

2025.06.28



WHS 팀 프로젝트 중간 발표

클라우드 환경에서 발생하는 로그 기반 침해사고 탐지 환경 구축

AWS지 말라고 했지

팀 구성



MENTOR 송수호



PL 우동규



PM 김기원



강유림



권도원



김진서



박도은



손형은



조민혁



장희영

목차

01 개요

02 프로젝트 목표

03 진행 상황

04 향후 계획

01

개요

프로젝트 배경

주제

클라우드 환경을 이용한 로그 기반 침해사고 탐지 환경 구축

선정 배경

1. 기존 온프레미스 환경에서 벗어나, **클라우드 환경**에서 발생하는 보안 위협에 **능동적으로 대응**하는 경험
2. 실제 사용되는 AWS 서비스 기반 인프라를 활용하여, 현업 수준의 **탐지/대응 역량 강화**
3. 로그 분석을 통해 **정상/비정상 트래픽을 식별**하고 **탐지 시스템을 구축**

기술 스택

Infra



Compute



EC2



Lambda

Storage



S3

Management & Monitoring



CloudTrail



CloudWatch



EventBridge



Config

Security & Access



IAM

Messaging & Notification



SNS

Infrastructure as Code



Alarm Trigger Output



Discord



Email

Team Communication



Kakaotalk



Notion



Discord



Zoom

02

프로젝트 목표

목표

01



실무 역량 강화

02



시나리오 워크북 제작

03



자격증 취득

기대 효과

1

클라우드 인프라 구성요소 실무 이해

2

보안 사고 대응 역량 강화

3

워크북을 통한
다양한 학습자 지원

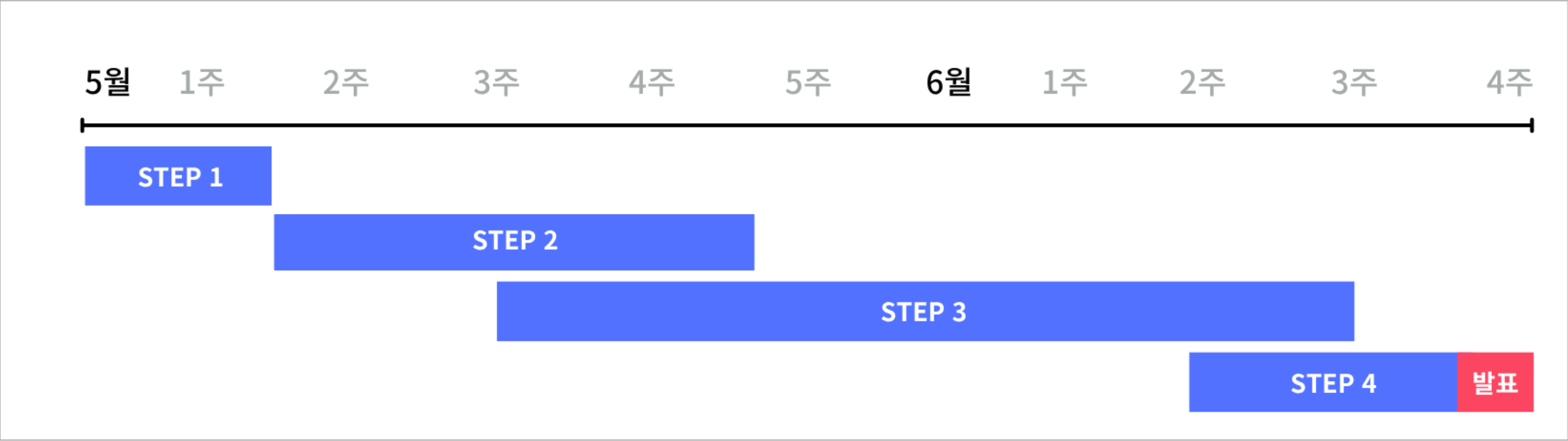
4

자동화 및 실습 환경 표준화

03

진행 상황

프로젝트 진척도



STEP 1
팀원 구성 및 체계 정립

STEP 2
AWS 서비스 학습

STEP 3
초급, 중급 시나리오 구현
및 워크북 작성

STEP 4
중간 발표 준비

프로젝트 진척도

[illegible]

STEP 3

STEP 4

초급, 중급시나리오 구현 및 워크북 작성

중간 발표 준비

선행 학습

1

AWS 주요 서비스

AWS 주요 서비스 간 연계 및 자동화 시나리오 구축 역량을 강화하고, 이벤트 대응 체계를 설계할 수 있는 기반을 마련하기 위해 **S3, EC2, IAM, Config, SNS, CloudWatch, CloudTrail, EventBridge, Lambda** 총 9개 서비스 각각의 기능과 역할을 이해했다.

