사용자 행위 기반 구글 워크스페이스 분석 및 이상 탐지 솔루션 개발

이경재 | 김근수 | 김정욱 | 송지현

목차

1 프로젝트 소개

1. 팀 소개
2. 주제 및 선정 이유

1. 팀 소개

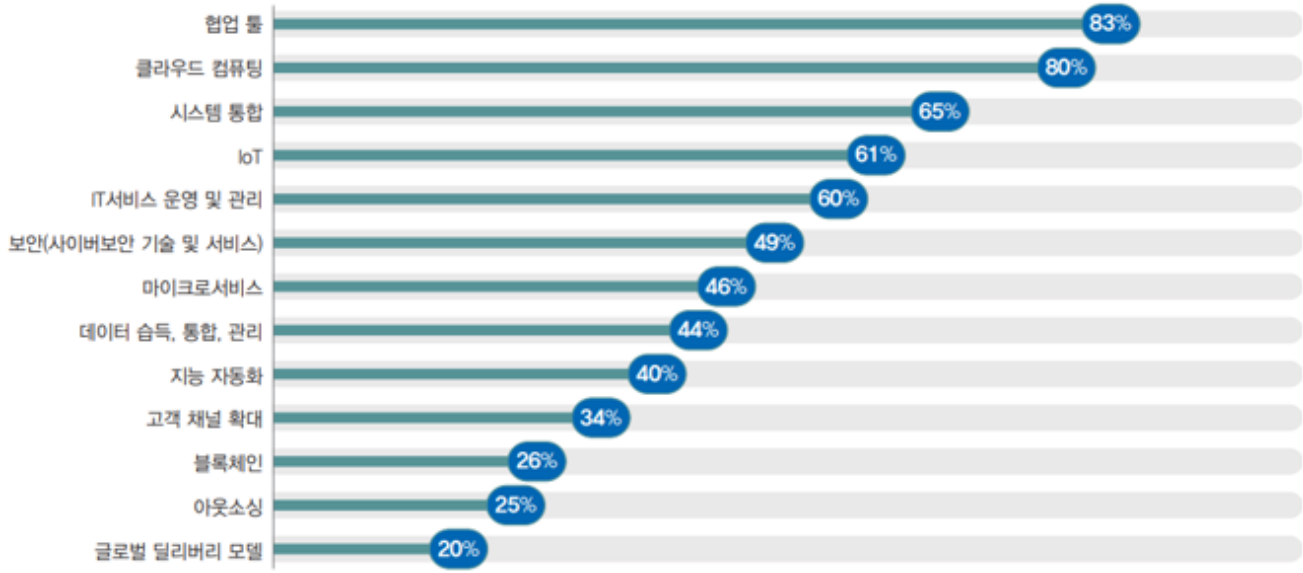
2. 주제 및 선정 이유

“사용자 행위 기반 구글 워크스페이스 분석 및 이상 탐지 솔루션 개발”

코로나 발생 이후 3년간 월별 재택근무 비율

코로나19로 인한 재택 근무 증가

코로나19 이후 투자가 확대된 디지털 인프라 기술



계속되는 클라우드 협업 툴 사용량 증가

자료1 출처 : 시프티, 자료2 출처 : KPMG, 2021

2. 주제 및 선정 이유

01. Sass 환경의 보안 강화 필요성

1. 해당 환경에서 어떤 식으로 보안을 강화 시켜야 하는가?
2. 협업 툴 이므로 로그량 과부하 상황에서 어떻게 효율적으로 이상탐지를 할 것인가?

