re:Inforce 2023 RECAP

Eunsu Shin

Security Specialist, Principal Solutions Architect

AWS re:Inforce

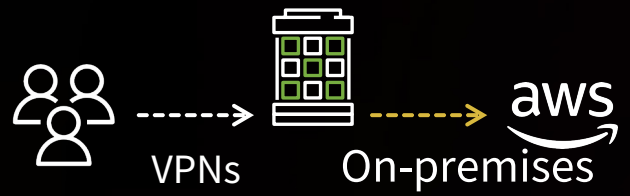
JUNE 13 - 14, 2023 | ANAHEIM, CA

Amazon Verified Access

GA Seoul

편리하지만 더욱 안전한 접속 환경

온프레미스 네트워크 경유



AWS Direct Connect
AWS Site-to-Site VPN

직접 연결

AWS
Client VPN

상세 접근 제어

어플리케이션 별 접근 정책
브라우저 기반 접근
Agentless

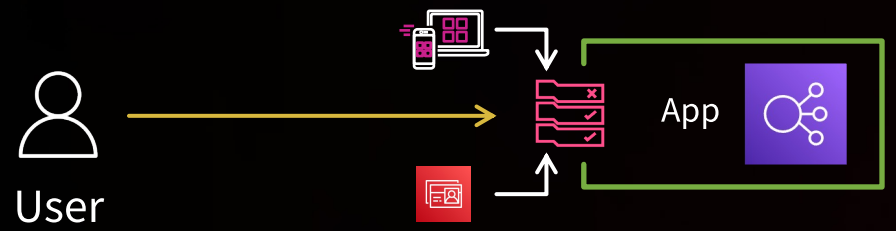
Zero Trust 구현을 위한 고객의 선택

GA Seoul

내부 어플리케이션에 대한 Zero Trust 연결

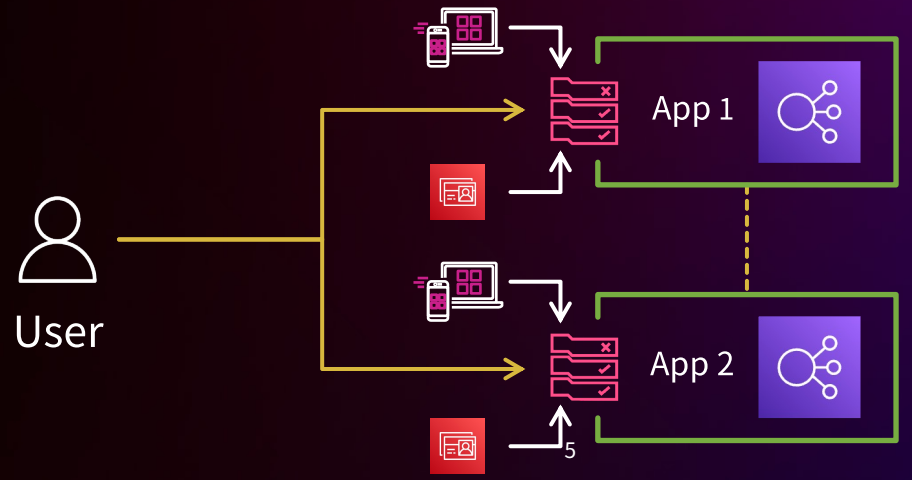
Zero Trust 는 디지털 자산과 관련한 보안 통제에 있어 전통적으로 사용하던 네트워크 보안 경계나 통제 수단에 의존하는 것이 아닌 보안 통제를 제공할 수 있는 여러 매커니즘을 연계하는 접근제어 모델을 말합니다.

접근 권한을 확인하기 위해 추가 정보를 활용



더 많은 소스로부터 더 높은 신뢰도 확보

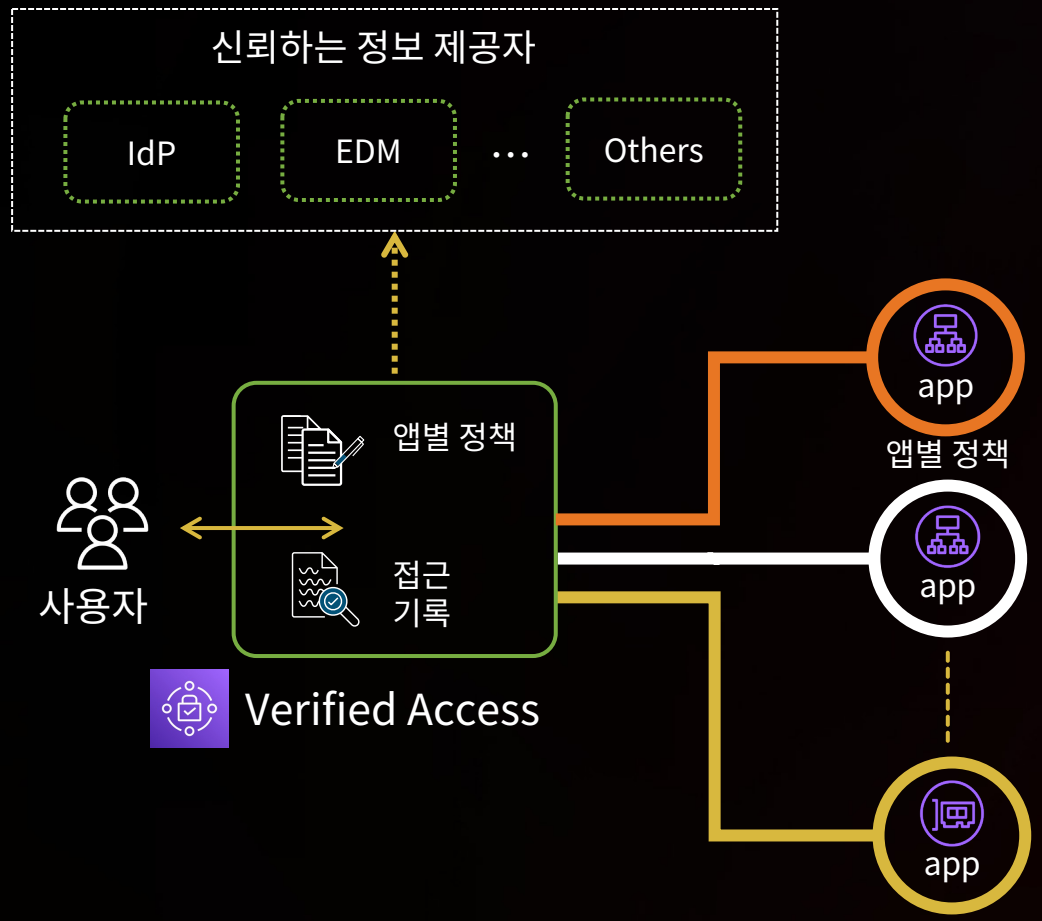
지속적인 검사



각 요청에 대해 평가

GA Seoul

내부 어플리케이션에 대한 보안 강화



상세하고 동적인 인가

각 요청에 대해 어플리케이션(앱)별 정책 평가

관측 가능성 개선

보다 빠른 사고 대응 및 감사, 규정 준수

기존 보안 서비스 사용

업계의 주요 자격증명 공급자 및 단말 보안 솔루션과 연계

GA Seoul

AWS 파트너 솔루션과의 통합

Verified Access

앱별 정책

접근 기록

신뢰하는 공급자

IdP 파트너 – 사용자의 보안주체 정보 제공

단말기 보안 파트너 – 단말에 대한 컨텍스트 제공

컨텍스트 데이터 제공자 – 행위기반 분석, 지역 정보 등과 같은 부가적인 정보 제공

SIEM/관측 가능성 제공자

위험 분석 및 전체적인 가시성 확보

관리형 연결 제공자

관리형 연결 서비스 제공

Amazon Verified Permissions

GA Seoul

Amazon Verified Permission 소개

어플리케이션에 대한 상세한 인가 및 권한 관리

외부 인가 정책및 스키마 관리

빌드 동적이며 빠른 인가 결정 구조를 기반으로한 Zero Trust 아키텍처를 지원하는 어플리케이션 구현

통합 사용자 프로파일, 속성 및 그룹 정보 등을 기존 계정 공급자와 동기화

거버넌스 정책 생명주기에 기반한 어플리케이션 및 데이터에 대한 상세한 권한 관리

간소화 잉여권한 부여에 대한 감사 및 워크플로우에 대한 모니터링을 확장성 있는 환경에서 구현

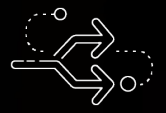
분석 강력한 자동화된 추론 기법을 기반으로 어플리케이션에서 사용되는 수많은 권한에 대한 분석

