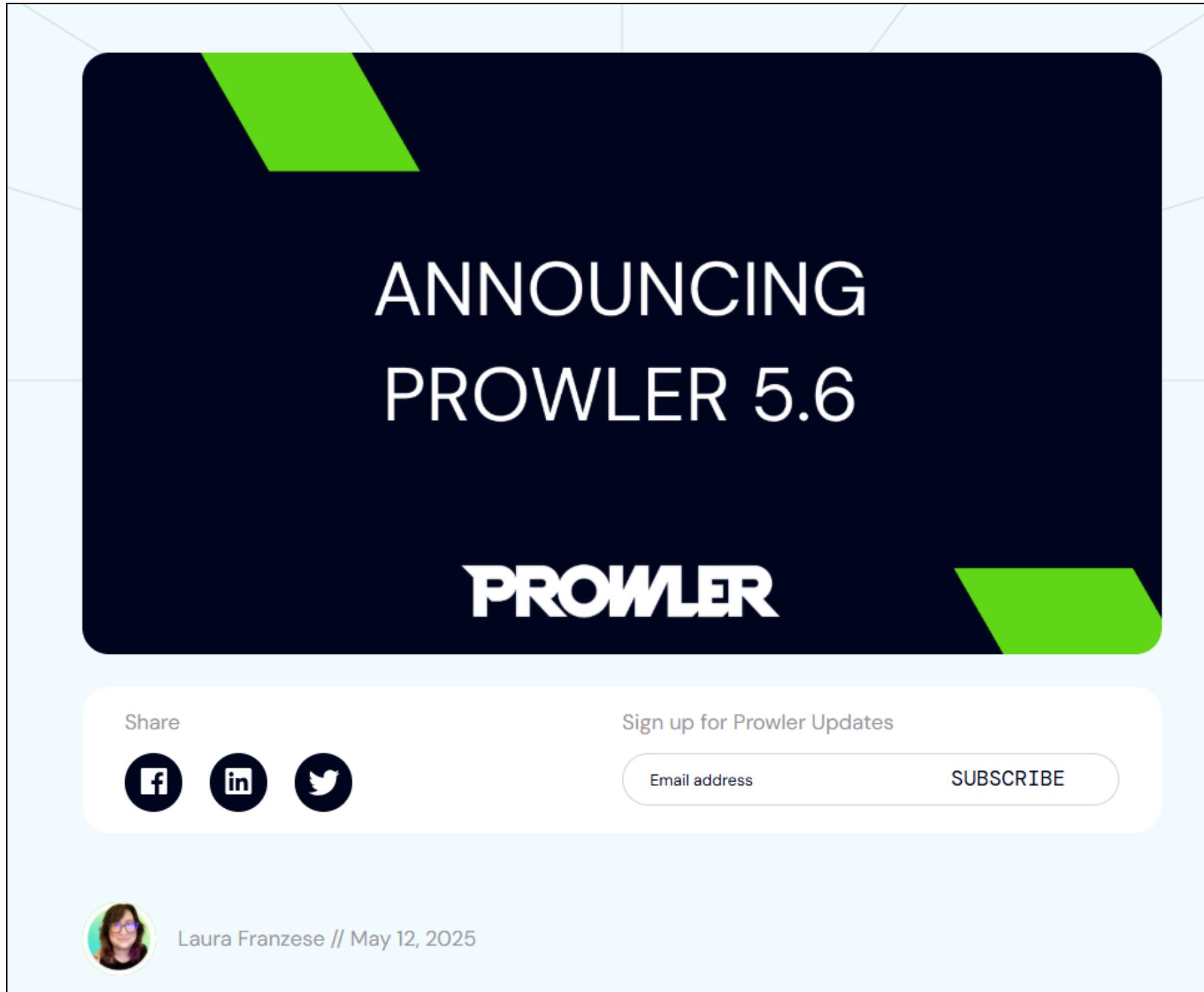
1.4 PROWLER V5

: Prowler Studio를 필두로 한 AI 기능 확대 + MCP와 Fixer 기능 추가

INTRO

MCP 제작

CLOSING



About

Prowler Studio is an AI assistant that helps you to create threat detection checks, remediations and update compliance frameworks for Prowler. It can be used as a CLI tool or as a web application.

security

cloud

threat

controls

compliance

AI 기능 강화와 자체 IaC 스니펫 추가

1.4 PROWLER V5

: Prowler Studio를 필두로 한 AI 기능 확대 + MCP와 Fixer 기능 추가

INTRO

MCP 제작

CLOSING

Prowler Fixer (remediation)

Prowler allows you to fix some of the failed findings it identifies. You can use the `--fixer` flag to run the fixes that are available for the checks that failed.

```
prowler <provider> -c <check_to_fix_1> <check_to_fix_2> ... --fixer  
Executing 1 check, please wait...  
Check ID: ec2_ebs_default_encryption - ec2 [medium]  
  FAIL eu-west-1: EBS Default Encryption is not activated.  
  FAIL us-east-1: EBS Default Encryption is not activated.  
-> Scan completed! | 1/1 [100%] in 32.6s  
  
Running Prowler Fixer, please wait...  
Fixing fails for check ec2_ebs_default_encryption...  
  FIXING eu-west-1...  
  DONE  
  FIXING us-east-1...  
  DONE  
  
2 findings fixed!
```

보안 대응 IaC 스니펫

자동 수정 실행: `--fixer` 플래그를 사용해 진단 실패한 항목에 대한 자동 수정(Remediation) 명령을 실행

Fixer 코드 작성 가능: `check_id_fixer.py` 파일을 작성해, 특정 검사에 대해 리전 또는 리소스 단위로 해결 로직을 제공하는 Custom Fixer 구현이 가능

설정 기반 유연성 제공: `--list-fixers` 명령으로 사용 가능한 Fixer 목록을 확인할 수 있으며, `--fixer-config` 옵션을 통해 YAML 기반 설정을 적용해 실행 동작을 커스터마이징 가능