---

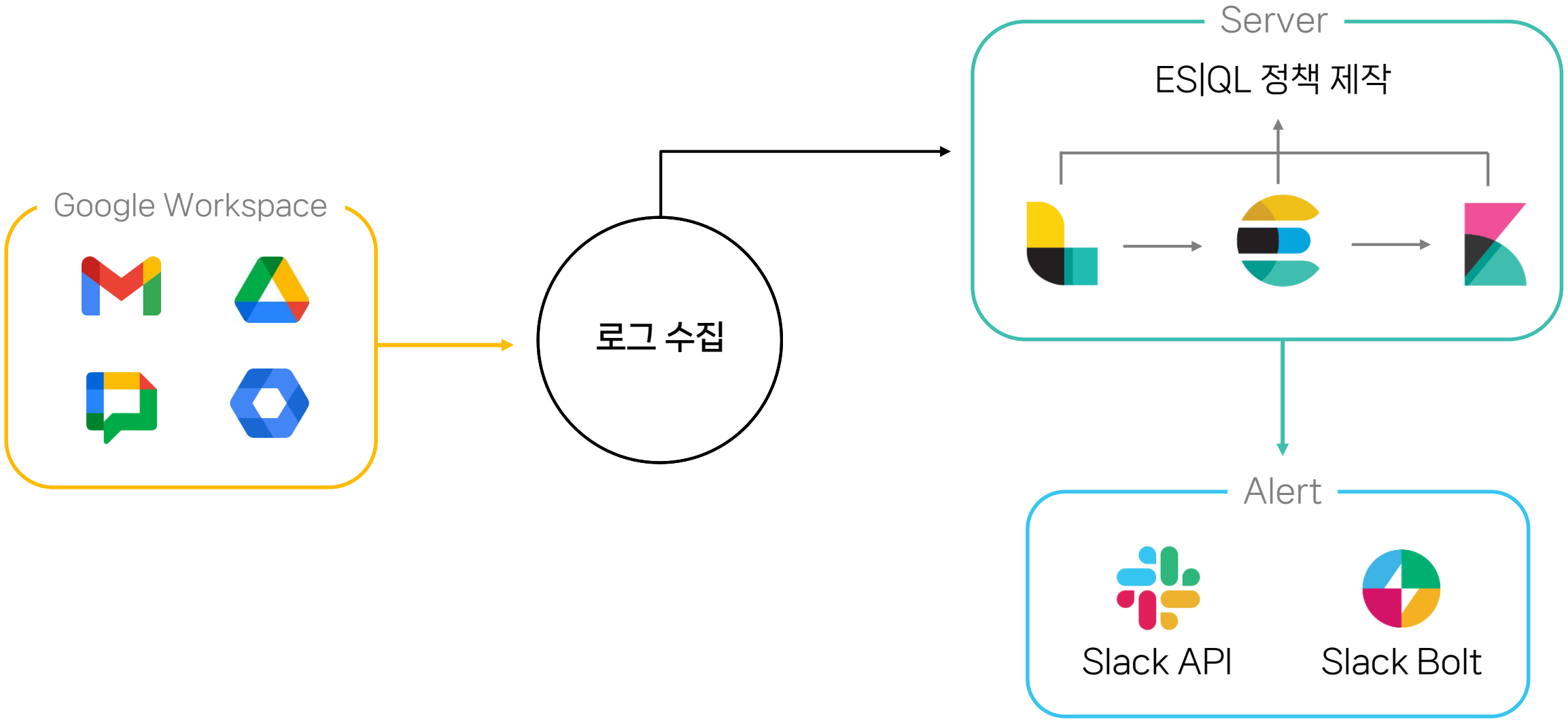
02. 정책을 통한 보안 운영 체계 제안

1. Audit 로그를 통해 행위 식별 및 로그 분석 가능
2. 로그 간 차이점을 통해 정책 제작
3. 사용자의 이상 행위 탐지하는 하나의 보안 인프라 구성 가능

2 프로젝트 구성

1. 구상도
2. 주요 타겟 & 수집 과정
3. 시각화 및 정책 수립
4. Alert

1. 구상도


Server
ES|QL 정책 제작
Google Workspace
로그 수집
Alert
Slack API
Slack Bolt

2. 주요 타겟 & 수집 과정

Google Workspace

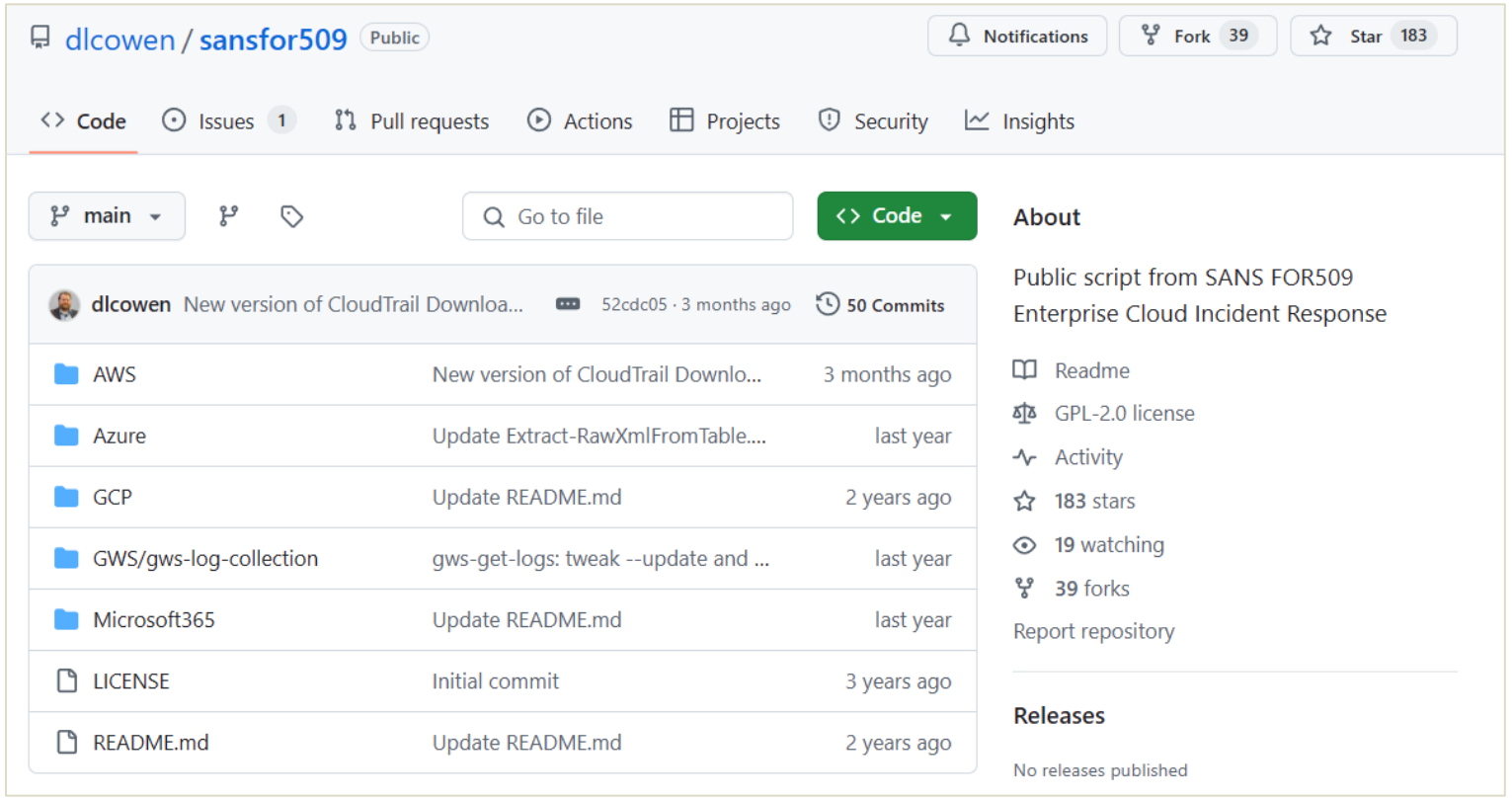
Gmail, Meet, Chat, Drive 등을 포함하는 구글 서비스

장소, 시간, 기기에 상관없이 협업을 도모하고, 업무 능률을 향상 시킬 수 있는 도구

2. 주요 타겟 & 수집 과정

Google Workspace

2. 주요 타겟 & 수집 과정



1. Github를 참고하여
   로그 수집 코드 Remake