2

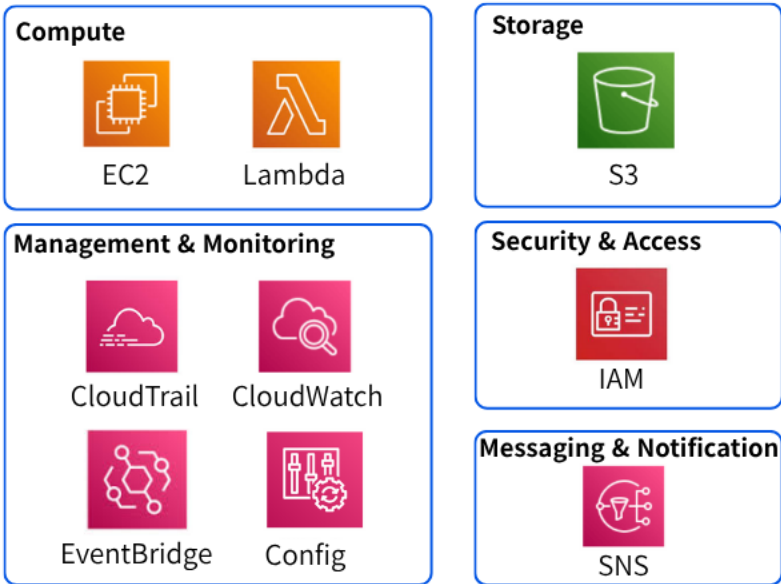
웹 서버 구축 및 테라폼 학습

기본 VPC 환경에서 Subnet, Security Group, EC2 인스턴스를 구성하고 **웹 서버를 설치**하여 서비스를 직접 구축한 뒤, 이를 테라폼 코드로 변환하여 **코드 기반 인프라 구성(IaC)** 경험을 쌓았다. 이 과정에서 테라폼 기본 명령어인 **init, plan, apply, destroy**에 대해 학습하였다.

선행 학습

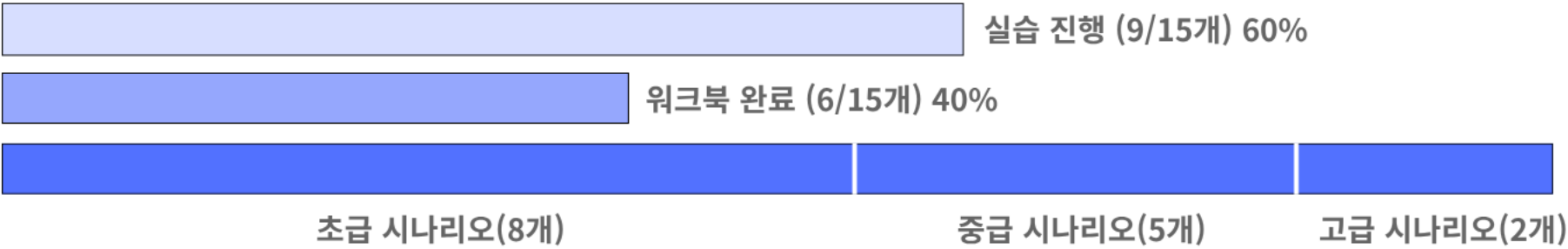
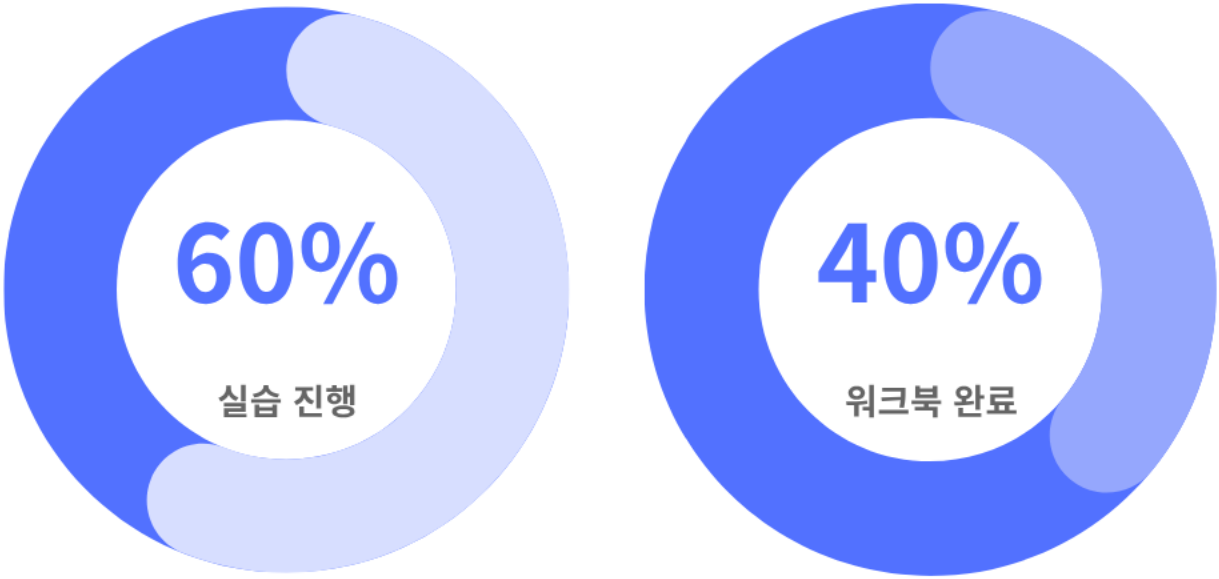
AWS 주요 서비스