Prowler Fixer

1.4 PROWLER V5

: Prowler Studio를 필두로 한 AI 기능 확대 + MCP와 Fixer 기능 추가

INTRO

MCP 제작

CLOSING



Date: 2025-08-21 16:30:33

```
- accessanalyzer_enabled
- awslambda_function_not_publicly_accessible
- cloudtrail_logs_s3_bucket_is_not_publicly_accessible
- cloudtrail_multi_region_enabled
- cloudtrail_threat_detectionEnumeration
- cloudtrail_threat_detection_llm_jacking
- cloudtrail_threat_detection_privilege_escalation
- codeartifact_packages_external_public_publishing_disabled
- documentdb_cluster_public_snapshot
- ec2_ami_public
- ec2_ebs_default_encryption
- ec2_ebs_public_snapshot
- ec2_ebs_snapshot_account_block_public_access
- ec2_instance_account_imdsv2_enabled
- ec2_instance_port_cassandra_exposed_to_internet
- ec2_instance_port_cifs_exposed_to_internet
- ec2_instance_port_elasticsearch_kibana_exposed_to_internet
- ec2_instance_port_ftp_exposed_to_internet
- ec2_instance_port_kafka_exposed_to_internet
- ec2_instance_port_kerberos_exposed_to_internet
- ec2_instance_port_ldap_exposed_to_internet
- ec2_instance_port_memcached_exposed_to_internet
- ec2_instance_port_mongodb_exposed_to_internet
- ec2_instance_port_mysql_exposed_to_internet
- ec2_instance_port_oracle_exposed_to_internet
- ec2_instance_port_postgresql_exposed_to_internet
- ec2_instance_port_rdp_exposed_to_internet
- ec2_instance_port_redis_exposed_to_internet
- ec2_instance_port_sqlserver_exposed_to_internet
- ec2_instance_port_ssh_exposed_to_internet
- ec2_instance_port_telnet_exposed_to_internet
- ec2_securitygroup_allow_ingress_from_internet_to_high_risk_tcp_ports
- ecr_repositories_not_publicly_accessible
- glacier_vaults_policy_public_access
- guardduty_is_enabled
- iam_password_policy_expires_passwords_within_90_days_or_less
- iam_password_policy_lowercase
- iam_password_policy_minimum_length_14
- iam_password_policy_number
- iam_password_policy_reuse_24
- iam_password_policy_symbol
- iam_password_policy_uppercase
- kms_cmk_not_deleted_unintentionally
- kms_cmk_rotation_enabled
- neptune_cluster_public_snapshot
- opensearch_service_domains_not_publicly_accessible
- rds_instance_no_public_access
- rds_snapshots_public_access
- s3_account_level_public_access_blocks
- s3_bucket_policy_public_write_access
- s3_bucket_public_access
- s3_bucket_public_list_acl
- s3_bucket_public_write_acl
- securityhub_enabled
- sqs_queues_not_publicly_accessible
```

There are 55 available fixers.

1.4 PROWLER V5

: Prowler Studio를 필두로 한 AI 기능 확대 + MCP와 Fixer 기능 추가

INTRO

MCP 제작

CLOSING

Prowler Studio

Prowler Studio is an AI-powered toolkit for generating and managing security checks for [Prowler](#). It is modular, model-agnostic, and supports multiple workflows and integrations.

| Note: The code generated by the AI system should be reviewed by a human before use.

Components Overview

Prowler Studio consists of several main components. Each is documented in detail in the `docs/` directory. Below is a summary of each component and a link to its full documentation.

1. Core ([docs/core.md](#))

The foundational logic and workflows for check and fixer generation, check knowledge base using Retrieval Augmented Generation (RAG), and compliance mapping. Model-agnostic and designed for extensibility.

- **Main features:**
 - Modular workflow orchestration (LlamaIndex-based).
 - RAG dataset and semantic search in Prowler checks.
 - Provider abstraction for LLMs and embeddings.
- **Technical details and architecture:** [docs/core.md](#)

Prowler Studio

Prowler Lighthouse

Prowler RAG를 이용한 AI 챗봇으로, 자연어 질의, 상세한 수정 가이드, 상황 맥락 기반 분석을 제공하는 멀티에이전트 기반 구조.