2. 각 앱 별 로그 수집

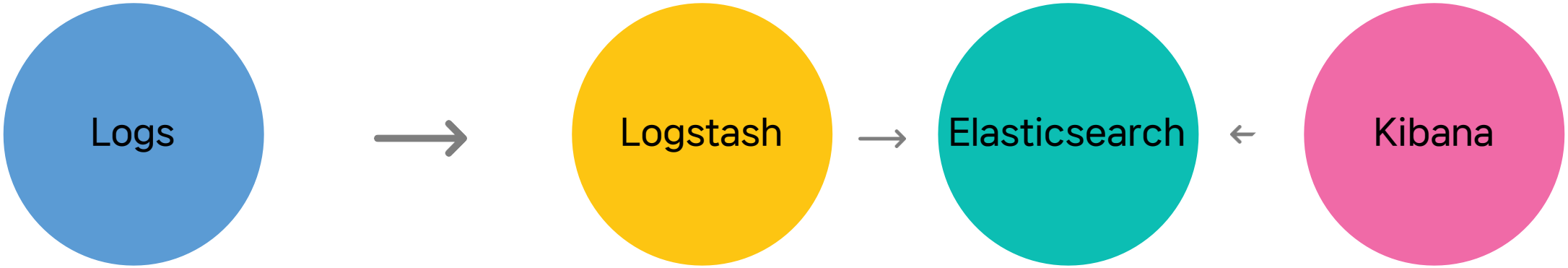
3. Daemon화를 통해 자동화

출처 : https://github.com/dlcowen/sansfor509

2. 주요 타겟 & 수집 과정

출처 : https://github.com/dlcowen/sansfor509

3. 시각화 및 정책 수립


Logs
Logstash
Elasticsearch
Kibana
행위 로그 수집
수집 로그 정제
로그 인덱싱
및 적재
시각화

3. 시각화 및 정책 수립

File-Related Anomalies_(파일 관련 이상 징후)

- GDrive_External_Sharing (드라이브 문서 외부 공유 탐지)
- GDrive_Permanent_Delete (드라이브 내 파일 영구 삭제 탐지)
- GDrive_High_Vol_Upload (드라이브 내 대량 업로드 탐지)
- GDrive_High_Vol_Download (드라이브 내 대량 다운로드 탐지)
- Alert_Ext_File_Type_Detection (금지 파일 확장자 탐지)