GA Seoul

동적인 인가를 구현하기 위한 정책 기반 접근 제어

정교함

개별 자원 및 사용자 레벨까지 접근 정책을 세분화



실시간

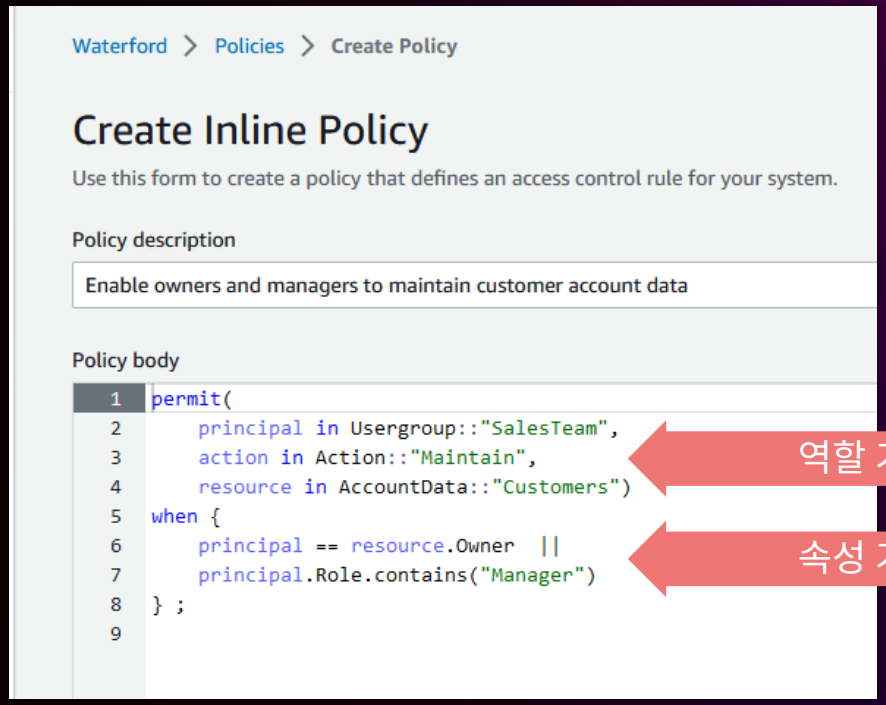
보안 주체나 자원의 현재 속성에 기반하여 접근에 대한 의사 결정을 진행

확장성

어플리케이션 코드에 대한 변경 없이 사용자 권한 관리가 가능하며 사용자 권한에 대한 정책을 보다 쉽게 이해하고 관리 가능

사용자 관리 접근

사용자가 어플리케이션 자원에 대한 접근 권한 위임 가능



GA Seoul

Authorization as a Service

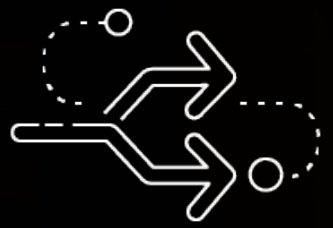
정의

관리자는 여러 정책에 대한 중앙 저장소를 관리

사용자는 실시간으로 정책을 생성하여 어플리케이션 내의 권한을 관리

거버넌스

관리자는 거버넌스 요건을 만족하고 각종 규정 준수 요구사항을 준수하기 위하여 수백만 개의 권한에 대한 분석 및 테스트 가능



결정

각 정책은 개별 접근에 대한 허용여부를 실시간으로 평가하여 밀리초 이내에 결정

적용

Amazon API Gateway 나 AWS AppSync 와 같은 서비스와 통합하거나 이용하여 어플리케이션에 대한 접근 허용 여부를 적용

Amazon Inspector 코드 스캐닝

Amazon Inspector

Amazon Inspector는 소프트웨어 취약성과 의도하지 않은 네트워크 노출에 대해 워크로드를 지속적으로 스캔하는 자동화된 취약점 관리 서비스

- Agent 기반 – 어플리케이션 보안 수준 진단
- 빌트인 진단규칙 패키지
- 보안 진단 결과 – 가이드 제공
- API 를 통한 대응 자동화

스캐닝 인프라를 별도로 구축하는 것이 비싸거나 효과적이지 않기 때문에,Inspector 는 자동화되고, 반복적으로 적용하여 비용을 절감하고 효과적으로 보안성을 높이도록 제작됨.

고객 서버, 서비스, 인프라의 보안을 강화하는데 주력해온 AWS의 보안 노하우를 활용.

구체적으로 실행 가능한 해결책에 대해 자세하게 가이드.

GA Seoul

Lambda 함수 지원

Lambda 표준 스캐닝

- Lambda 함수에 사용되는 어플리케이션 패키지 디펜던시와 ZIP 으로 패키징된 레이어의 소프트웨어 취약점(CVE)을 식별
- 애플리케이션 기능이 Lambda 서비스에 배포될 때, 초기 스캔으로 수행하고 해당 기능에 영향을 미치는 새로운 CVE가 게시되면 자동으로 다시 스캔

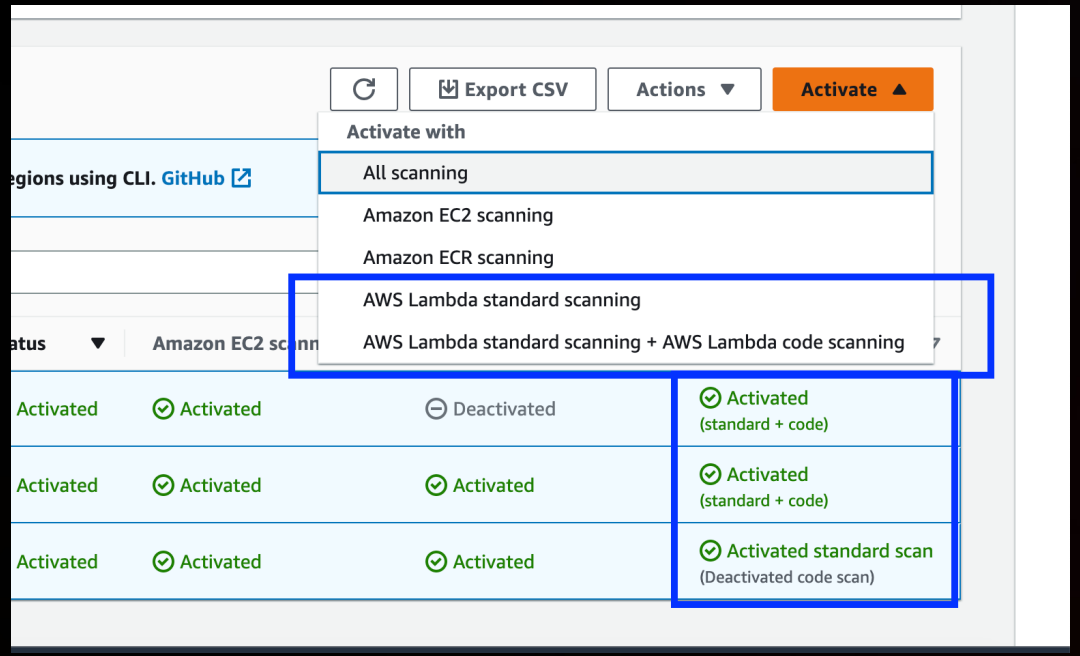
Lambda 코드 스캐닝

- 주입 결함, 데이터 유출, 취약한 암호화 또는 AWS 보안 모범 사례를 기반으로 한 암호화 누락과 같은 코드 보안 취약성에 대해 Lambda 함수 내의 애플리케이션 코드를 스캔
- 애플리케이션 기능이 Lambda 서비스에 배포될 때 수행되는 초기 검사를 수행하고 새로운 코드 탐지기가 라이브러리에 추가되면 자동으로 재검사

GA Seoul

Lambda 함수 지원

Lambda 표준 및 코드 스캐닝 활성화



표준 스캐닝 탐지내역

CVE-2020-26137 - urllib3

Finding ID: arn:aws:inspector2:eu-central-1:674634298277:finding/ae6d2a0f51a315b4e049fcf3a51d18fd

urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). NOTE: this is similar to CVE-2020-26116.

Finding overview	
AWS account ID	674634298277
Severity	Medium
Type	Package Vulnerability
Fix available	Yes
Exploit available	Yes
Last known public exploit at	January 15, 2023 10:14 PM (UTC-08:00)
Created at	November 21, 2022 11:07 AM (UTC-08:00)

Affected packages	
Name	urllib3
Installed version / Fixed version	0:1.24.3 / 1.25.9
Package manager	PYTHONPKG 0:1.24.3 / 1.25.9
File paths	urllib3-1.24.3.dist-info/METADATA

Remediation

Upgrade your installed software packages to the proposed fixed in version and release.

- Update urllib3 to 1.25.9

코드 스캐닝 탐지내역

CWE-200 - Insecure Socket Bind

Finding ID: arn:aws:inspector2:eu-central-1:674634298277:finding/26ac191e607e8c9faa7181183d460867

Binding the socket with an empty IP address will allow it to accept connections from any IPv4 address provided, thus can introduce security risks.

Vulnerability location

```
 9    os.environ['AWS_LAMBDA_FUNCTION_NAME'] =
10    # print("Scenario 1 ends")
11
12    # print("Scenario 2");
13    s = socket.socket(socket.AF_INET, socket
14    s.bind(('',0))
15    # print("Scenario 2 ends")
16
17    return {
18        'statusCode': 200,
19        'body': json.dumps("Inspector Code S
```

Suggested remediation

Binding a socket with an empty IP address causes the bound address to default to 0.0.0.0. This might bind a socket to all interfaces, which opens the socket to traffic from any IPv4 address and creates security risks.Learn more

Amazon Inspector SBOM

GA Seoul

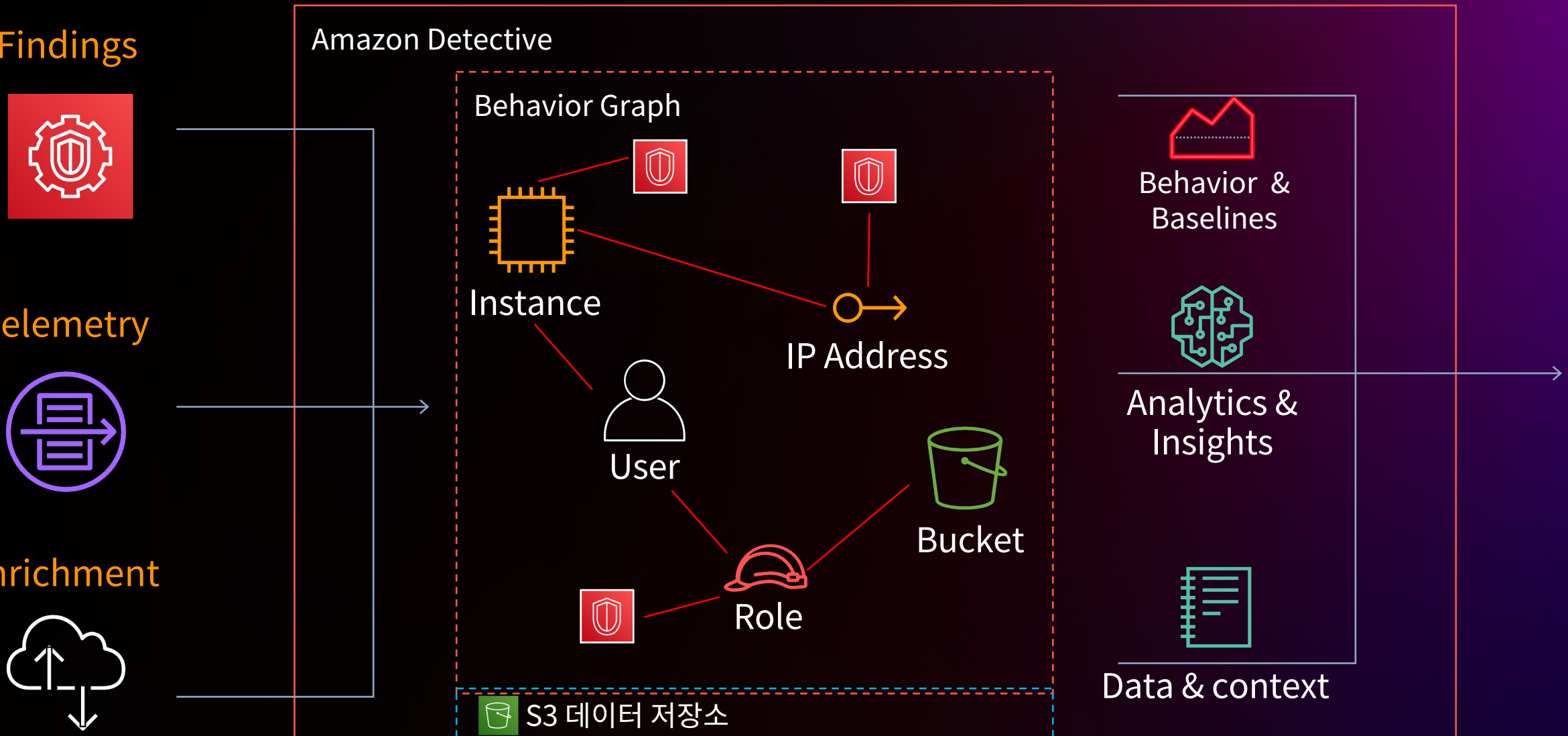
Software Bill of Material(소프트웨어 구성 명세서)