Prowler Cloud MCP

Google과 openAI API를 기반으로 한 MCP로, AI 코드 어시스트 통합(IDE, cursor 등)을 지원

1.4 PROWLER V5

: Prowler Studio를 필두로 한 AI 기능 확대 + MCP와 Fixer 기능 추가

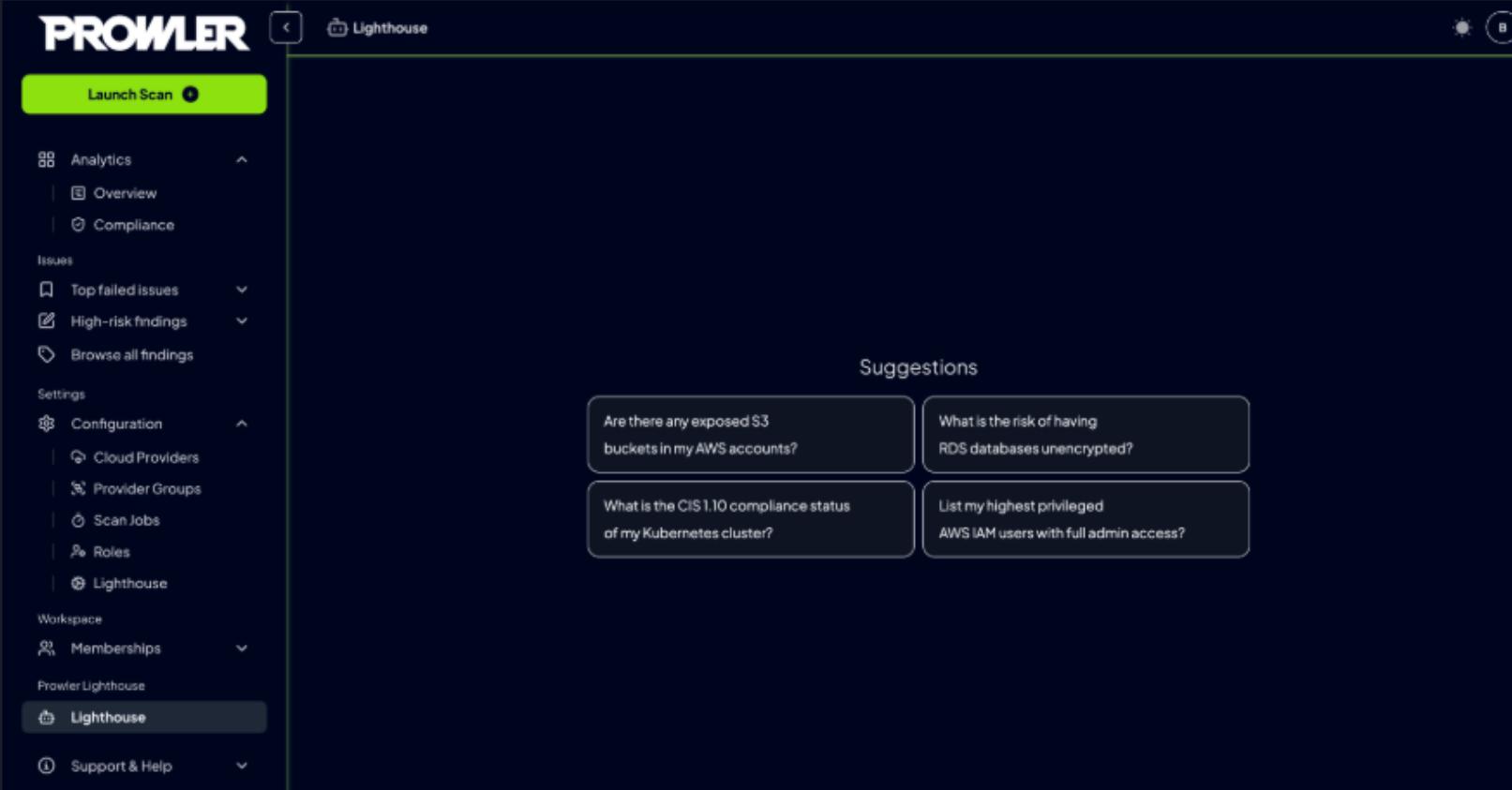
INTRO

MCP 제작

CLOSING

Prowler Lighthouse AI

Prowler Lighthouse AI is a Cloud Security Analyst chatbot that helps you understand, prioritize, and remediate security findings in your cloud environments. It's designed to provide security expertise for teams without dedicated resources, acting as your 24/7 virtual cloud security analyst.

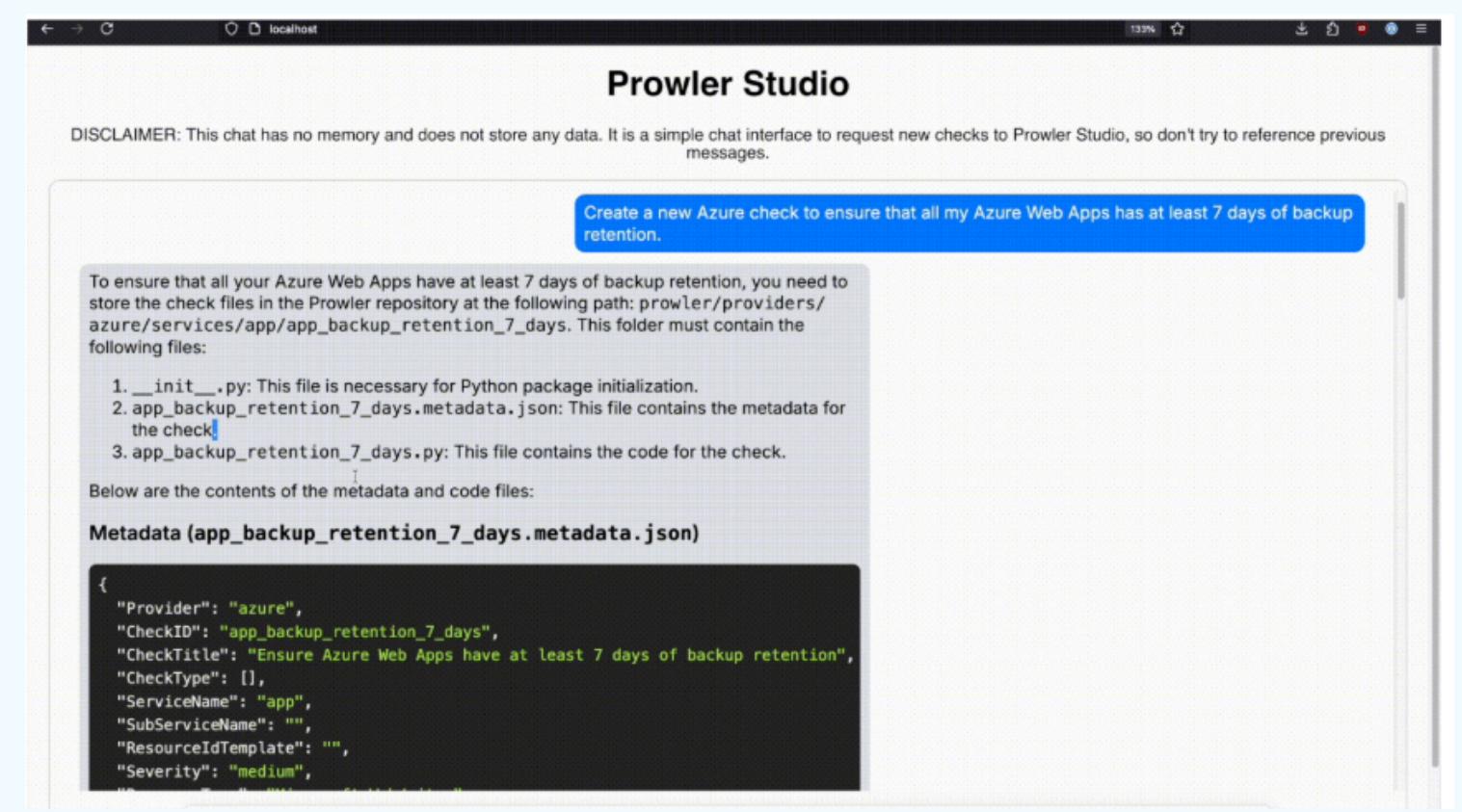


The screenshot shows the Prowler Lighthouse AI interface. On the left is a dark sidebar with the Prowler logo at the top. Below it are sections for Analytics (Overview, Compliance), Issues (Top failed issues, High-risk findings, Browse all findings), Configuration (Cloud Providers, Provider Groups, Scan Jobs, Roles), and Settings (Lighthouse, Workspace, Memberships). At the bottom are links for Prowler Lighthouse and Support & Help. The main area has a heading 'Suggestions' and four cards: 'Are there any exposed S3 buckets in my AWS accounts?', 'What is the risk of having RDS databases unencrypted?', 'What is the CIS 1.10 compliance status of my Kubernetes cluster?', and 'List my highest privileged AWS IAM users with full admin access?'. A large green button at the top says 'Launch Scan'.

Prowler Lighthouse

- `prowler-studio` (includes Core + CLI by default)
- `prowler-studio-core`
- `prowler-studio-cli`
- `prowler-studio-api`
- `prowler-studio-mcp-server`

This release also introduces seamless integration with AI Code assists via MCP Server and comprehensive improved documentation for each component.