AWS 주요 서비스 간 연계 및 자동화 시나리오 구축 역량을 강화하고, 이벤트 대응 체계를 설계할 수 있는 기반을 마련하기 위해 **S3, EC2, IAM, AWS Config, SNS, CloudWatch, CloudTrail, EventBridge, Lambda** 총 9개 서비스 각각의 기능과 역할을 이해했다.



S3	객체 스토리지, 로그 저장 및 아카이브 서비스
EC2	AWS의 가상 서버 서비스, 원하는 컴퓨팅 환경을 구성하여 애플리케이션을 유연하게 배포 및 운영 가능
IAM	AWS 리소스에 대한 인증과 인가 담당 조직 내 사용자, 애플리케이션, 서비스가 어떤 리소스에 어떤 작업을 수행할 수 있는지를 결정
Config	리소스 구성 상태의 변경 추적 및 규정 준수 관리 서비스. 규칙 위반 발생 시 NON_COMPLIANT(비준수) 상태로 전환
CloudWatch	AWS 리소스의 로그를 수집·모니터링하는 서비스
CloudTrail	AWS 계정 내에서 발생한 이벤트를 기록하여, 누가 언제 어떤 작업을 했는지 추적할 수 있는 서비스
EventBridge	Cloudtrail에 기록된 이벤트 중 루트 계정의 콘솔 로그인 이 기록되면 SNS로 전달
SNS	Eventbridge로 부터 이벤트를 수신하고, SNS 를 구독하고 있는 대상(이메일, Lambda 함수)로 알림 전송
Lambda	사전 지정한 외부 Webhook(Slack, Discord 등)으로 메시지를 전달

시나리오 진행률



시나리오 진행률

☒ 진행 완료 ☒ 진행중 ☐ 진행 예정

초급 시나리오 / 기초적인 보안 모니터링

- ☒ S3 퍼블릭 버킷 생성 탐지 및 알람
- ☒ 루트 계정 로그인 알람
- ☒ AWS Cloudtrail 비활성화 탐지
- ☒ Security group의 정책 변경 탐지
- ☒ 새로운 IAM User의 생성, 삭제 탐지
- ☒ 로그 그룹 삭제 또는 변경 탐지
- ☒ 스냅샷 / 자원 공유를 통한 은폐 및 유출 시도 시나리오
- ☒ 계정에 생성된 AMI 를 외부에 공개로 등록하거나 외부 계정에 공유하는 시도 탐지

중급 시나리오 / AWS 서비스를 활용한 서비스 및 보안 모니터링

- ☒ EC2 내 bash history 조작 시도 탐지
- ☐ Athena 기반 CloudTrail 비정상 API 사용 분석
- ☐ Guardduty를 Threat IP List를 활용한 모니터링 정책 구현
- ☐ AWS WAF를 정책 관리 시나리오 및 모니터링 정책 구현
- ☐ Security group의 정책 변경 탐지

