SG 검토 대시보드 개발 및 활용기

공지훈(26.2.25.)

소개

- 현) 라포랩스
- 전) KISA, 금융보안원, 카카오뱅크
- ISMS-P 인증심사원 / Kubestronaut
- KITRI 화이트햇스쿨 멘토
- AWSKRUG 보안소모임 오거나이저

RAPPORT LABS

패션 버티컬 커머스

4050 여성 3명 중 1명 사용

누적 다운로드 720만 이상

산지직송 식품 커머스

누적 다운로드 300만 이상

4050이 신뢰하는 전국팔도 제철 먹거리 판매

목차

1. 들어가며

AI for Security를 기대하셨다면...

반복적인 업무를 어떻게 자동화 하는지

어떤 업무를 자동화하는지

(다른 사람들은 어떤 아이디어가 있는지)

2. 문제의식

2. 문제의식

(ISMS-P) 2.10.1 보안시스템 운영
(ISO 27001) 5.36 Compliance with policies, rules and standards for information security

항 목	2.10.1 보안시스템 운영
인증기준	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
주요 확인사항	• 조직에서 운영하고 있는 보안시스템에 대한 운영절차를 수립·이행하고 있는가? • 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가? • 보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하고 있는가? • 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가? • 보안시스템에 설정된 정책의 타당성 여부를 주기적으로 검토하고 있는가? • 개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출 방지를 위하여 관련 법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하고 있는가?

2. 문제의식

- SG가 어떤 리소스에 attach되어 있는지, 미사용하고 있는지 한눈에 파악 어려움
- 출발지/목적지를 IP가 아닌 SG를 참조하는 경우 정책 흐름 파악이 복잡함
- 출발지 IP 혹은 서비스 범위가 과도하게 넓은 룰을 일괄적으로 조회하기 어려움
- 순환 참조나 정책 충돌이 발생했는지 확인하기 불편함
- AWS 계정이 수십 개라면?

너무너무 어려운 SG 검토.. 쉽고 편하지만 정확하게 하고싶다!

3. 도구 개발 및 활용

Steampipe와 Powerpipe를 활용하자!

3. 도구 개발 및 활용

✅ 공통점

1. 오픈소스 도구

- 둘 다 Turbot에서 개발한 **오픈소스 도구**입니다. GitHub +1

2. 클라우드 인프라 및 서비스 분석

- 공통적으로 **클라우드 리소스나 API 데이터를 처리**하는 데 사용되며, DevOps·SecOps·CloudOps 등의 팀에서 활용됩니다. Steampipe ...

3. SQL 기반 데이터 처리

- Steampipe가 API 데이터를 SQL로 쿼리하도록 만들면, Powerpipe는 그러한 데이터를 **시각화 및 분석**하는 데 활용됩니다. Steampipe | sele...

4. 상호 연동

- Powerpipe는 기본적으로 Steampipe의 데이터(예: Steampipe가 변환한 테이블)를 시각화하는 데 *잘 연동*되도록 설계되어 있습니다. Steampipe | sele...

3. 도구 개발 및 활용

❗ 차이점

항목	Steampipe	Powerpipe
핵심 역할	API → SQL 쿼리 도구 클라우드/서비스 데이터를 **SQL로 쿼리**	Steampipe/DB로부터 받은 데이터를 **대시보드/벤치마크/시각화**
주요 기능	• API를 table로 매핑 • 실시간 데이터 질의 • SQL로 클라우드 리소스 분석	• 대시보드 시각화 • 보안·컴플라이언스 벤치마크 실행 • 보고서 생성
사용 언어 / 방식	SQL 쿼리 중심	*HCL 기반* 대시보드 및 벤치마크 정의
데이터 저장소 의존성	자체 Steampipe DB 또는 다이렉트 API	PostgreSQL, SQLite, DuckDB 등 다양한 DB에서 시각화 가능 Powerpipe ...
초점	데이터 *추출/질의*	데이터 *분석/시각화/벤치마킹*

~~Steampipe와 Powerpipe를 활용하자!~~
대시보드 표현에 제약

Steampipe로 데이터를 수집해서 뷰를 직접 그리자!