Abnormal Usage_(비정상적 사용)

- GDrive_External_Sharing_Confidential(gmail)
- GDrive_External_Sharing_Confidential(drive)
  (알림센터 : 내부용, 기밀, 중요 라는 단어를 2개이상 포함한 파일 외부 공유 탐지)
- GDrive_Mobile_Action (모바일 환경에서 구글 드라이브 행위 탐지)
- GChat_High_Vol_Upload (채팅 스페이스 내 대량 파일 업로드 탐지)

Unauthorized Access / External Communication_(비인가 접근 / 외부 커뮤니케이션)

- GChat_Ext_Domain_Space (외부 도메인 채팅 스페이스 시작 탐지)
- GChat_Ext_User_Chat (외부 사용자와 채팅 탐지)
- GChat_Ext_File_Upload (외부 사용자와 채팅 시 파일 업로드 감지)
- Alert_Sensitive_Info_Sharing(drive) (알림센터 : 금융정보(카드번호, , 주민번호, 관련 단어) 포함된 문서 공유)
- Alert_Sensitive_Info_Sharing(chat) (민감 정보 문서 공유 탐지)

✓ 총 16개 정책 제작

Unauthorized Access / User Management_(비인가 접근 / 사용자 관리)

- GChat_User_Block (내부 사용자 차단 탐지)

Access Time Violations_(접근 시간 위반)

- Common_Off_Hours (정해진 시간 외 활동 탐지)

3. 시각화 및 정책 수립


```
{
  "type": "acl_change",
  "name": "change_user_access",
  "parameters": [
    { "name": "primary_event", "boolValue": true },
    { "name": "billable", "boolValue": true },
    { "name": "visibility_change", "value": "external" },
    { "name": "target_user", "value": "jiniluce7@naver.com" },
    { "name": "old_value", "multiValue": ["none"] },
    { "name": "new_value", "multiValue": ["can_edit"] },
    { "name": "old_visibility", "value": "private" },
    { "name": "owner_is_shared_drive", "boolValue": false },
    { "name": "owner", "value": "revenants@redhat12.xyz" },
    { "name": "doc_id", "value": "12ks7dxsVcf3bithh7eJZgb9-h5JO9uci" },
    { "name": "doc_type", "value": "msword" },
    { "name": "is_encrypted", "boolValue": false },
    { "name": "doc_title", "value": "2024 악성코드 분석 레포트_92212879 송w지현 - 복사본_어셈티비.docx" },
    { "name": "visibility", "value": "shared_externally" },
    { "name": "originating_app_id", "value": "211604355607" },
    { "name": "actor_is_collaborator_account", "boolValue": false },
    { "name": "owner_is_team_drive", "boolValue": false }
```


1. 편집 이벤트

가시성 : shared_externally
(외부와 공유됨)

2. 사용자 접근 권한 변경 이벤트

기존 접근 권한: 없음

새로운 접근 권한: can_edit (편집 가능)

기존 가시성: private

기타 정보: jiniluce7@naver.com
계정이 편집할 수 있는 권한이 부여

"2024 악성코드 분석 레포트_92212879 송지현 - 복사본_어셈티비.docx" 문서 편집

해당 문서를 외부 사용자(jiniluce7@naver.com)와 공유, 편집 권한 부여

3. 시각화 및 정책 수립

File-Related Anomalies_(파일 관련 이상 징후)

- GDrive_External_Sharing (드라이브 문서 외부 공유 탐지)
- GDrive_Permanent_Delete (드라이브 내 파일 영구 삭제 탐지)
- GDrive_High_Vol_Upload (드라이브 내 대량 업로드 탐지)
- GDrive_High_Vol_Download (드라이브 내 대량 다운로드 탐지)
- Alert_Ext_File_Type_Detection (금지 파일 확장자 탐지)

ES|QL 쿼리

```
SQL
FROM drive_logs*
| MV_EXPAND events.name
| WHERE events.name == "change_user_access"
| WHERE event.original LIKE "*can_edit*"
| EVAL original_parameters.name = events.parameters.name
| EVAL original_parameters.value = events.parameters.value
| EVAL original_parameters.name2 = original_parameters.name
| MV_EXPAND original_parameters.name
| MV_EXPAND original_parameters.value
| MV_EXPAND events.parameters.name
| MV_EXPAND events.parameters.value
| WHERE original_parameters.name == "target_user" AND original_parameters.value LIKE "*@*" AND NOT orig
| WHERE events.parameters.name == "doc_title"
  AND (
    events.parameters.value LIKE "*.hwp" OR
    events.parameters.value LIKE "*.pdf" OR
    events.parameters.value LIKE "*.docx" OR
    events.parameters.value LIKE "*.xlsx" OR
    events.parameters.value LIKE "*.png" OR
    events.parameters.value LIKE "*.jpg" OR
    events.parameters.value LIKE "*.avi"
  )
| STATS event_count = COUNT(), last_event_time = MAX(id.time), event.original = VALUES(event.original),
| SORT last_event_time DESC
```