The screenshot shows the Prowler Studio interface. It features a header 'Prowler Studio' and a disclaimer: 'DISCLAIMER: This chat has no memory and does not store any data. It is a simple chat interface to request new checks to Prowler Studio, so don't try to reference previous messages.' Below is a message box with a blue button 'Create a new Azure check to ensure that all my Azure Web Apps has at least 7 days of backup retention.' A text box contains instructions: 'To ensure that all your Azure Web Apps have at least 7 days of backup retention, you need to store the check files in the Prowler repository at the following path: prowler/providers/azure/services/app/app_backup_retention_7_days. This folder must contain the following files: 1. __init__.py: This file is necessary for Python package initialization. 2. app_backup_retention_7_days.metadata.json: This file contains the metadata for the check. 3. app_backup_retention_7_days.py: This file contains the code for the check.' Below is a section titled 'Metadata (app_backup_retention_7_days.metadata.json)' with a code block:

```
{ "Provider": "azure", "CheckID": "app_backup_retention_7_days", "CheckTitle": "Ensure Azure Web Apps have at least 7 days of backup retention", "CheckType": [], "ServiceName": "app", "SubServiceName": "", "ResourceIdTemplate": "", "Severity": "medium", "...}
```

Prowler Cloud MCP

1.4 PROWLER V5

: LIGHTHOUSE를 필두로 한 MCP와 Fixer 기능 추가

INTRO

MCP 제작

CLOSING

Prowler Lighthouse / Prowler Cloud MCP

The screenshot shows the Prowler Studio MCP Server interface. At the top, there's a header with a folder icon labeled "mcp_server", the text "chore: update core deps...", and a timestamp "2 months ago". Below the header, the main area is titled "Prowler Studio MCP Server" and has a sub-section "Overview" which contains a brief description of the MCP Server. Further down, there's a section titled "Demo Time!" with a small icon. The bottom half of the screen is dominated by a large code editor window displaying Python code related to AWS SQS queue configuration checks. To the right of the code editor, there are several floating tool windows: one for creating a new check, another for generating code, and others for accepting or rejecting changes. A status bar at the bottom indicates "Generating" and "Stop X".

만들고 있던 기능을 공식 팀이 먼저 발표함!
어떡하지?

1.4 PROWLER V5

: LIGHTHOUSE를 필두로 한 MCP와 Fixer 기능 추가

INTRO

MCP 제작

CLOSING

Prowler Cloud MCP

Configuration

- Set `GOOGLE_API_KEY` (required) and `OPENAI_API_KEY` (optional) in your environment or `.env` file.
- Configure your IDE to connect to the MCP server (see below for examples).

Integration Examples

Cursor IDE

With Docker:

```
{  
  "mcpServers": {  
    "prowler-studio": {  
      "command": "docker",  
      "args": ["run", "--rm", "-e", "OPENAI_API_KEY=your_openai_api_key", "-e", "GOOGLE_API_KEY=your_google_api_key", "-i", "prowler-studio"],  
      "image": "prowler-studio"  
    }  
  }  
}
```

1.4 PROWLER V5

: 공식 MCP가 있으면 우리는 어떻게 하지?

INTRO

MCP 제작

CLOSING

Prowler Cloud MCP

Configuration

- Set `GOOGLE_API_KEY` (required) and `OPENAI_API_KEY` (optional) in your environment or `.env` file.
- Configure your IDE to connect to the MCP server (see below for examples).

Integration Examples

Cursor IDE

With Docker:

**Google API key/OpenAI API key가 필수적이고, IDE에 연결해서 쓰는 형식이네~
우리는 CLAUDE Desktop 용으로 만들고, IaC tool과 연동되게 만들자!**

```
{
  "mcpServers": [
    "prowler-stu"
  ],
  "command": "ls",
  "args": [
    "-l"
  ]
}
```

2. MCP 제작

2.1 기본 아이디어

2.2 Claude desktop MCP 제작

2.3 시연영상



2.1 기본 아이디어

: 컴플라이언스 점검 + 대응 + 알림이 한번에 되는 도구를 만들자!

INTRO

MCP 제작

CLOSING

컴플라이언스 점검 + 대응 + 알림이 한번에 되는 도구를 만들자!

점검



대응



알림



2.1 기본 아이디어

: 컴플라이언스 점검 + 대응 + 알림이 한번에 되는 도구를 만들자!

INTRO

MCP 제작

CLOSING

왜 MCP여야 하는가?

Prowler는 CLI 중심(Cloud는 유료) → 비개발자 접근성이 낮음

로컬 데이터 파싱, Slack 알림, AWS Security Hub 연계 같은 기능을
하나의 **자연어 인터페이스**로 묶고 싶었음

현재 공식 MCP는 자체 개발한 UX를 사용함.
Claude Desktop을 이용하면 **시안성+확장성**
(다른 MCP를 같이 불러낼 수 있음) up

2.1 기본 아이디어

: 컴플라이언스 점검 + 대응 + 알림이 한번에 되는 도구를 만들자!

INTRO

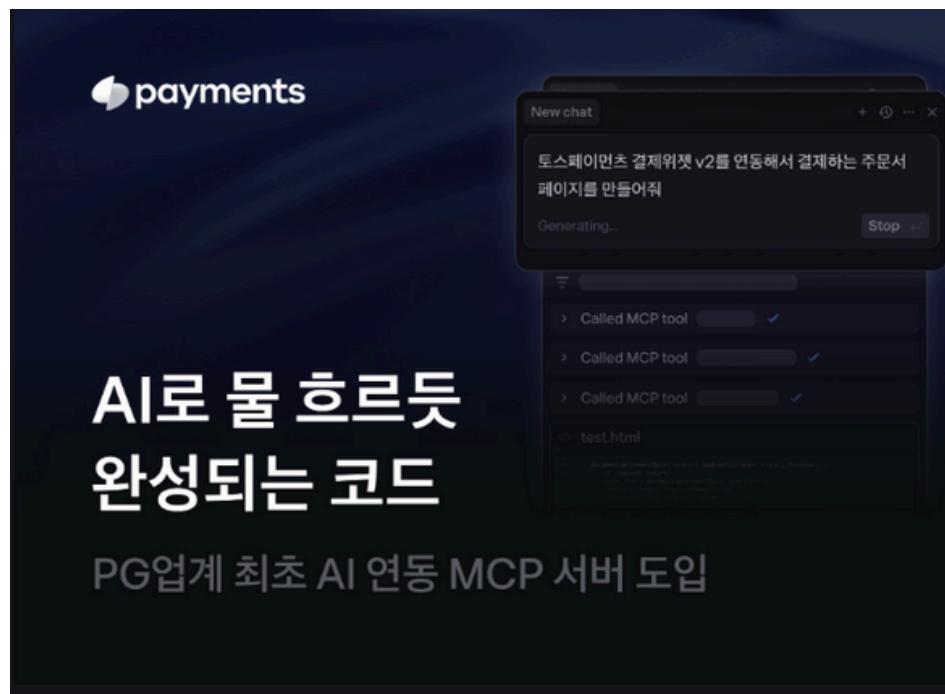
MCP 제작

CLOSING

LLM에 우리 인스턴스 상태를 노출시켜도 안전한가?