3. 도구 개발 및 활용

```
1. extract_and_visualize_v2.py 실행
      ↓
2. Steampipe 쿼리 호출
      ├─ EC2 인스턴스 정보
      ├─ Security Group 정보
      ├─ SG Rules (Ingress/Egress)
      └─ VPC 정보
      ↓
3. 데이터 수집 및 가공
      ├─ 노드 데이터 생성 (EC2, SG)
      ├─ 엣지 데이터 생성 (연결 관계)
      └─ VPC 정보 매핑
      ↓
4. 대시보드 HTML 템플릿에 데이터 업데이트
      └─ sg_interactive_graph_v2.html
      ↓
5. 브라우저에서 시각화
      └─ vis.js 라이브러리로 인터랙티브 그래프 렌더링
```

3. 도구 개발 및 활용

```
1. extract_and_visualize_v2.py 실행
        ↓
2. Steampipe 쿼리 호출
        ├─ EC2 인스턴스 정보
        ├─ Security Group 정보
        ├─ SG Rules (Ingress/Egress)
        └─ VPC 정보
        ↓
3. 데이터 수집 및 가공
        ├─ 노드 데이터 생성 (EC2, SG)
        ├─ 엣지 데이터 생성 (연결 관계)
        └─ VPC 정보 매핑
        ↓
4. 대시보드 HTML 템플릿에 데이터 업데이트
        └─ sg_interactive_graph_v2.html
        ↓
5. 브라우저에서 시각화
        └─ vis.js 라이브러리로 인터랙티브 그래프 렌더링
```

- Steampipe 설정 구성
- 멀티 어카운트 인증 정보 확인

3. 도구 개발 및 활용

```
1. extract_and_visualize_v2.py 실행
        ↓
2. Steampipe 쿼리 호출
        ├─ EC2 인스턴스 정보
        ├─ Security Group 정보
        ├─ SG Rules (Ingress/Egress)
        └─ VPC 정보
        ↓
3. 데이터 수집 및 가공
        ├─ 노드 데이터 생성 (EC2, SG)
        ├─ 엣지 데이터 생성 (연결 관계)
        └─ VPC 정보 매핑
        ↓
4. 대시보드 HTML 템플릿에 데이터 업데이트
        └─ sg_interactive_graph_v2.html
        ↓
5. 브라우저에서 시각화
        └─ vis.js 라이브러리로 인터랙티브 그래프 렌더링
```

- Steampipe를 통해 검토에 필요한 정보 수집
- 사전에 정의한 SQL 쿼리 실행
- steampipe aggregator로 수집 속도 병목 해결

3. 도구 개발 및 활용

```
1. extract_and_visualize_v2.py 실행
      ↓
2. Steampipe 쿼리 호출
      ├─ EC2 인스턴스 정보
      ├─ Security Group 정보
      ├─ SG Rules (Ingress/Egress)
      └─ VPC 정보
      ↓
3. 데이터 수집 및 가공
      ├─ 노드 데이터 생성 (EC2, SG)
      ├─ 엣지 데이터 생성 (연결 관계)
      └─ VPC 정보 매핑
      ↓
4. 대시보드 HTML 템플릿에 데이터 업데이트
      └─ sg_interactive_graph_v2.html
      ↓
5. 브라우저에서 시각화
      └─ vis.js 라이브러리로 인터랙티브 그래프 렌더링
```

- 수집한 정보를 노드로 변환
- 노드간 관계 구성

3. 도구 개발 및 활용

```
1. extract_and_visualize_v2.py 실행
        ↓
2. Steampipe 쿼리 호출
        ├─ EC2 인스턴스 정보
        ├─ Security Group 정보
        ├─ SG Rules (Ingress/Egress)
        └─ VPC 정보
        ↓
3. 데이터 수집 및 가공
        ├─ 노드 데이터 생성 (EC2, SG)
        ├─ 엣지 데이터 생성 (연결 관계)
        └─ VPC 정보 매핑
        ↓
4. 대시보드 HTML 템플릿에 데이터 업데이트
        └─ sg_interactive_graph_v2.html
        ↓
5. 브라우저에서 시각화
        └─ vis.js 라이브러리로 인터랙티브 그래프 렌더링
```

- 대시보드 템플릿 html에 생성된 데이터 업데이트

Demo

3. 도구 개발 및 활용

- SG가 어떤 리소스에 attach되어 있는지, 미사용하고 있는지 한눈에 파악 어려움
- 출발지/목적지를 IP가 아닌 SG를 참조하는 경우 정책 흐름 파악이 복잡함
- 출발지 IP 혹은 서비스 범위가 과도하게 넓은 룰을 일괄적으로 조회하기 어려움
- 순환 참조나 정책 충돌이 발생했는지 확인하기 불편함
- AWS 계정이 수십 개라면?