SBOM(Software Bill of Material)은 소프트웨어 구성 요소를 구성하는 "중첩된 인벤토리, 구성 요소 목록"으로 정의됩니다.

- ✓ SBOM 포맷 지원: CycloneDx 및 SPDX
- ✓ SBOM 은 전체 조직에 대한 내용을 내보내기 하거나 리소스처럼 세분화된 내역 기준의 내보내기 가능
- ✓ Inspector 에 의해 모니터링되고 있는 모든 자원에 대해 내보내기 가능
- ✓ 무료

Amazon Detective 탐지내역 그룹

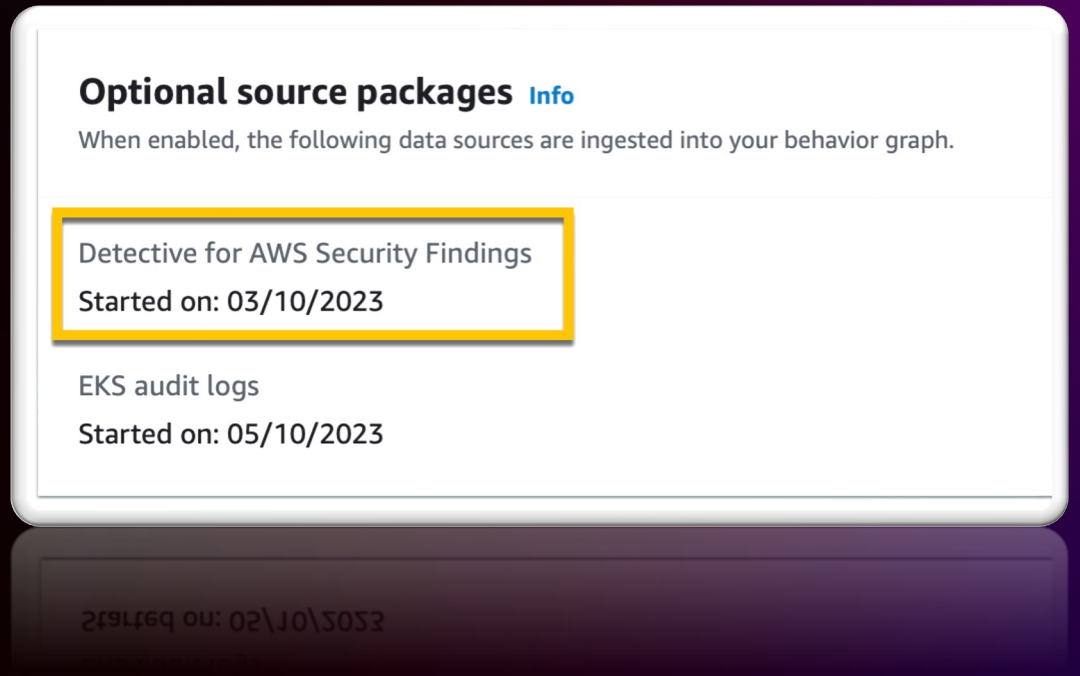
Amazon Detective



GA Seoul

새로운 데이터 소스 및 탐지 내역

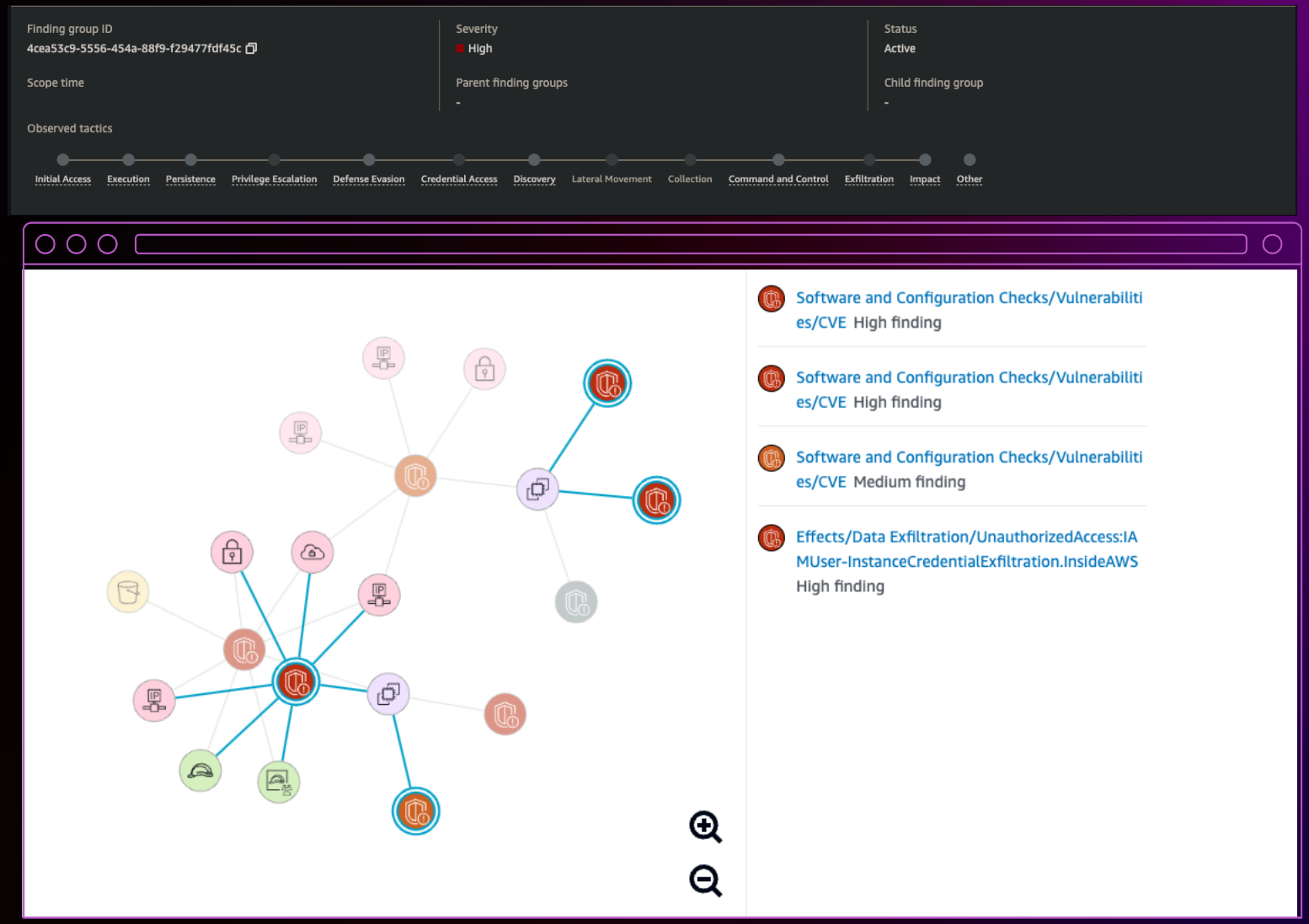
- AWS Security Hub 에 수집된 탐지내역을 Detective 를 이용하여 조사
- Security Hub 를 지원하는 AWS 서비스가 Detective 의 지원 대상
- GuardDuty protection for RDS, Lambda 및 EKS 런타임 모니터링 기능도 추가



GA Seoul

탐지내역 그룹 및 시각화

- 단일 보안 사고와 관련하여 영향 받는 자원을 확인하고 그룹핑하여 탐지내역을 시각화
- 근본 원인을 파악하기 위하여 모든 상세 정보, 활동 이력 등을 단일 공간에서 조사
- 소프트웨어 취약점과 GuardDuty 에서 탐지한 네트워크 노출과 관련한 연관성을 파악하기 위해 Inspector 탐지 내역을 포함



AWS Security Hub 자동화 규칙

위협 탐지 : AWS Security Hub

Insights 및 규정 준수 확인

- 규정 준수 확인 (CIS Foundation v1.2.0, PCI DSS v3.2.1, AWS Foundational Security Best Practice v1.0.0)
- AWS 보안서비스나 3rd Party 보안 서비스에서 탐지한 다양한 보안 탐지 내역을 통합하여 모니터링
- 보안 트렌드에 대한 분석 및 발견된 보안 탐지 내역에 대한 가중치 기준 선별