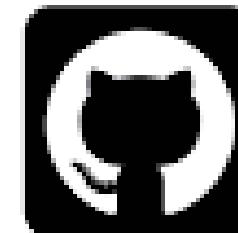
당연히 완벽하게 안전하지는 않음 → **Local MCP제작 고려중**

그러나 일단은, prowler scan 결과에서 특별히 민감정보가 노출되지 않는다고 판단했음
+ 익명처리해서 해결해도 됨!



github/github-mcp-server

GitHub's official MCP Server



Ak

Contributors

11

Issues

595

Stars

23

Forks

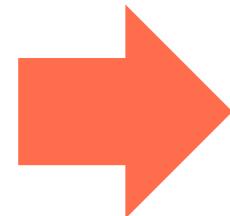
2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING

점검



Prowler CLI로 scan해서 나온 로컬 파일



로컬 스캔 결과 불러오기, CSV·HTML·JSON 파일 파싱

컴플라이언스 결과를 자연어로 쉽게 풀어서 설명

점검 결과 내 Pass/Fail 항목을 사유와 함께 요약

Prowler CLI의 output 위치만 설정하면 – MCP가 알아서 파일을 읽고 사용자에게 설명/질의응답

2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING

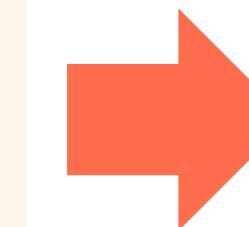
대응



컨텍스트와 함께 취약점 요약

가장 시급한 보안 문제 우선순위 지정

수정사항을 IaC 코드로 작성, YAML 파일 생성



분석에서 실행까지 – 스캔 결과를 IaC 코드로 즉시 사용할 수 있는 수정 조치로 전환

대응

IaC 구현 툴 선택의 이유?

Custodian과 Ansible(개발중)은 운영 환경에서 변경 사항을 빠르게 반영하거나, 정책 기반의 자동 수정을 수행하는 데 적합하였음

특히 **Custodian**의 경우 **정책 기반** 관리 및 자동화가 가능해 최우선적으로 개발함

또한, Prowler fixer는 prowler에 최적화되어 있고, 기본제공된 스니펫을 사용할 수 있어 토큰 소모가 적었음(Claude의 개입 X)

분석에서 실행까지 – 스캔 결과를 IaC 도구로 즉시 사용할 수 있는 수정 조치로 전환

2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING

IaC 구현 툴 선택의 이유?



Cloud
CustodianSM

클라우드 리소스를 **정책 기반으로** 자동 관리하는 오픈소스 툴,
개별 리소스에 대한 조건에 맞는 조치를 수행하는 데 최적화

정책 (Policy) 기반 관리

YAML 파일로 “어떤 리소스에, 어떤 조건일 때, 어떤 작업을 할지” 정의

우리 mcp는 이 YAML 파일을 만듦
ex) 퍼블릭 S3 버킷이 있으면 → 접근차단

```
policies:  
  - name: close-public-s3  
    resource: aws.s3  
    filters:  
      - type: global-grants  
        perms: [READ, WRITE]  
    actions:  
      - type: set-permissions  
        block-public-acls: true
```

AWS, Azure, GCP, k8s+ 지원

```
aws  
  
policies:  
  - name: my-aws-instances  
    resource: aws.ec2  
    filters:  
      - type: value  
        key: "tag:owner"  
        value: "sam"  
  
import boto3  
  
client = boto3.client('ec2')  
  
custom_filter = [{  
  'Name': 'tag:owner',  
  'Values': ['sam']}]  
  
response =  
client.describe_instances(Filters=custom_filter)
```

동작 구조

1) 리소스 필터링
정책에서 조건 지정
(public: true, tag: Enviroment:dev)

2) 액션
조건에 맞는 리소스에 대해 조치 수행
(set-permission, delete, stop)

3) 로깅 & 보고
실행 결과를 json형태로 s3, CloudWatch 등에 저장

2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING

대응

왜 IaC 구현에서 Terraform은 안 했나요?

Terraform은 선언형 IaC로 인프라 전체를 관리하는 데 강점이 있지만,
단일 리소스·설정 변경을 빠르게 반영하는 시나리오에서는
Custodian/Ansible이 더 단순하고 효율적.

MCP에서 자연어 → 액션 변환 시, Custodian/Ansible은
단일 Playbook/Policy 파일 생성으로 즉시 실행 가능.

이번 버전은 보안 점검 → 즉시 대응이 목적이어서
필요한 리소스만 신속히 수정 가능한 툴을 선택.

분석에서 실행까지 – 스캔 결과를 IaC 도구로 즉시 사용할 수 있는 수정 조치로 전환

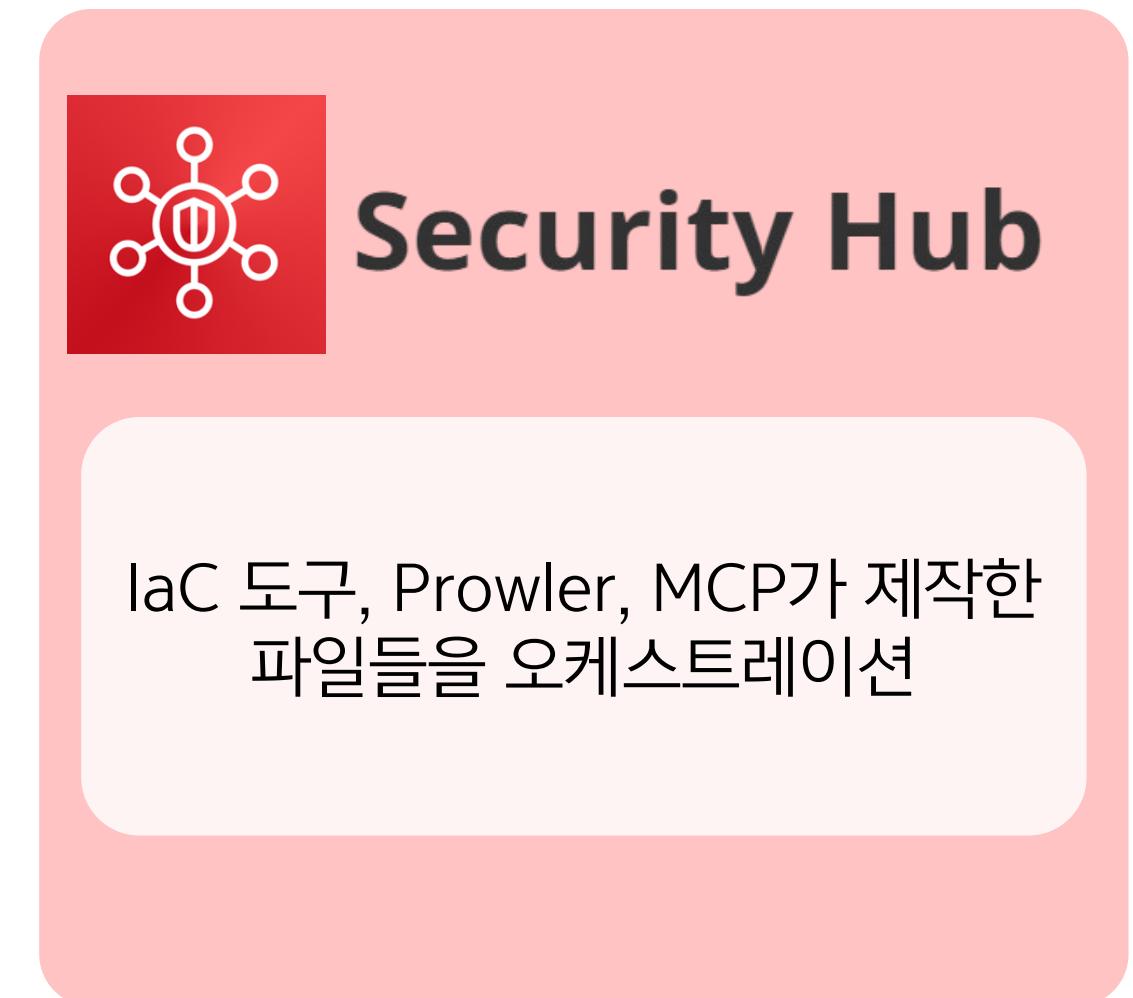
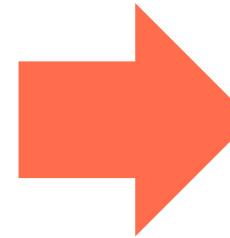
2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING