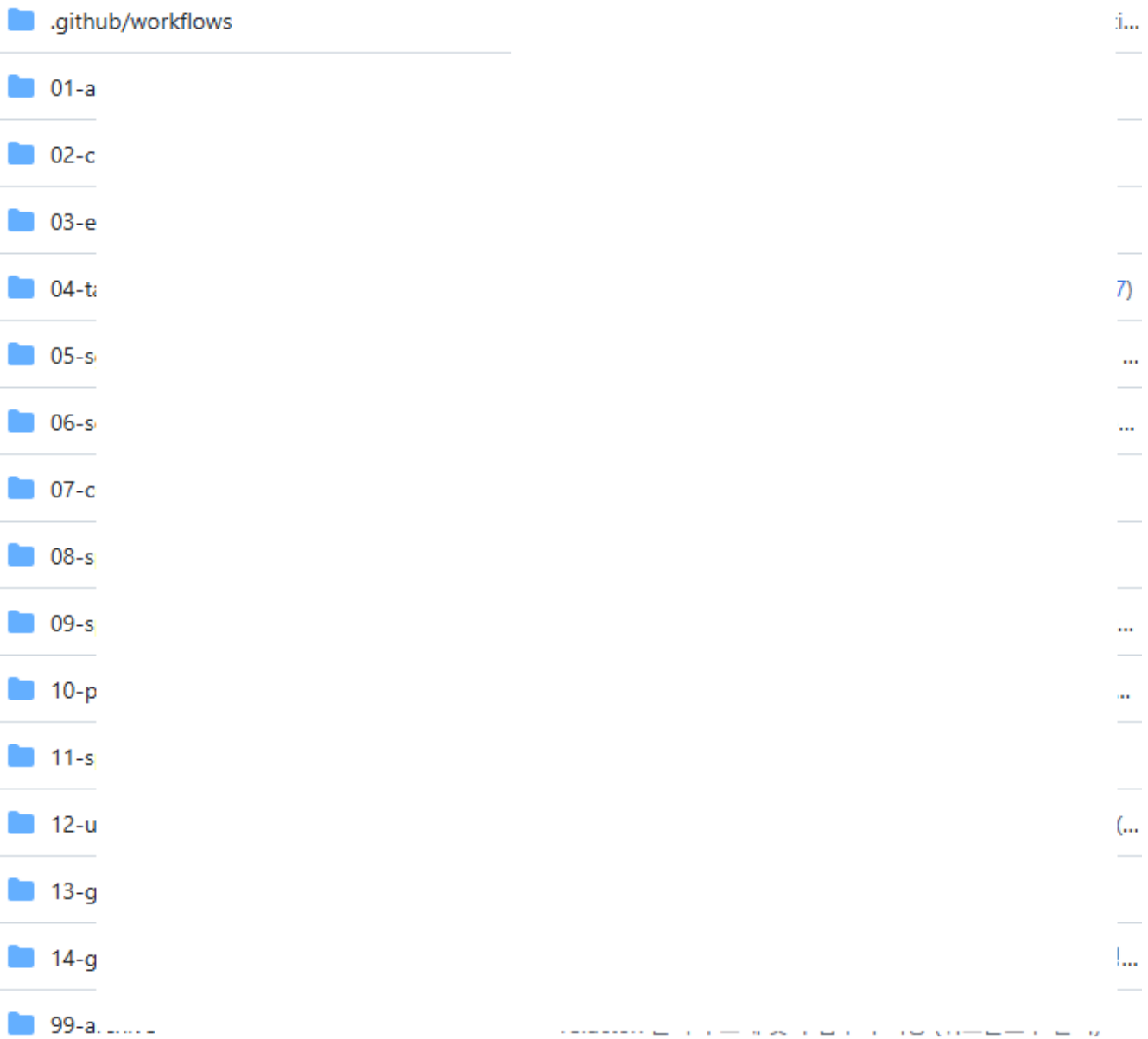
- SG가 어떤 리소스에 attach되어 있는지, 미사용하고 있는지 한눈에 파악 어려움
- 출발지/목적지를 IP가 아닌 SG를 참조하는 경우 정책 흐름 파악이 복잡함
- 출발지 IP 혹은 서비스 범위가 과도하게 넓은 룰을 일괄적으로 조회하기 어려움
- 순환 참조나 정책 충돌

모든 고민 해결!

- AWS 계정이 수십 개라면?

4. 다른 자동화 도구들

4. 다른 자동화 도구들


.github/workflows
01-a
02-c
03-e
04-t
05-s
06-s
07-c
08-s
09-s
10-p
11-s
12-u
13-g
14-g
99-a

4. 다른 자동화 도구들

- 레포 시크릿 스캔
- 깃헙 Org 및 멤버 퍼블릭 레포 탐지 자동화
- 엑소스피어 신규 입사자 초대 자동화
- 퇴사자 발생시 알람 / 캘린더 체크 자동화
- Prowler 데일리 점검 및 결과 리포팅 자동화
- 퇴사자 계정(7개 애플리케이션) 삭제 자동화
- PC보안점검 미조치 인원 CAA 접근 차단 및 복구 자동화
- 퍼블릭 스프레드시트 스캔 및 조치 도구
- 해킹메일 스캔 및 삭제 도구 / GWS 보안점검 도구
- CloudCustodian 정책을 비롯한 기타 자잘한 도구...

QnA

감사합니다.