3. 시각화 및 정책 수립

File-Related Anomalies_(파일 관련 이상 징후)

- GDrive_External_Sharing (드라이브 문서 외부 공유 탐지)
- GDrive_Permanent_Delete (드라이브 내 파일 영구 삭제 탐지)
- GDrive_High_Vol_Upload (드라이브 내 대량 업로드 탐지)
- GDrive_High_Vol_Download (드라이브 내 대량 다운로드 탐지)
- Alert_Ext_File_Type_Detection (금지 파일 확장자 탐지)

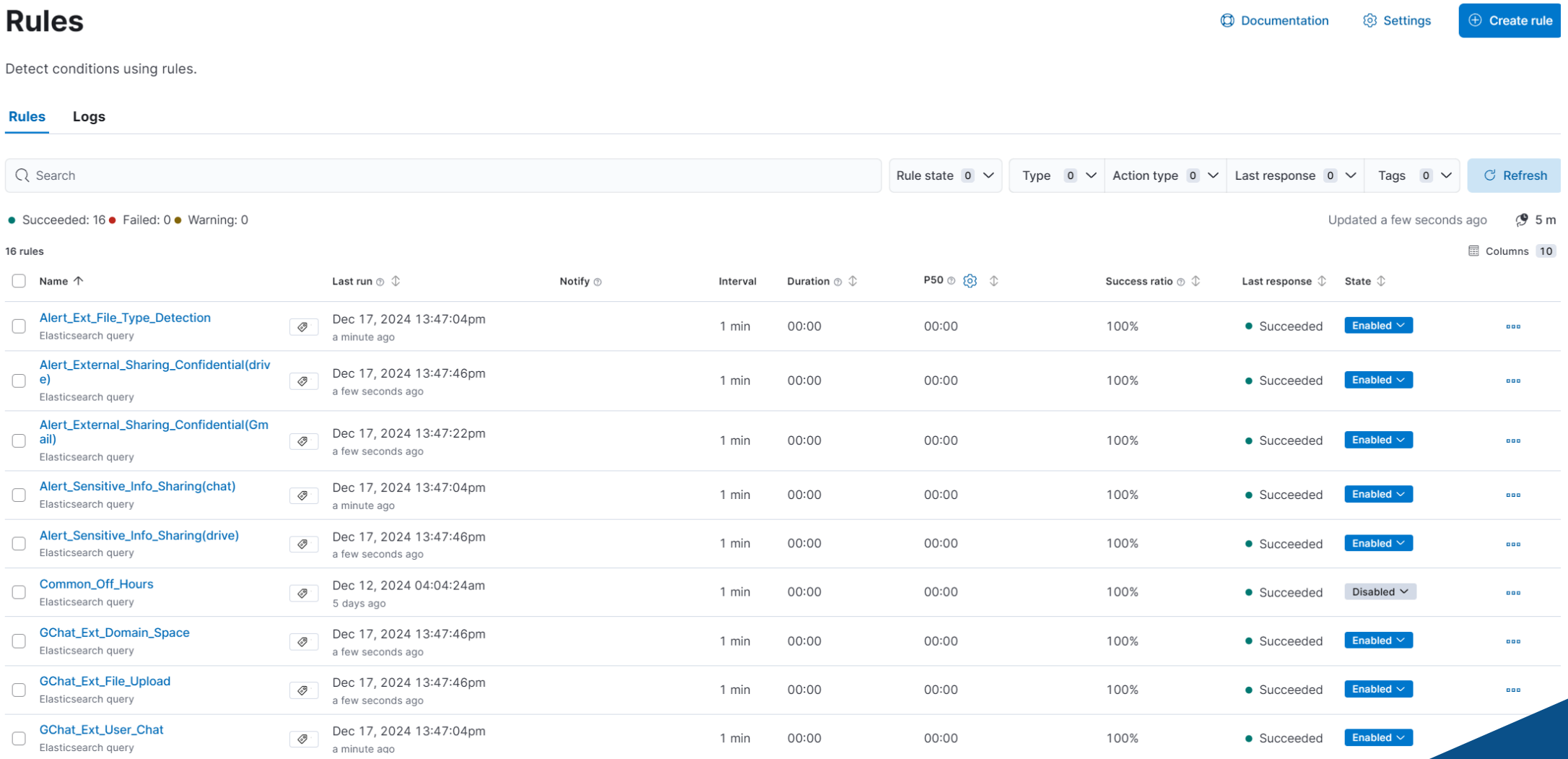
Action 쿼리

SQL

```
{
  "alert": {
    "id": "{{alert.id}}"
  },
  "context": {
    "message": "{{context.message}}"
  },
  "rule": {
    "name": "{{rule.name}}",
    "id": "{{rule.id}}"
  },
  "params": {
    "source": {
      "time": "{{date}}",
      "action": "change_user_access",
      "actor": "revenants@redhat12.xyz",
      "target_user": "{{#context.hits}}{{#_source.original_parameters}}{{#value}}{{.}},{{/value}}{{/_s
      "attachment_name": "{{#context.hits}}{{#_source}}{{#name}}{{.}},{{/name}}{{/_source}}{{/context.
    },
    "original": [
      {
        "index": "[{{#context.hits}}{{_source.event.original}}{{^@last}}, {{/@last}}{{/context.hits}}]
      }
    ]
  }
}
```