알림



모든 MCP 플로우와 IaC 드라이런 결과를 Slack 알림으로 전달

2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING

알림

MCP에서 dry run 자동 기능을 제거하고
별도 대시보드를 제작한 이유?

처음에는 “딸깍” 하면 모든 대응이 자동화되는 도구를 만들고자
대화 안에서 Custodian Run까지 되게 하려고 하였음

보안적으로 안전하지 않다고 팀 내부에서 판단 → MCP는 custodian yaml 파일까지 제작,

yaml 파일에 사용자가 credentials을 직접 추가한 후 대시보드에서 dry run할 수 있게 함

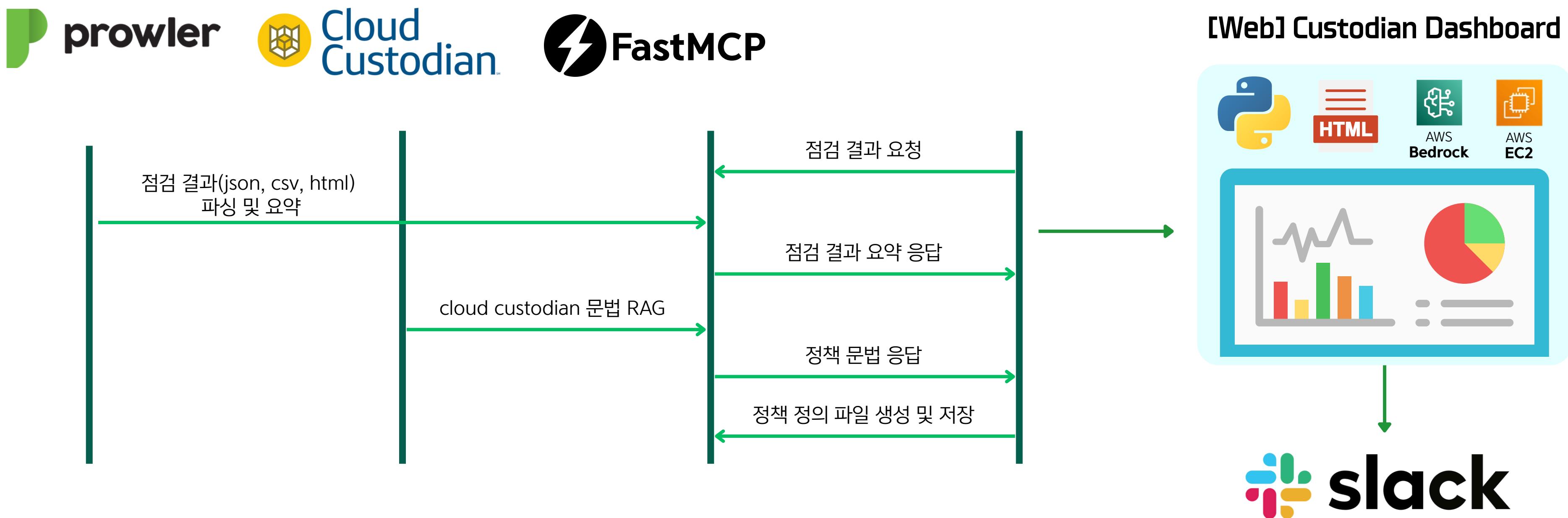
파일 읽기/쓰기 + yaml 생성 등 중요한 워크플로우 및 주요 위험사항 등 중요 보안내용은
Slack 알림까지!

2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING



2.2 CLAUDE DESKTOP MCP 제작

: AI 및 SASS 사용의 허가

INTRO

MCP 제작

CLOSING

제작한 MCP의 tool(함수) :

get_latest_file

analyze_html_file

analyze_csv_file

analyze_json_file

analyze_prowler_results

get_prowler_reports_list

get_security_summary

get_cloud_custodian_aws
_resource_reference_html

write_yaml_file

create_yaml_directory

list_iac_files

get_iac_file_content

notify slack,
auto dry run laC,
analyze laC run results

2.2 CLAUDE DESKTOP MCP 제작

INTRO

MCP 제작

CLOSING

: 오픈소스로 공개!

The screenshot shows a GitHub repository page for 'Compler_MCP'. The repository is public and has 25 commits. The commits are listed as follows:

- Merge pull request #1 from comproowler/fix/add-prowler-server (woohyun212) · 8e4f87e · 3 weeks ago
- Update parser.py (src) · 3 weeks ago
- Update README.md (README.md) · 3 weeks ago
- feat: initialize uv project-compler with main function and pro... (main.py) · 3 weeks ago
- feat: add function to generate HTML reference for AWS reso... (pyproject.toml) · 3 weeks ago
- feat: implement HTML parsing for Prowler results and updat... (requirements.txt) · 3 weeks ago
- Update run.bat (run.bat) · 3 weeks ago
- feat: add function to generate HTML reference for AWS reso... (uv.lock) · 3 weeks ago

The repository has 4 stars and 0 forks. The README file contains the following text:

Prowler MCP Server for Claude Desktop by Compler

This is an MCP server that analyzes Prowler security scan results.