AWS Security Hub

Findings

보안 탐지 내역 제공 서비스

Amazon Inspector

Amazon GuardDuty

Amazon Macie

AWS Config

Firewall Manager

IAM Access Analyzer

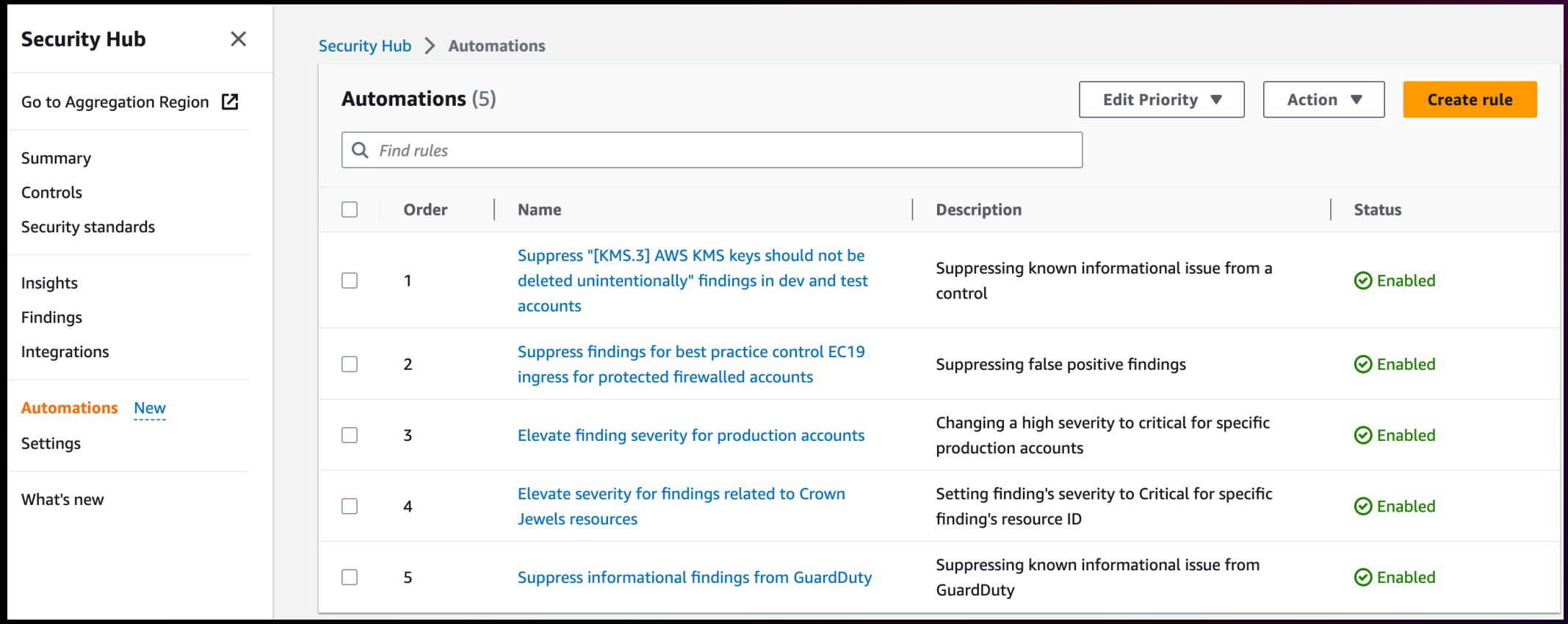
파트너 솔루션

추후 추가 예정

GA Seoul

Security Hub 자동화 규칙

"자동화 규칙" 기능을 이용하여 별도의 코드 작성 없이 Security Hub 탐지 내역에 대한 업데이트, 예외처리와 같은 작업이 가능합니다.

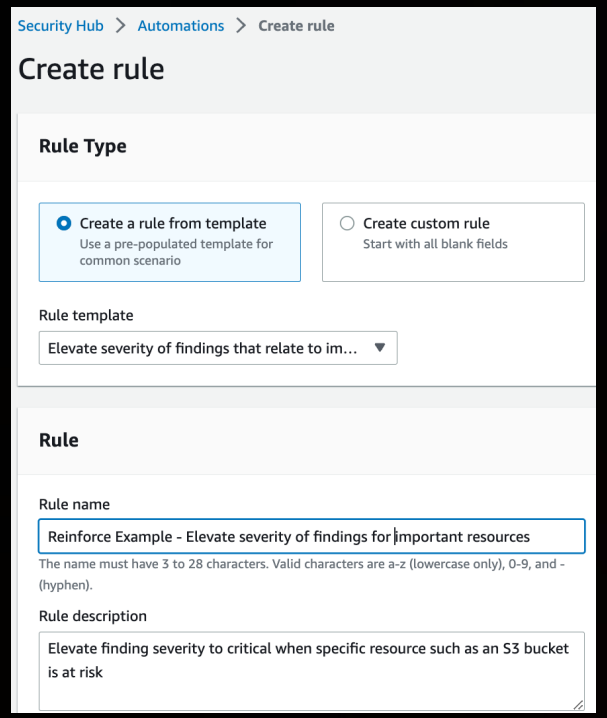


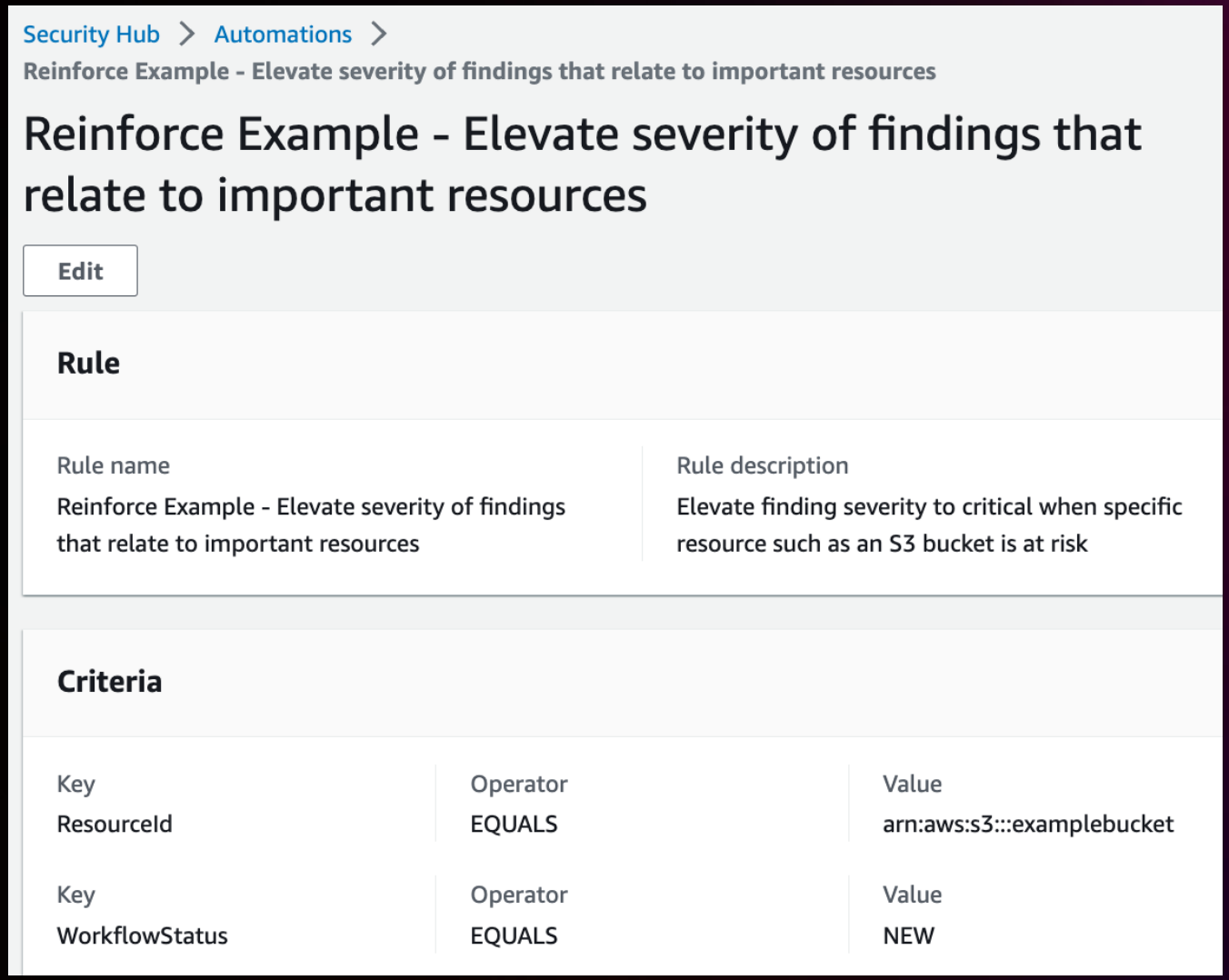
GA Seoul

Security Hub 자동화 규칙

사용 사례:

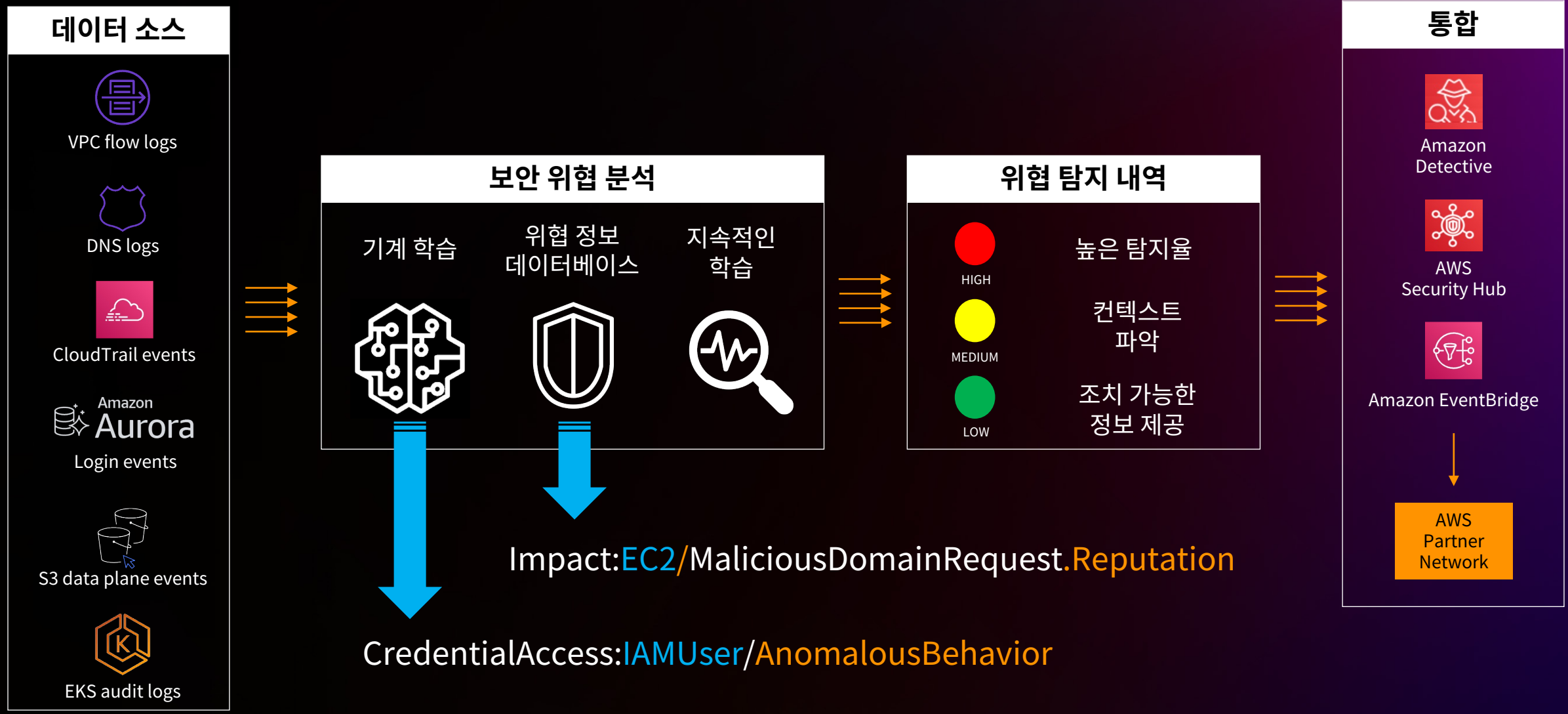
- **탐지내역에 대한 위험도 변경**
- **탐지내역 예외처리**
- **노트 추가**