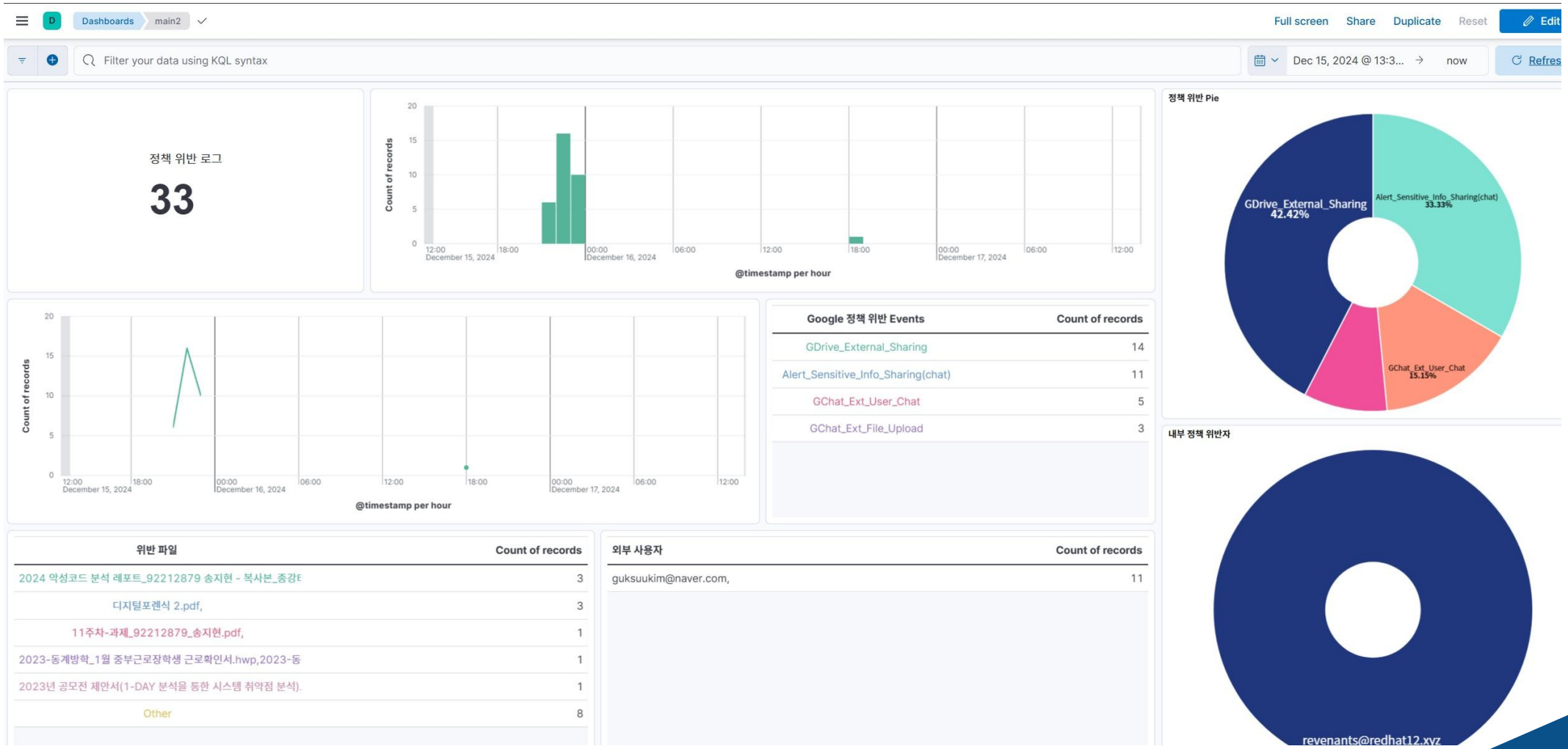
3. 시각화 및 정책 수립

Rules 화면



3. 시각화 및 정책 수립

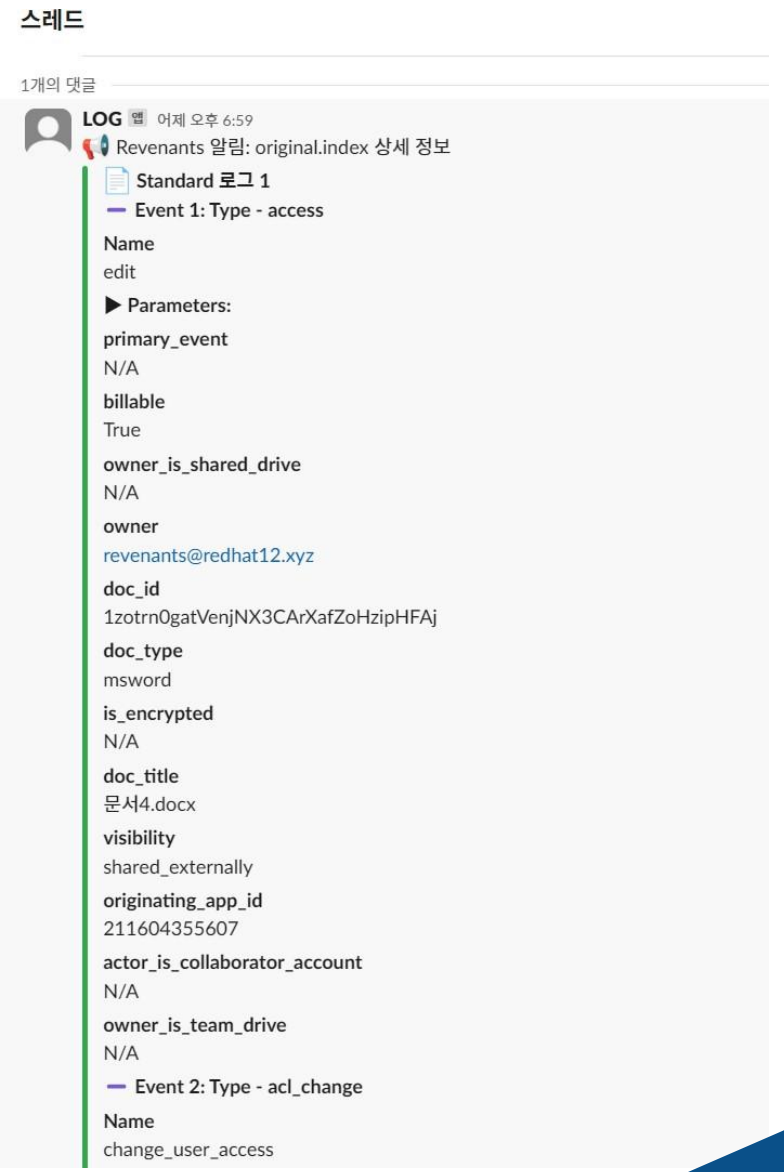
Dashboards 화면



4. Alert

Slack alert 구현

- Slack API + Slack Bolt

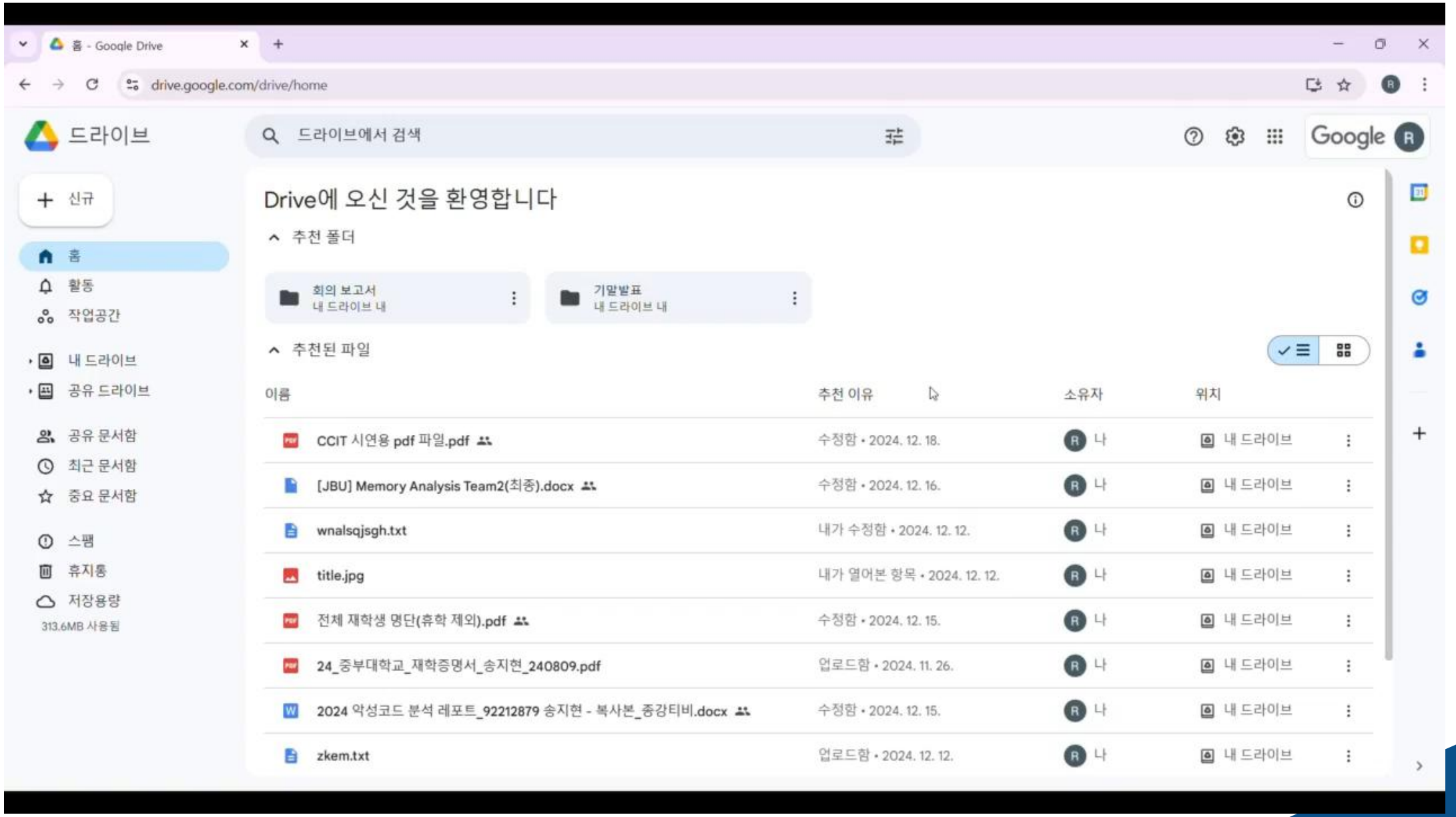


3 프로젝트 결과

1. 산출물 및 결과

2. 향후 계획

1. 산출물 및 결과


홈 - Google Drive
drive.google.com/drive/home
드라이브
드라이브에서 검색
Google
신규
홈
활동
작업공간
내 드라이브
공유 드라이브
공유 문서함
최근 문서함
중요 문서함
스팸
휴지통
저장용량
313.6MB 사용됨
Drive에 오신 것을 환영합니다
추천 폴더
회의 보고서
내 드라이브 내
기말발표
내 드라이브 내
추천된 파일
이름
추천 이유
소유자
위치