Features

- `get_latest_prowler_file` : Retrieve latest file information
- `analyze_prowler_results` : Detailed security analysis (now)

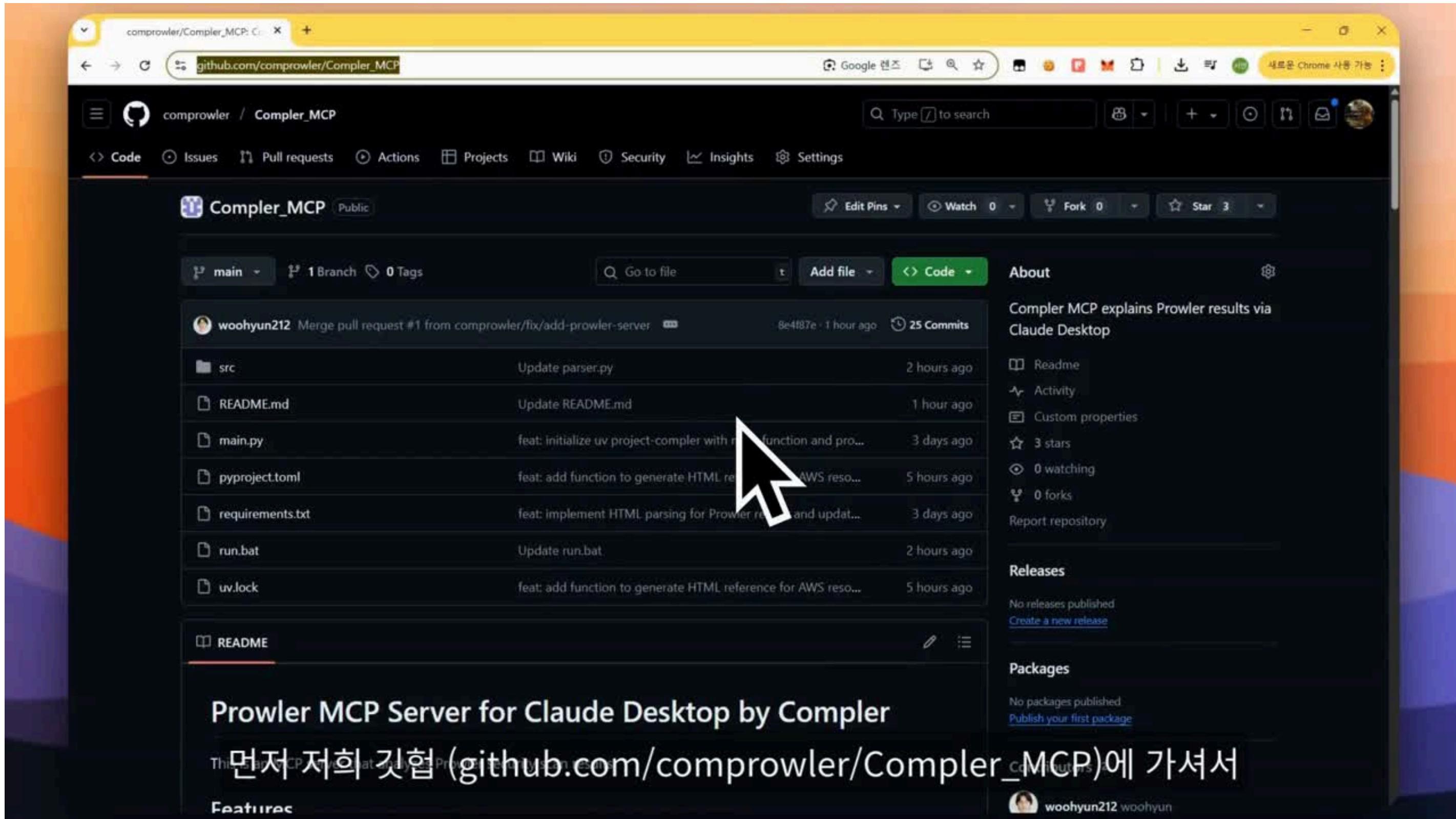
The right sidebar provides repository statistics and links to 'About', 'Releases', 'Packages', and 'Contributors'.