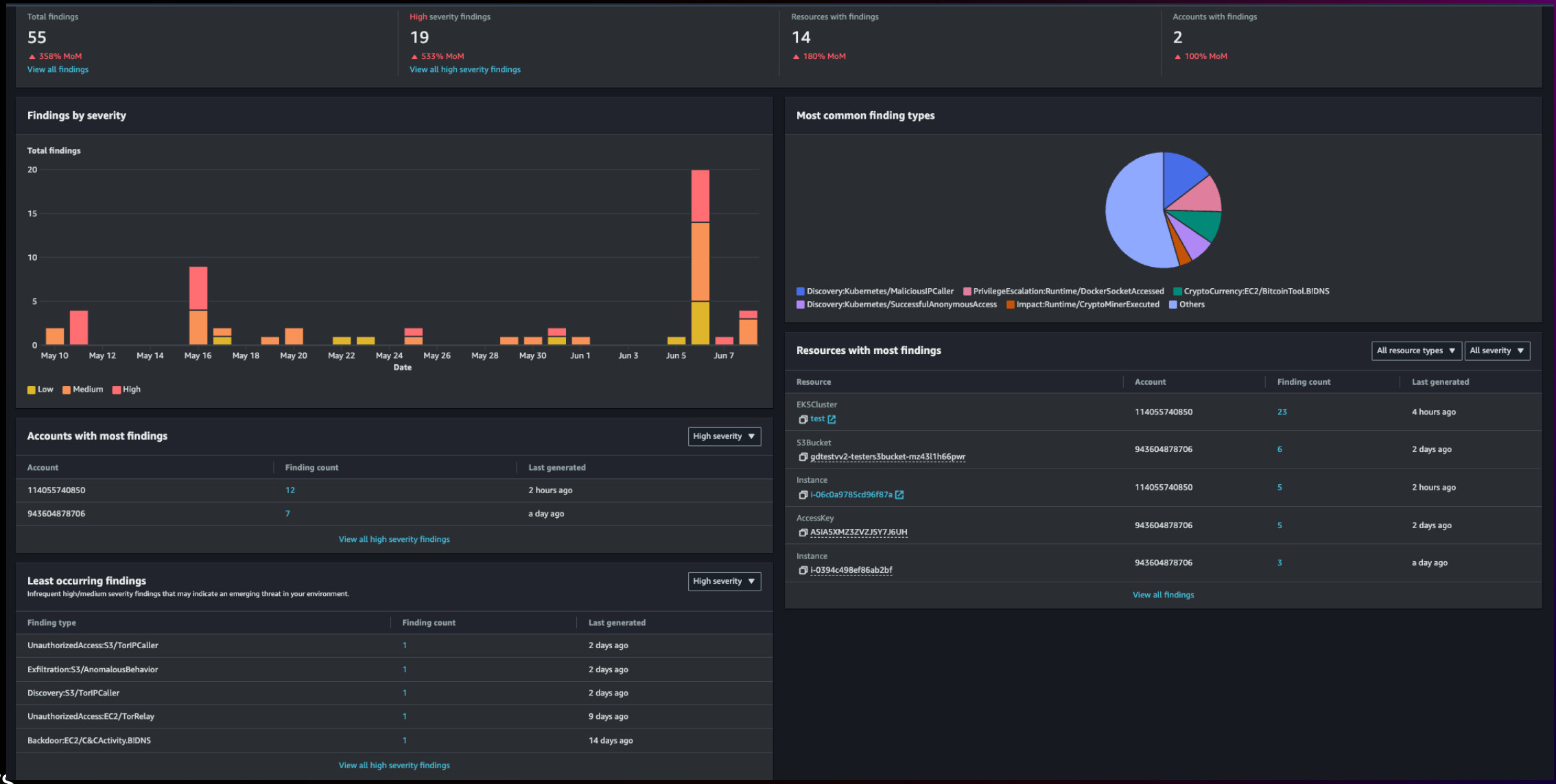
Amazon GuardDuty 요약 보기

Amazon GuardDuty



GA Seoul

Amazon GuardDuty 요약 보기



Amazon S3

GA Seoul

Amazon S3 Encryption

Bucket

S3 Bucket 의 기본 암호화 설정 = SSE-S3 로 변경

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS) 기능추가

Amazon Security Lake

GA Seoul

Amazon Security Lake

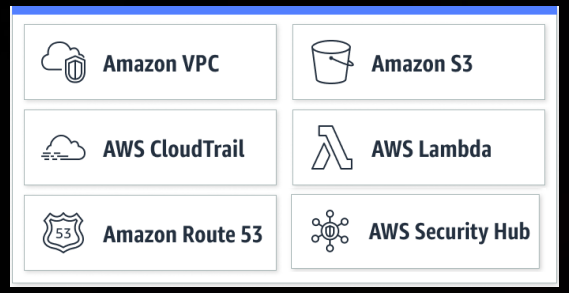
자동으로 보안 데이터에 대한 집중화

- 클라우드, 온프레미스, 서로 다른 리전에 위치한 사용자 정의 보안 자원 등에 대해 자동으로 데이터 집중화 구현
- 보다 효율적인 저장 공간과 질의 성능을 위하여 보안 데이터를 최적화하고 관리
- 다양한 분석 도구에서 활용되고 쉽게 공유될 수 있도록 데이터를 산업 표준 포맷으로 일반화 처리
- 보안 데이터에 대한 소유권과 통제권을 보유한 상태에서 선호하는 분석도구를 이용하여 분석 수행

GA Seoul

Security Lake 동작 원리

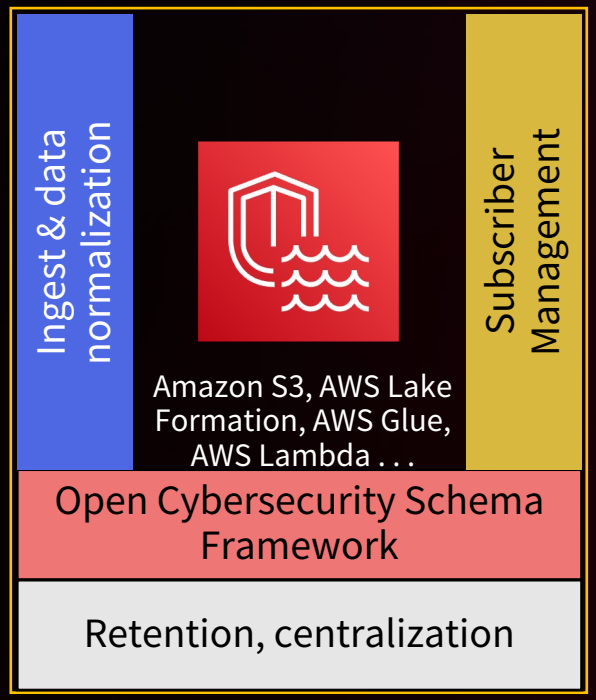
AWS 로그 및 50개 이상의
보안 솔루션의 탐지 내역



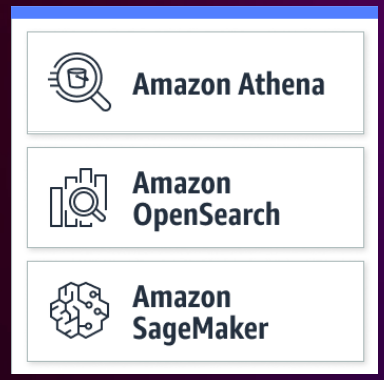
AWS Partner
보안 솔루션

고객의 데이터

Amazon Security Lake



AWS 분석 도구



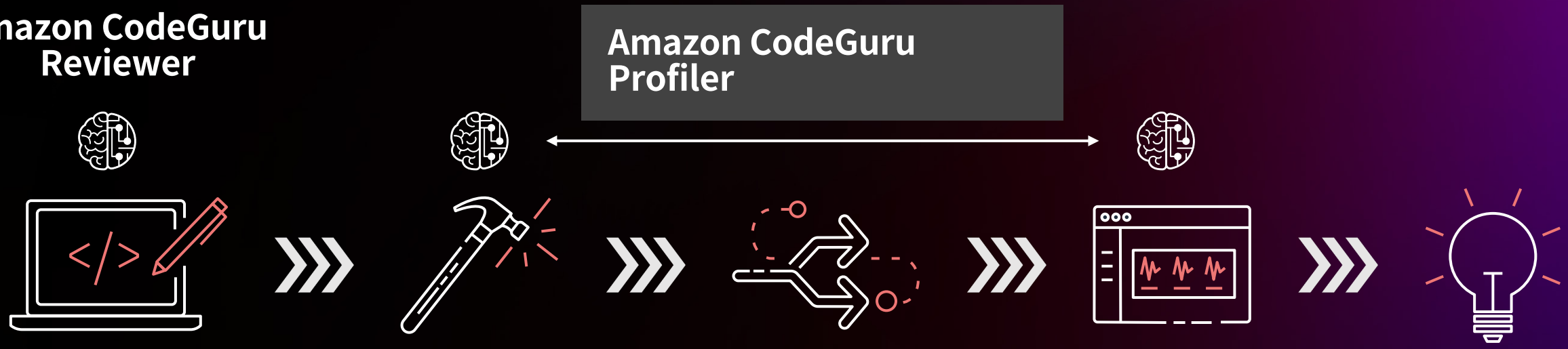
AWS Partner
분석 도구

고객 소유의
관리형 데이터 레이크

Amazon CodeGuru Security

GA Seoul

Amazon CodeGuru



실행 가능한 권장 사항들을 제공하는 빌트인 코드 검토 도구

복잡하고 길게 구성된 코드를 탐지하고 최적화

프러덕션 환경에서 비용 및 성능 개선 사항을 손쉽게 식별

GA Seoul

Amazon CodeGuru Security

- AI/ML 및 자동화된 추론을 기반으로 한 낮은 오탐 비율
- API 기반 설계로 통합, 중앙 집중화 및 확장성 용이
- 버그 추적은 코드 수정 사항을 자동으로 감지하고 사용자 개입 없이 결과를 종료