고급 시나리오

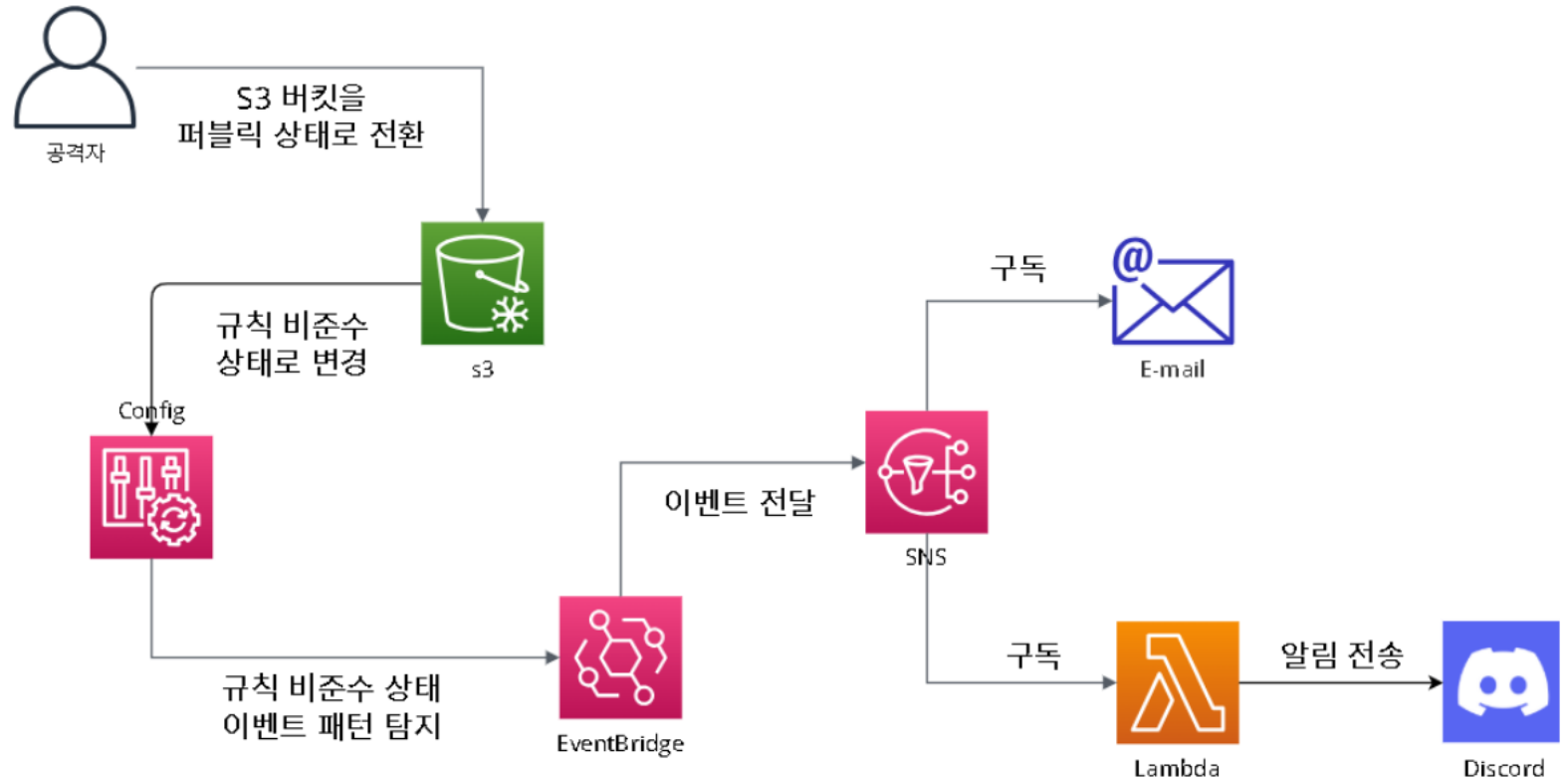
- ☐ 상용 SIEM을 활용한 이벤트 수집 및 분석
- ☐ Guardduty 탐지 기반 자동화 대응

초급 시나리오

S3 퍼블릭 버킷 생성 탐지 및 알림

학습목표

S3 버킷은 정적 웹 서비스 용도로 사용하는 것 외에는 업무 목적이나 민감정보가 포함될 수 있어 관리가 필요하다. 이에 S3 버킷이 **외부로 공개(Public)** 되었을 경우 탐지해 **알림**을 보내는 체계를 구현한다.