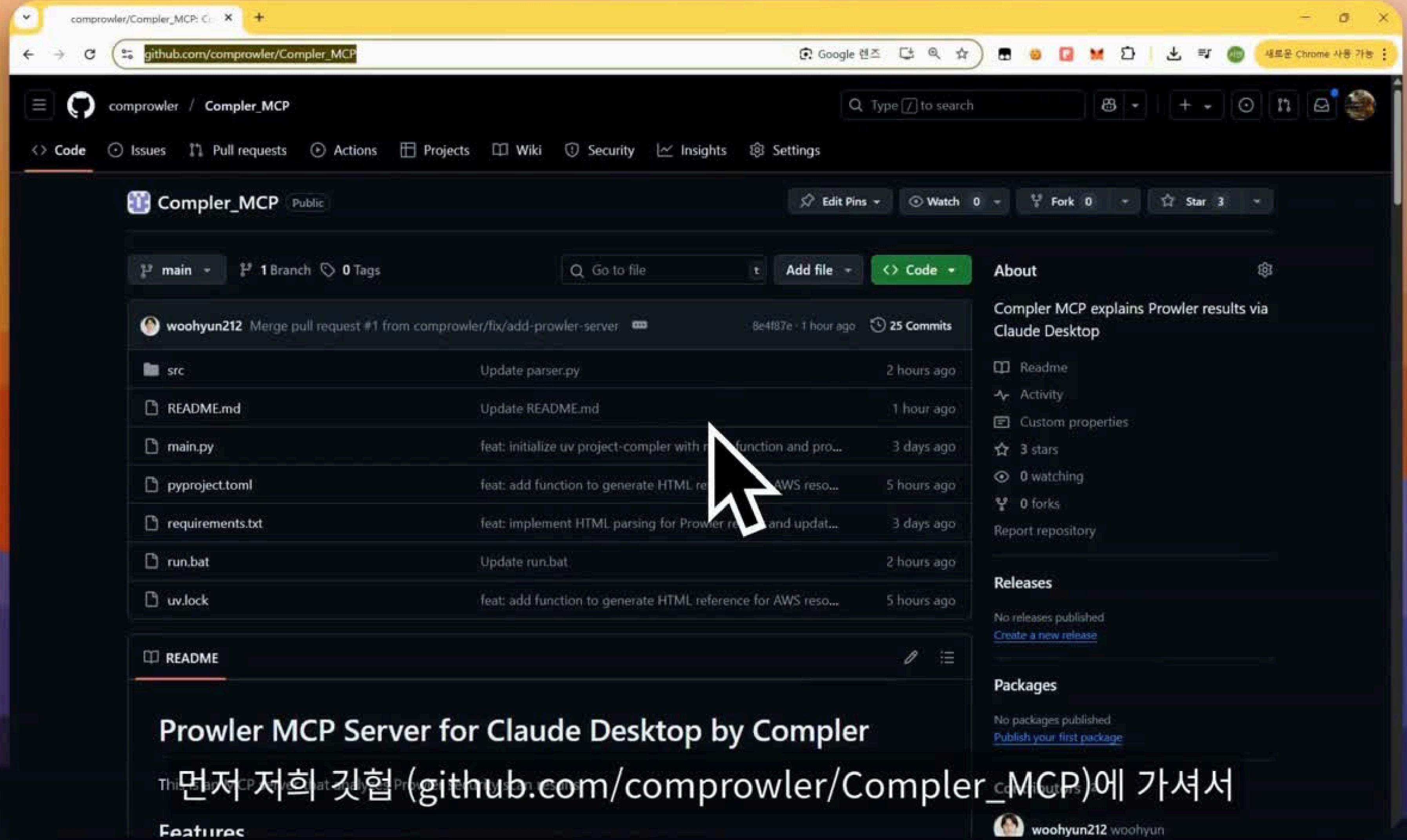
2.4 시연영상

INTRO

MCP 제작

CLOSING





3. CLOSING

3.1 향후계획



3.2 향후계획

INTRO

MCP 제작

CLOSING

:커뮤니티에서 요청받은 기능 추가 및 QA 진행, 가능하다면 망분리 환경에서 사용할 수 있는 로컬 MCP까지

6개의 댓글



Chandrapal Badshah 7월 26일 오후 1:08

This is a cool project 🤝. I have a few questions:

1. The tools parse Prowler output files. Do you plan to extend it with Prowler App APIs?
2. There are around 10 tools. The performance of LLMs degrade with increasing number of MCP tools. In the Claude demo are you using Prowler along with other MCP tools? Is Claude able to pick up right tools all times? Have you setup some automated evaluation to see that LLM picks right tools always?

Prowler App API 지원 확대

MCP tool 통합

비슷한 기능을 가진 MCP 도구들을 병합해 claude에 노출되는 도구의 개수를 줄여 간소화 및 최적화

사용자 가이드 제공

최적의 결과를 얻을 수 있도록
프롬프트 가이드라인과
효과적인 프롬프트 예시 제공 예정

품질 보증(QA) 테스트 강화

도구가 올바르게 호출되는지 확인
MCP 도구 선택 문제 및
Claude의 환각(hallucination) 가능성 최소화

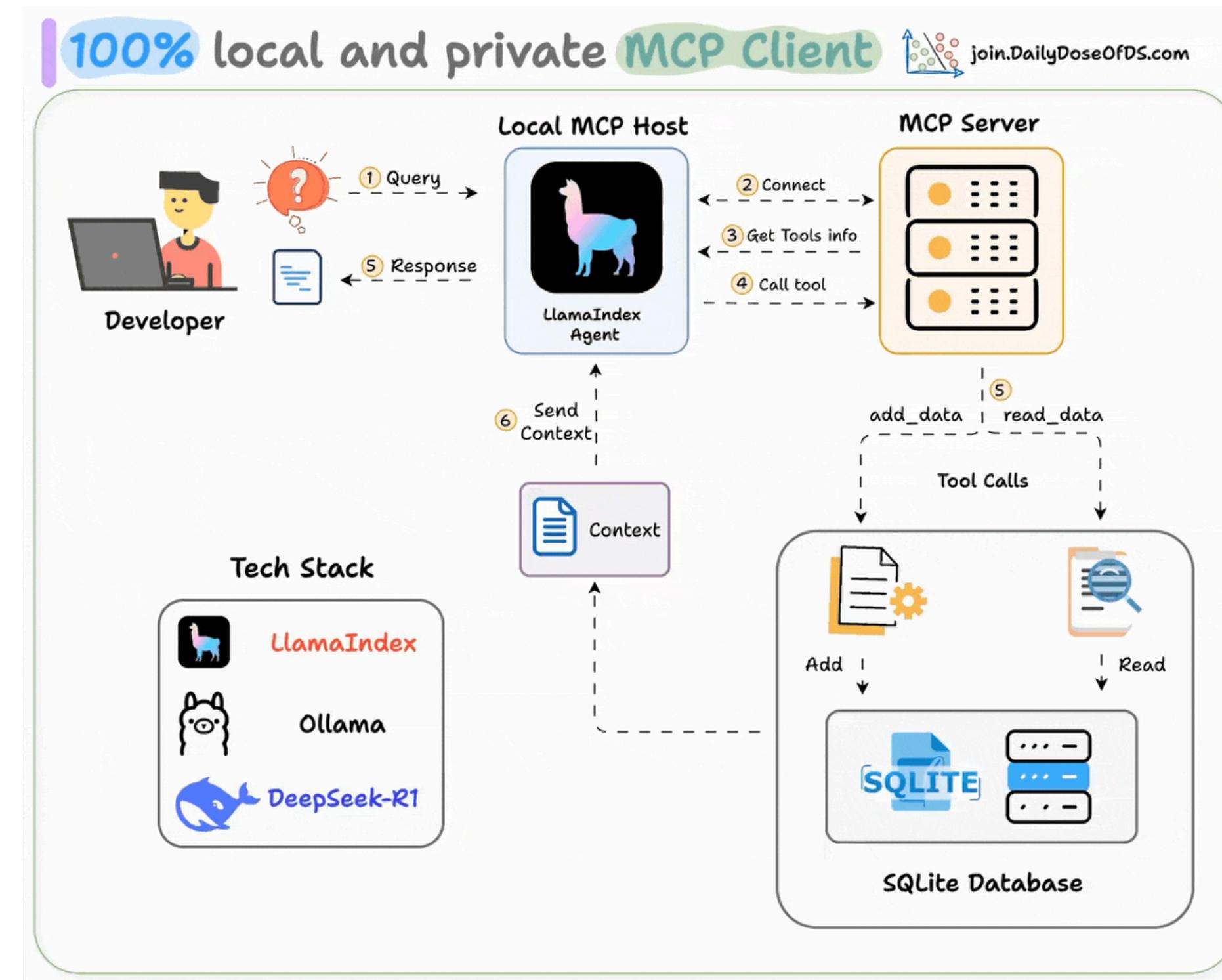
3.2 향후계획

INTRO

MCP 제작

CLOSING

:커뮤니티에서 요청받은 기능 추가 및 QA 진행, 가능하다면 망분리 환경에서 사용할 수 있는 로컬 MCP까지



#AWSKRUG

Prowler MCP 개발 및
AWS 취약점 점검 / 조치 자동화 아키텍처
구성기 ↗

Thank you for
Watching!

#AWSKRUG

Prowler MCP 개발 및 AWS 취약점 점검 / 조치 자동화 아키텍처 구성기 ↗

Q & A