GA Seoul

대상 영역

- **Java, Python 및 JavaScript**
- **GitHub, GitLab, BitBucket 및 CodeCommit**
- 중요 Open Web Application Security Project (OWASP Top 10) 취약점
- Common Weakness Enumeration 취약점 (CWE Top 25)
- AWS 환경에서 발생할 수 있는 일반적인 보안 취약점

Amazon CodeWhisperer

GA Seoul

CodeWhisperer: ML 기반 코딩 도우미

직전에 사용한 코드나 주석과 같은
컨텍스트 정보를 기반으로 하여 자연어
기반의 권고 코드 제공

- **생성:**
- 컨텍스트에 기반한 완전히 새로운 코드
- 영어 주석을 기반으로 생성된 코드
- 전체 함수
- **주요 IDE 도구에서 확장자를 통해 사용 가능**

```
# Write a function to upload a file to S3.
def upload_file_to_s3(file_name, bucket_name, object_name):
    """
    Uploads a file to an S3 bucket

    :param file_name: File to upload
    :param bucket_name: Bucket to upload to
    :param object_name: S3 object name. If none then file_name is used
    :return: True if file was uploaded, else False
    """

    # Upload the file
    s3_client = boto3.client('s3',
                             aws_access_key_id=AWS_ACCESS_KEY_ID,
                             aws_secret_access_key=AWS_SECRET_ACCESS_KEY,
                             region_name=AWS_REGION_NAME)

    try:
        s3_client.upload_file(file_name, bucket_name, object_name)
        print(f'File {file_name} uploaded to S3 bucket {bucket_name} as {object_name}')
        return True
    except FileNotFoundError:
        print(f'File {file_name} not found')
```

GA Seoul

CodeWhisperer 기능

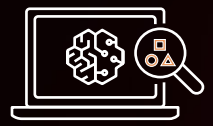
1 개발자 생산성

Languages: C#, Python, Java, JavaScript, TypeScript

IDEs: JetBrains, Visual Studio Code, AWS Cloud9, AWS Lambda console

First-class support for AWS APIs

2 AI 기반



Reference tracker

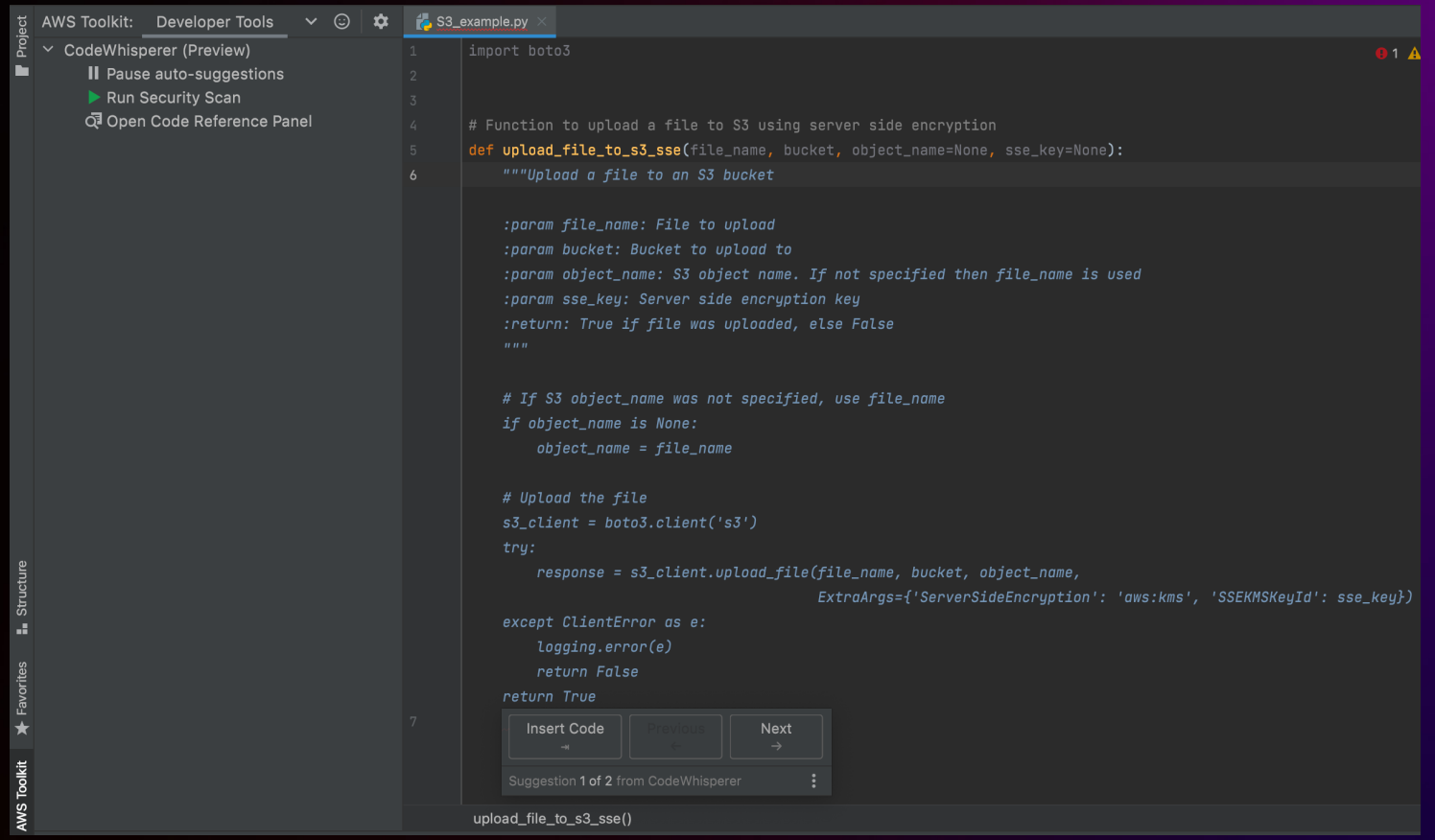
Bias mitigation

Security scan

GA Seoul

AWS 상의 어플리케이션 빌드 간소화

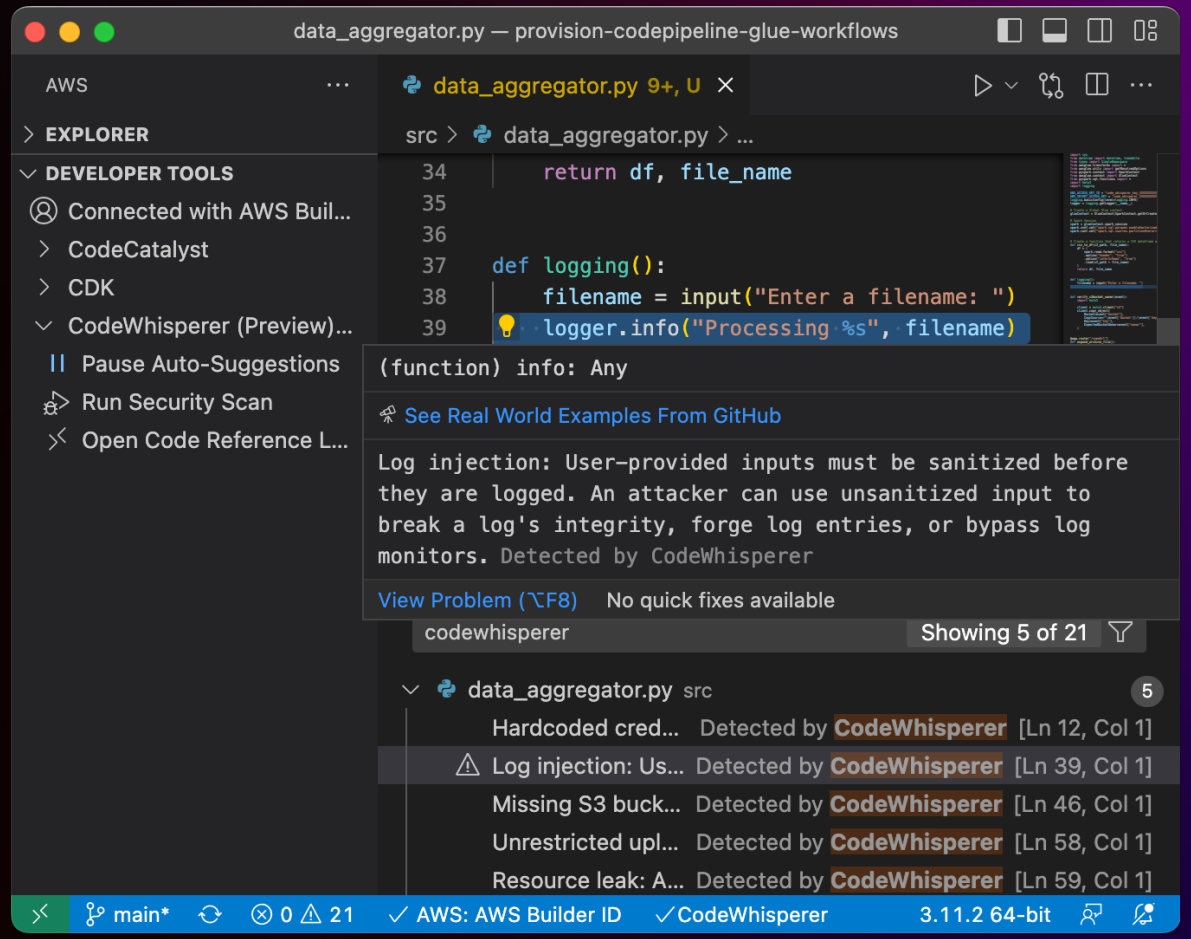
Amazon EC2, AWS Lambda 및 Amazon S3를 포함하여 가장 널리 사용되는 서비스에서 AWS API에 대한 ML 기반 코드 권장 사항 사용