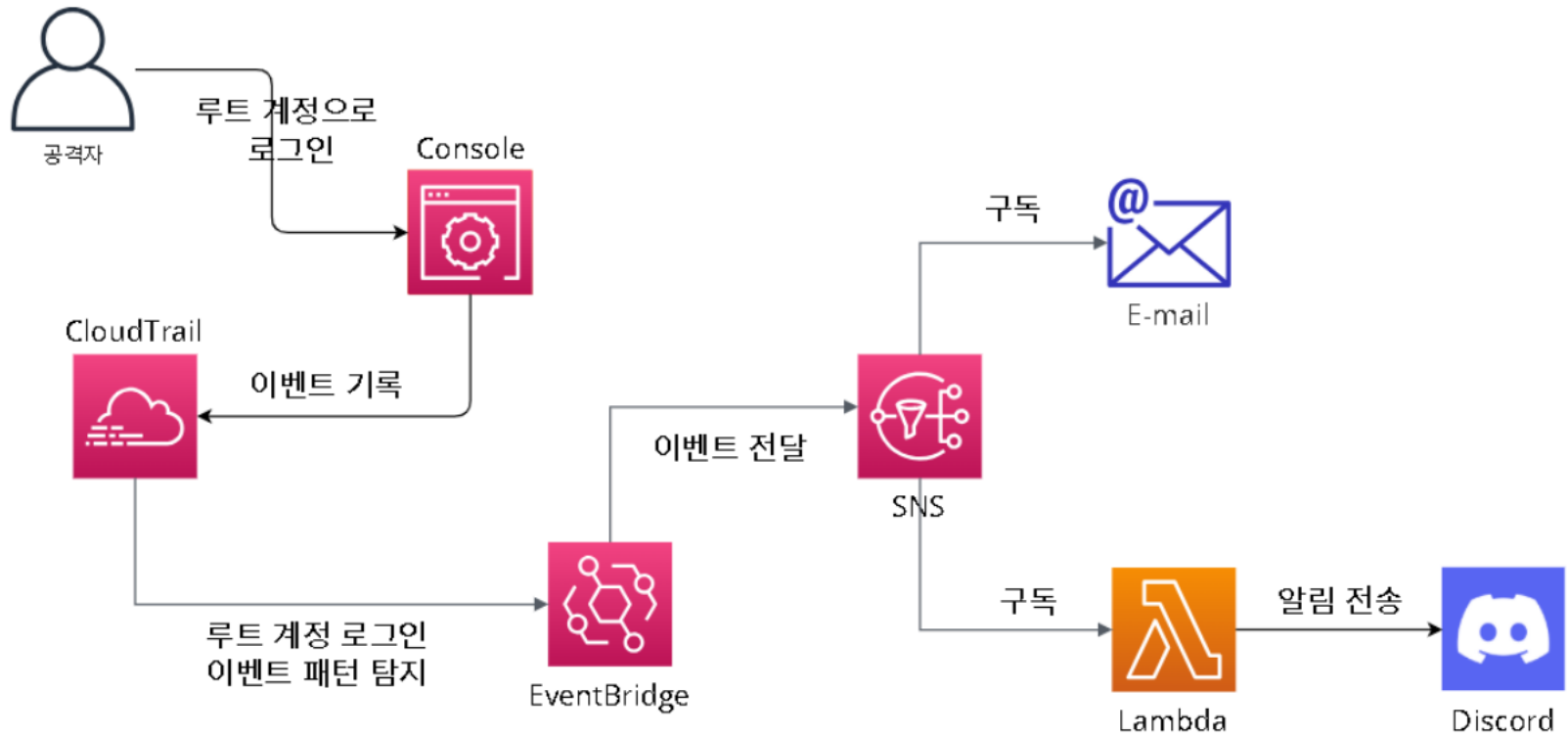


초급 시나리오

루트 계정 로그인 알림

학습목표

운영 환경에서 사용이 최소화되어야 하는
AWS 루트 계정의 콘솔 로그인을
실시간으로 탐지하고, 관리자에게 이메일
및 디스코드 메시지를 통한 **알림**을 전송하
여 신속한 대응을 가능하게 한다.