CCIT 시연용 pdf 파일.pdf
수정함 • 2024. 12. 18.
나
내 드라이브
[JBU] Memory Analysis Team2(최종).docx
수정함 • 2024. 12. 16.
나
내 드라이브
wnalsqjsgh.txt
내가 수정함 • 2024. 12. 12.
나
내 드라이브
title.jpg
내가 열어본 항목 • 2024. 12. 12.
나
내 드라이브
전체 재학생 명단(휴학 제외).pdf
수정함 • 2024. 12. 15.
나
내 드라이브
24_중부대학교_재학증명서_송지현_240809.pdf
업로드함 • 2024. 11. 26.
나
내 드라이브
2024 악성코드 분석 레포트_92212879 송지현 - 복사본_종강티비.docx
수정함 • 2024. 12. 15.
나
내 드라이브
zkem.txt
업로드함 • 2024. 12. 12.
나
내 드라이브

1. 산출물 및 결과

논문 수상

1. 산출물 및 결과

사용자 행위 기반 GWS 이상 탐지 환경 개발

01.

로그 기반 사용자 행위 분석 환경 구축

Google Workspace의 Audit 로그를 수집하여 사용자 행위를 분석하고, 이상 탐지를 통해 비정상적인 활동을 효과적으로 식별

02.

효율적인 정책 관리와 확장성

수립된 보안 정책을 기반으로 정교한 규칙을 운영하며, 이를 정형화된 형태로 관리해 유연한 확장과 유지보수를 제안

03.

실시간 대응 및 시각화

탐지된 이상 행위를 대시보드로 시각화하고 Slack과 같은 협업 도구를 통해 즉각적인 알림 체계를 제공해 보안 운영의 효율성

2. 향후 계획

향후 계획

01.

Alert 기능 뿐 아니라 대응 기능 추가 연구

alert에서 끝나는 것이 아니라 각 정책에 따른 플레이 북과 대응 방안에 대해 추가 연구

02.

GWS 경험을 토대로 여러 협업 환경에서의 SIEM 환경 구축

GWS 뿐만 아니라 여러 협업 환경들을 경험해보고 종합적으로 관리하고 SIEM기능을 추가한 환경을 구축

감사합니다.

이경재 | 김근수 | 김정욱 | 송지현