GA Seoul

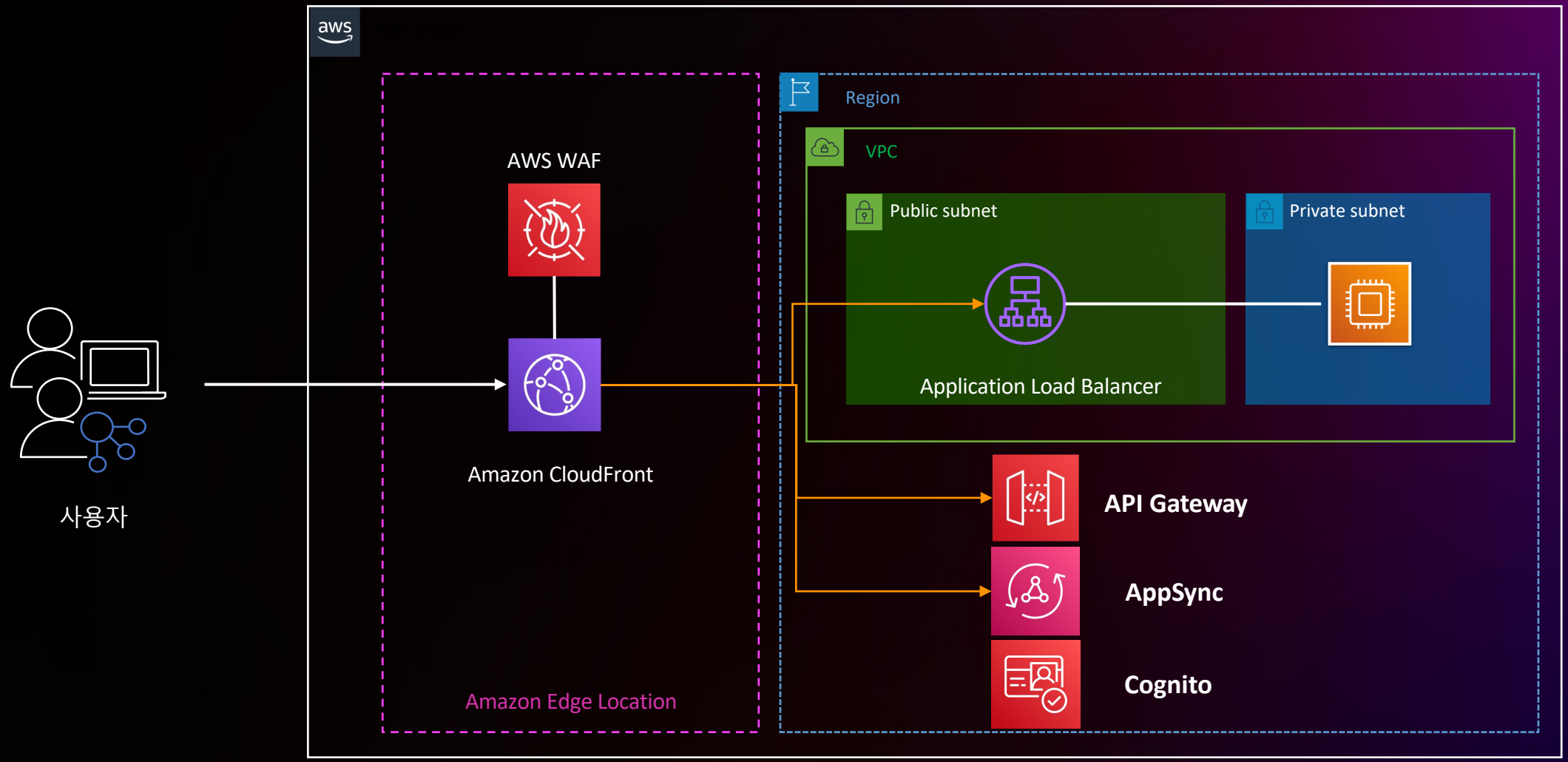
Security Scanning

- 보안 취약점을 탐지하기 위해 생성되거나 개발자가 작성한 코드를 스캔
- 취약점 교정 권고 수신
- 찾기 어려운 보안 취약점에 대해 스캔
- Python, Java, JavaScript 에 대해 VS Code 와 JetBrains IDE 지원



AWS WAF Account Creation Fraud Prevention

AWS WAF



GA Seoul

AWS WAF 계정 생성 사기 예방

사기성 계정 생성 감지 및 완화

- 계정의 오남용 방지
- 피싱이나 다운스트림 사기 방지
- 사람이나 자동화된 봇에 의해 시도되는 과도한 회원가입 시도 차단

- 사기 방지를 위한 다계층 보안 접근
- 평판 정보 및 행위 기반 분석 포함
- 응답 트래픽을 검사

- 직/간접 적으로 비용을 보호
- 어플리케이션에 대한 계층화된 과금 체계

GA Seoul

AWS WAF 의 계정 방어 기능

Account Takeover Prevention + Account Creation Fraud Prevention

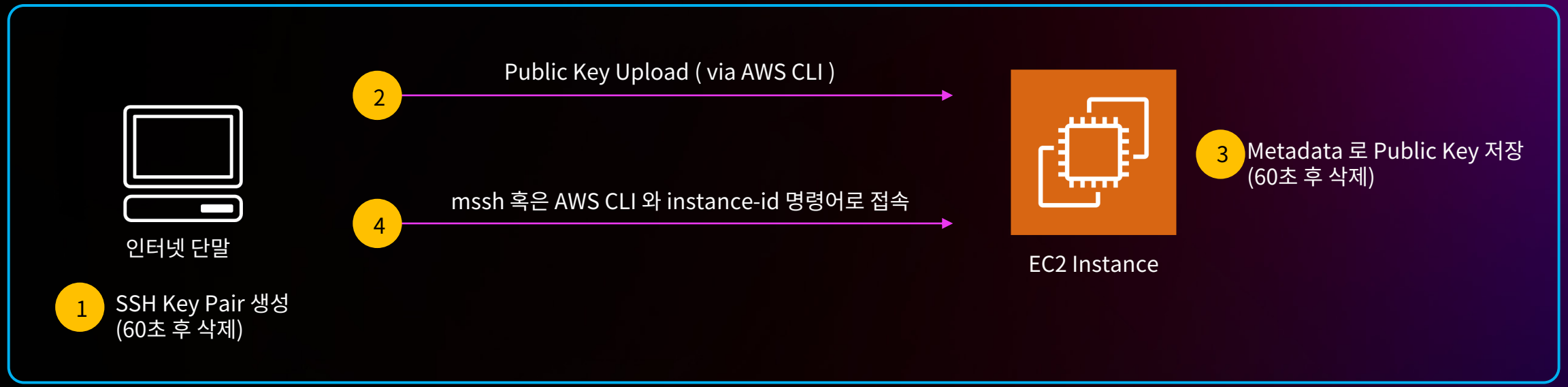
관리형 규칙 기반 계정 사기 차단

Amazon EC2 Instance Connect Endpoint

GA Seoul

EC2 Instance Connect

- EC2 인스턴스 생성 시 Key-Pair 등록 불필요
- 접속에 사용되는 Key-Pair 는 60초간 접속이 가능한 임시 Key 발급
- IAM Policy 를 이용하여 접속 권한 제어



mssh 설치

1. aws s3api get-object --bucket ec2-instance-connect --key cli/ec2instanceconnectcli-latest.tar.gz ec2instanceconnectcli-latest.tar.gz
2. pip install ec2instanceconnectcli-latest.tar.gz