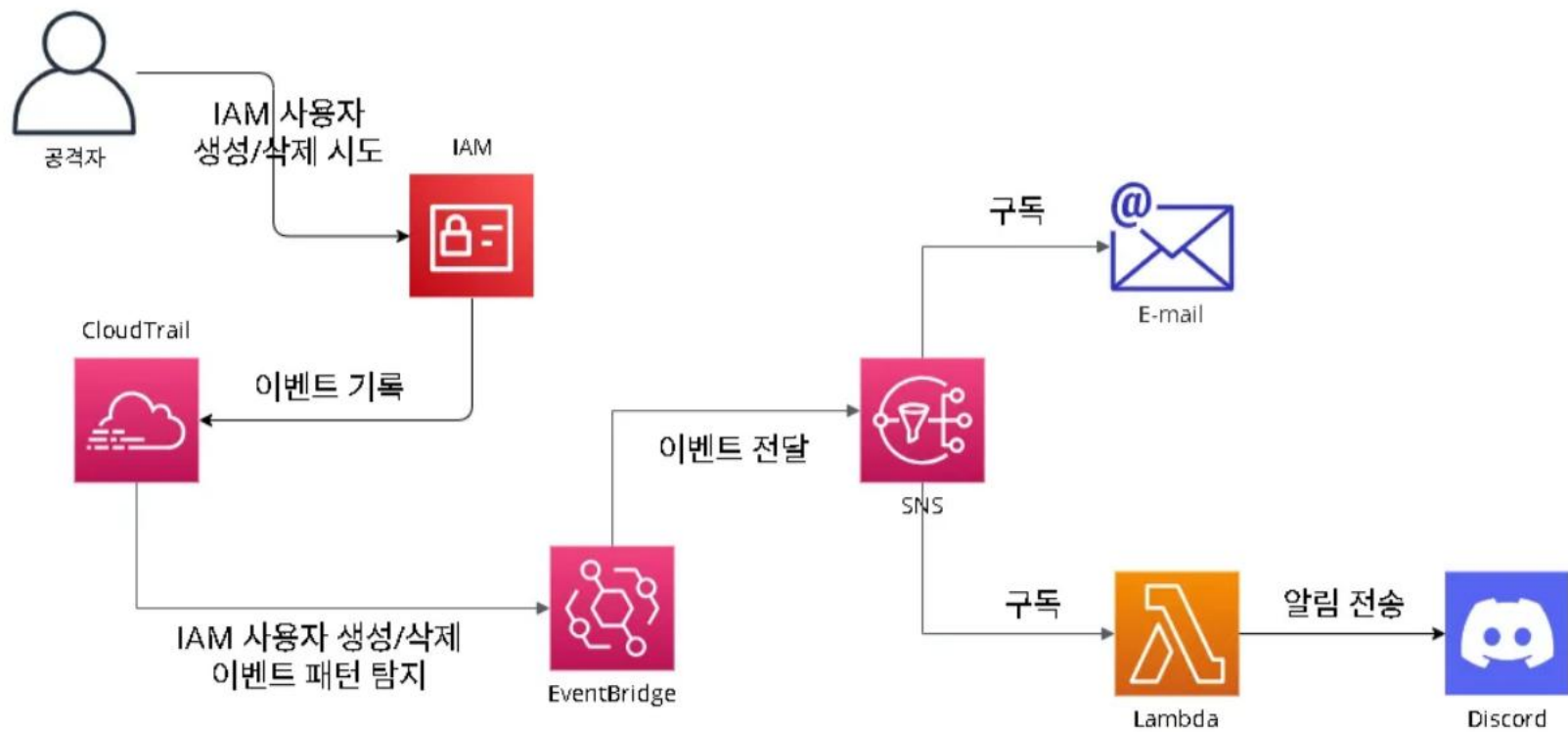
초급 시나리오

새로운 IAM User의 생성, 삭제 탐지

학습목표

IAM 사용자 생성 및 삭제 탐지는 권한 남용, 내부 위협, 외부 침해 행위와 같은 행위로 판단될 수 있다.

IAM 사용자 생성 및 삭제가 탐지되었을 경우를 관리자에게 **알림**을 전송하는 체계를 구현한다.



초급 시나리오

테라폼 구현

[콘솔 구현]

이 버킷의 퍼블릭 액세스 차단 설정

퍼블릭 액세스는 ACL(엑세스 제어 목록), 버킷 정책, 액세스 지정 정책 또는 모두를 통해 버킷 및 객체에 부여됩니다. 이 버킷 및 해당 객체는 이 버킷 및 해당 액세스 지정에만 적용됩니다. AWS에서는 모든 퍼블릭 액세스 차단을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 버킷에 대한 어느 정도 수준의 퍼블릭 액세스가 필요한 경우 특정 스토리지 사용 사례에 맞게 아래 개별 설정을 사용자 지정할 수 있습니다.

☒ 모든 퍼블릭 액세스 차단

이 설정을 활성화하면 아래 4개의 설정을 모두 활성화한 것과 같습니다. 다음 설정 각각은 서로 독립적입니다.

☒ 새 ACL(엑세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 새로 추가된 버킷 또는 객체에 적용되는 퍼블릭 액세스 권한을 차단하며, 기존 버킷 및 객체에 대한 새 퍼블릭 액세스 ACL 생성을 금지합니다. 이 설정은

☒ 임의의 ACL(엑세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 모든 ACL을 무시합니다.

☒ 새 퍼블릭 버킷 또는 액세스 지정 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 새 버킷 및 액세스 지정 정책을 차단합니다. 이 설정은 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존

☒ 임의의 퍼블릭 버킷 또는 액세스 지정 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 및 교차 계정 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 정책을 사용하는 버킷 또는 액세스 지정에 대한 퍼블릭 및 교차 계정 액세스를 무시합니다.

☐ 모든 퍼블릭 액세스 차단

이 설정을 활성화하면 아래 4개의 설정을 모두 활성화한 것과 같습니다. 다음 설정 각각은 서로 독립적입니다.

☐ 새 ACL(엑세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 새로 추가된 버킷 또는 객체에 적용되는 퍼블릭 액세스 권한을 차단하며, 기존 버킷 및 객체에 대한 새 퍼블릭 액세스 ACL 생성을 금지합니다. 이 설정은 ACL을

☐ 임의의 ACL(엑세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 모든 ACL을 무시합니다.

☐ 새 퍼블릭 버킷 또는 액세스 지정 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 새 버킷 및 액세스 지정 정책을 차단합니다. 이 설정은 S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존

☐ 임의의 퍼블릭 버킷 또는 액세스 지정 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 및 교차 계정 액세스 차단

S3은 버킷 및 객체에 대한 퍼블릭 액세스를 부여하는 정책을 사용하는 버킷 또는 액세스 지정에 대한 퍼블릭 및 교차 계정 액세스를 무시합니다.

[테라폼 구현]

```

resource "aws_s3_bucket" "my_bucket" {
  bucket = "my-bucket-for-terraform-test"
}

resource "aws_s3_bucket_public_access_block" "my_bucket_block" {
  bucket = aws_s3_bucket.my_bucket.id
  block_public_acls = false
  ignore_public_acls = false
  block_public_policy = false
  restrict_public_buckets = false
}

```

Terraform will perform the following actions:

```

# aws_s3_bucket_public_access_block.my_bucket_block will be updated in-place
~ resource "aws_s3_bucket_public_access_block" "my_bucket_block" {
  ~ block_public_acls = true -> false
  ~ block_public_policy = true -> false
    id = "my-bucket-for-terraform-test"
  ~ ignore_public_acls = true -> false
  ~ restrict_public_buckets = true -> false
    # (1 unchanged attribute hidden)
}

```

22

워크북 작성

Scenario Workbook

+ 속성 추가

댓글

댓글 추가

Scenario

▼ 초급 시나리오 / 기초적인 보안 모니터링

- 1 S3 퍼블릭 버킷 생성 탐지 및 알람
- 2 루트 계정 로그인 알람
- 3 AWS Cloudtrail 비활성화 탐지
- 4 Security group의 정책 변경 탐지
- 5 새로운 IAM User의 생성, 삭제 탐지
- 6 로그 그룹 삭제 또는 변경 탐지
- 7 스냅샷 / 자원 공유를 통한 은폐 및 유출 시도 시나리오
- 8 계정에 생성된 AMI 를 외부에 공개로 등록하거나 외부 계정에 공유하는 시도 탐지

초급 시나리오 피드백

▶ 1. S3 퍼블릭 버킷 생성 탐지 및 알람

▼ 7.스냅샷/자원 공유를 통한 은폐 및 유출 시도 시나리오

피드백 요청

7번 시나리오 피드백	장희영	2025년 6월 22일	김기원	2025년 6월 23일
시나리오 피드백	강유림	2025년 6월 22일	김진서	2025년 6월 23일
7번 시나리오 피드백	박도은	2025년 6월 22일	손형은	2025년 6월 23일
7번 시나리오 피드백	권도원	2025년 6월 22일	조민혁	2025년 6월 23일