GA Seoul

EC2 Instance Connect Endpoint

AWS EC2 Instance Connect

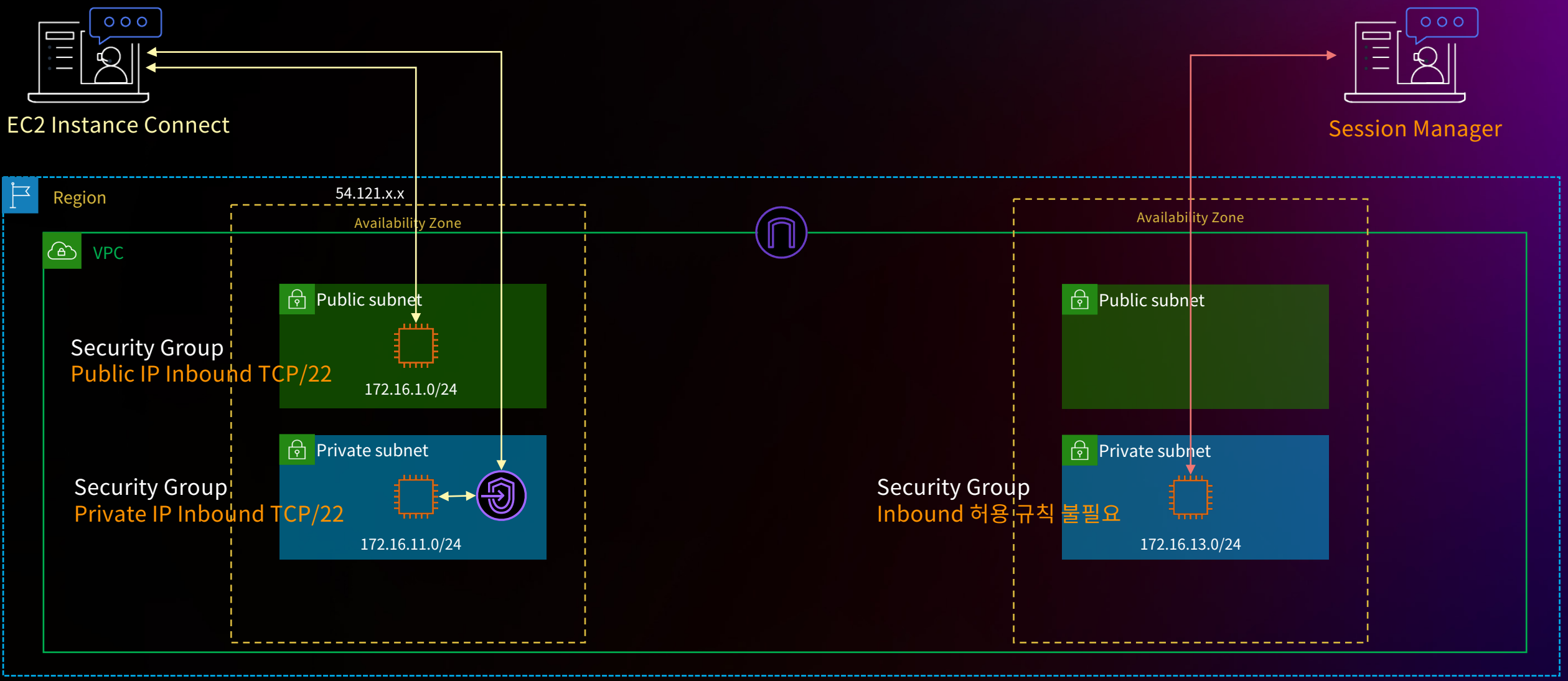
EC2 인스턴스에 대해 공인 아이피나 인터넷 게이트웨이 없이 연결

AWS CLI 나 콘솔, 3rd Party 툴을 이용해서 접속

제로 트러스트 환경을 위해 전통적인 Security Group 기반의 네트워크 통제와 IAM 기반 통제를 함께 사용

GA Seoul

EC2 Instance Connect w/ Endpoint



AWS Private CA Connector for Active Directory

AWS Private CA Connector for Active Directory

GA Seoul
Coming soon!

AWS Private CA

AWS Directory Service

- HSM 기반의 AWS Private CA 를 이용하여 PKI 환경에 대한 복잡도를 감소
- 완전 관리형 서비스를 이용함으로써 PKI 인프라환경에 대한 투자 및 운영 비용 절감
- On-premise AD 및 AWS 관리형 Microsoft AD 에 자동으로 인증서 배포

AWS Payment Cryptography

GA Seoul

AWS Payment Cryptography

탄력적인 결제 암호화 서비스

AWS Payment Cryptography

카드 결제 환경에서 필요한 요구사항을 만족하는 암호화 작업을 수행

PCI 표준 준수를 만족하는 관리형 서비스를 이용함으로써 운영 부담을 감소

AWS API 를 이용하여 기존 카드 결제 어플리케이션과의 손쉬운 통합

PCI 표준을 준수하는 키 교환, 생성, 저장 구현

GA Seoul

AWS Payment Cryptography 동작원리

AWS 결제 암호화는 전통적으로 결제 워크로드를 위해 사용하던 온프레미스 데이터 센터 전용 결제 HSM을 탄력적인 AWS API 서비스로 대체합니다.

- 카드 발급
- 트랜잭션 발생
- 발급자 트랜잭션 처리

AWS Payment Cryptography

- DUKPT를 이용하여 PCI PIN 데이터 변환
- P2PE 데이터 암호화/복호화
- 키 생성, 가져오기, 기타 키 관리
- 카드 및 PIN 데이터 생성 및 검증

Amazon CloudWatch

AWS CloudTrail

GA Seoul

AWS Payment Cryptography 장점

클라우드 마이그레이션 목표를 달성하면서 전용 결제 HSM에 대한 의존성을 제거

PCI(결제 카드 산업) 표준을 충족하도록 구축된 완전 관리형 서비스를 사용하여 운영 부담을 최소화

비즈니스에 따라 탄력적으로 확장되는 용량으로 높은 처리량과 짧은 지연 시간의 암호화 기능 활용

하드웨어 인스턴스를 프로비저닝 할 필요 없이 설정 간소화

AWS Identity Center

IAM Identity Center

자격증명 소스 선택

- Identity Center directory
- AWS Managed Microsoft AD
- okta Identity Platform
- Azure Active Directory
- Other AWS-supported SAML 2.0– and SCIM 2.0–compatible IdP

JumpCloud, onelogin by ONE IDENTITY, PingIdentity, Microsoft Active Directory, CYBERARK

Sync

Authenticate

IAM Identity Center

업무 환경 접근에 대한 단일 공간

다중 계정 권한

다양한 IAM 권한을 관리하는 단일 공간

Access

AWS 계정 (IAM)

어플리케이션 할당

다양한 어플리케이션 접근을 관리하는 공간

Access

AWS 에 통합된 SAML 2.0 앱

정책 관리자 위임

관리자 작업	위임된 관리자 계정	AWS Org 관리 계정
사용자/그룹의 추가, 수정 및 삭제	X	X
사용자 접근 활성화/비활성화	X	X
인입되는 속성의 활성화/비활성화 및 관리	X	X
자격증명 소스 변경	X	X
어플리케이션 생성/수정/삭제	X	X
MFA 설정	X	X
관리 계정에 배포되지않은 권한 집합 관리	X	X
관리 계정에 배포된 권한 집합 관리		X
AWS IAM Identity Center 활성화		X
AWS IAM Identity Center 설정 삭제		X
관리 계정의 사용자 접근에 대한 활성화/비활성화		X
특정 계정을 위임된 관리자 계정으로 등록하거나 등록 취소		X

IAM IdC 에서 새로운 임시 접속 관리를 위한 옵션 제공

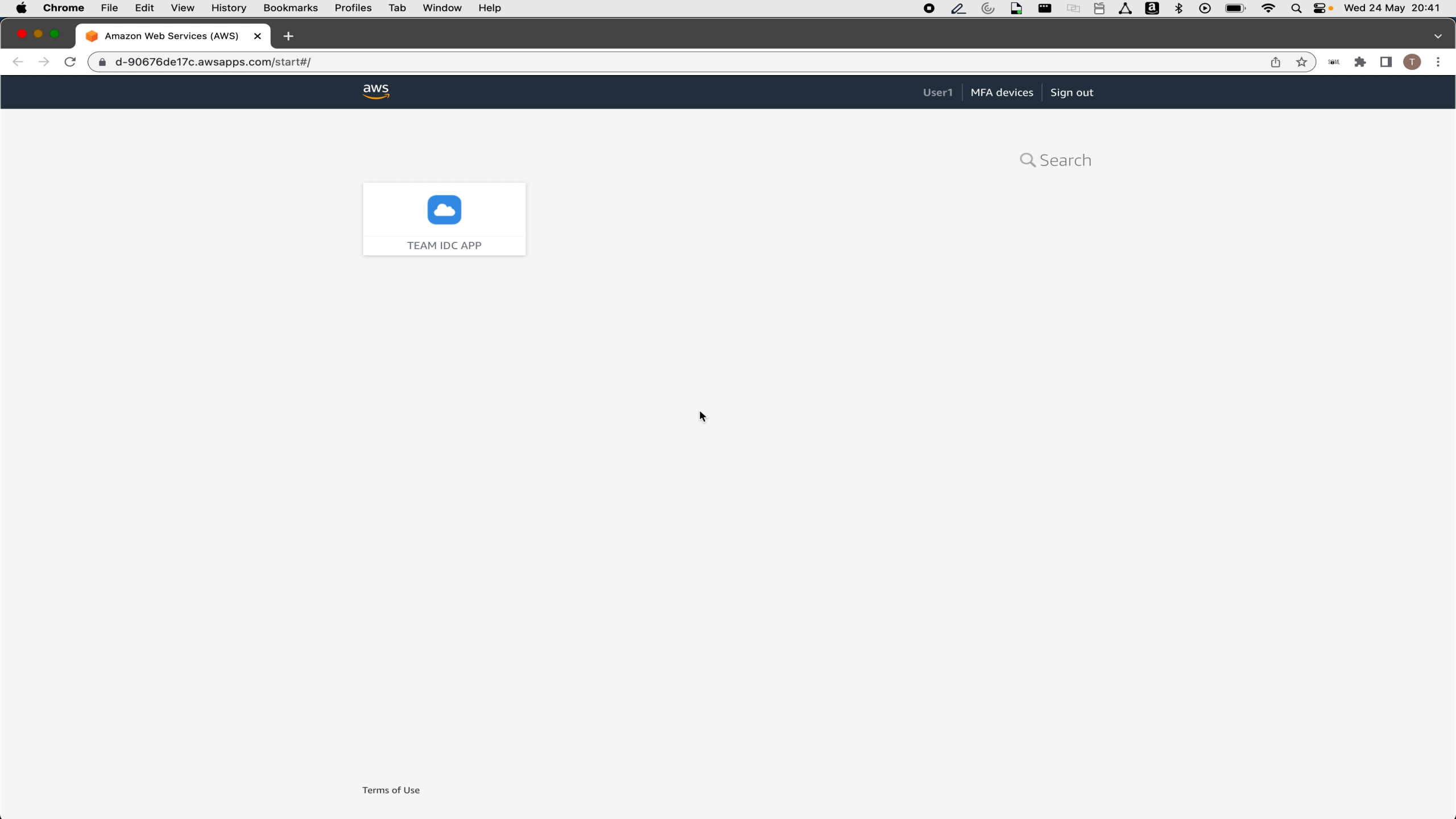
최소 권한 원칙을 준수하는 환경을 구현

Azure AD를 IdP로 사용하는 Identity Center가 있습니다. 시간 제한이 있고 승인된 계정에 대한 높은 액세스 권한이 필요합니다. *- 보안팀*

우리는 사용자에게 JIT 접근 권한 제공를 원합니다. 이를 위해 OKTA 파트너를 찾고 있습니다. *– 금융 고객*

우리는 개발자가 프로덕션 계정에 일시적으로 액세스할 수 있는 기본 솔루션을 원합니다. *- 개발자*

Demo


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed 24 May 20:41
Amazon Web Services (AWS)
d-90676de17c.awsapps.com/start#/
aws
User1
MFA devices
Sign out
Search
TEAM IDC APP
Terms of Use

AWS Cyber Insurance Partners

감사합니다!