피드백)

- eventbridge로는 알림만 받고 자동 대응은 하지 않으므로 “자동 대응” 문구 삭제 필요
- ‘누가 중지했는지’라는 부분이 어색하게 느껴짐. (최종적으로는 디스코드로 ‘누가 언제 어떤 이벤트를 발생시켰는지’를 모두 탐지하고 있으므로)
- EventBrige를 사용하는 목적성이 명확히 드러나지 않음.

04

향후 계획

향후 계획



STEP 1
워크북 양식 통일

STEP 2
중급/고급 시나리오 진행
AWS 자격증 시험 준비

STEP 3
프로젝트 마무리 및 최종 발표 준비

STEP 1 워크북 양식 통일

시나리오 워크북 공통 양식

구성 팀원

ex> 홍길동

워크북 작성 기간

2025.MM.DD - 2025.MM.DD

[목차]

[@번 시나리오 안내]

[시나리오 전체적인 흐름]

[실습 진행 전, 주의 사항] (선택 사항)

[@번 시나리오 상세 구현 과정]

1. SNS 주제 생성 - Email 알림용
2. EventBridge 규칙 만들기 - 조건 감지 및 SNS/Lambda 호출
3. Lambda 함수 생성 - Discord 알림용
4. CloudTrail 추적 생성
5. 테스트 - 스냅샷 공유 시도 후 알림 도착 확인
6. Terraform 구현 코드

STEP 2 중급/고급 시나리오 진행



진행 완료



진행중



진행 예정

중급 시나리오 / AWS 서비스를 활용한 서비스 및 보안 모니터링



EC2 내 bash history 조작 시도 탐지



Athena 기반 CloudTrail 비정상 API 사용 분석



Guardduty를 Threat IP List를 활용한 모니터링 정책 구현



AWS WAF를 정책 관리 시나리오 및 모니터링 정책 구현



Security group의 정책 변경 탐지

고급 시나리오




상용 SIEM을 활용한 이벤트 수집 및 분석



Guardduty 탐지 기반 자동화 대응

STEP 2 AWS 자격증 시험 준비

강의 수강



[NEW] Ultimate AWS Certified Cloud Practitioner CLF-C02 2025
 Full Practice Exam included + explanations | Learn Cloud Computing | Pass the AWS Cloud Practitioner...
 Stephane Maarek | AWS Certified Cloud Practitioner, Solutions...

베스트셀러 ★ 4.7 평점 253,803개 총 15시간 285개의 강의

초급자

기출 문제 풀이

Amazon AWS Certified Cloud Practitioner CLF-C02 Exam



719

719 Questions and Answers for the
 AWS Certified Cloud Practitioner CLF-
 C02 Exam



1056

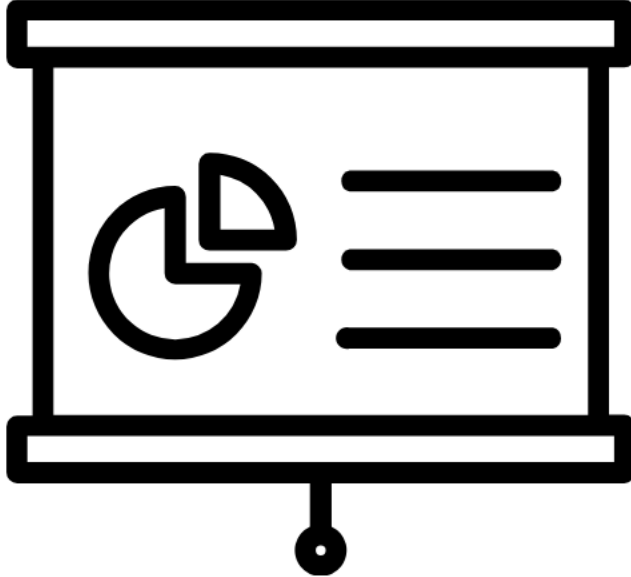
Students Passed the "AWS Certified
 Cloud Practitioner CLF-C02" exam



95.1%

Average score during Real Exams at
 the Testing Centre

STEP 3 프로젝트 마무리 및 최종 발표 준비





Thank you