4. SECURITY

NEXT OnAir 2020
베스핀글로벌 세션브리핑

Minimizing Permissions Using IAM Recommender

IAM Recommender를 사용한 권한 최소화

Abhi Yadav
Product Manager

Sonal Desai
Senior Cloud Security Engineer Uber

#Architect #Security Professional #System Administrator
#IT Professional #Manager #Intermediate

Week4.security

Minimizing Permissions Using IAM Recommender

IAM Recommender를 사용한 권한 최소화

Identity and Access Management (IAM)

- 클라우드 리소스에 대한 세부적인 액세스 권한을 부여하고 다른 리소스에 대한 액세스를 방지할 수 있습니다.
- IAM Recommender는 최소 권한(least privilege)의 보안 원칙을 적용하여 특정 리소스에 액세스하는 데 필요한 권한만 부여할 수 있게 도와줍니다.

IAM Policy (정책) 구조

- **IAM policy는** 어떤 역할이 어떤 구성원에게 부여되는지 정의하고 적용하며 이 정책은 리소스에 연결됩니다. 인증된 구성원이 리소스에 액세스를 시도하면 IAM는 리소스의 정책을 확인하여 작업 허용 여부를 결정합니다.
- **Binding (바인딩)은** Member (ID)와 역할이 포함되어 있습니다.
  - **Member** : 사용자 계정, 서비스 계정, Google 그룹 또는 도메인
  - **Role** : 이름이 지정된 권한 모음으로 Google Cloud 리소스에서 작업을 수행하는 데 필요한 액세스 권한을 부여함
- **Audit Configuration은** 어떤 권한 유형들이 로그 기록으로 남는지 결정할 수 있습니다.

고객사들이 보안 리스크를 최소화시키기 위해 고민하는 목표 및 문제점

✔ **목표**

구성원들에게 꼭 필요한 엑세스나 권한을 부여하여 완벽한 최소권한(least privilege) 상태를 구축

✔ **문제**

보안 위험성에 대해 사람들이 과소 평가하고 admin이 구성원들에게 필요 이상의 권한을 부여

보안성 관계자들이 최소 권한(least privilege) 상태를 편리하게 구성할수 있는 방법

첫째 : 현재 워크로드에 엑세스가 얼마나 부여되어있는지 파악

- Policy를 수립하기 위한 구성원들의 리소스 사용량에 대한 데이터 필요
- 해당 데이터로 수립한 정책이 조직 목표를 달성하는데 어떻게 도움되는지 파악
- 팀원 대상 교육을 통해 더 철저한 보안적 태도로 문화적 변화 추구

둘째 : 계획 설계

- 분기 마다 액세스 권한 검토
- High-level 권한 구성원에 대한 수시 검토
- 보안체계 자동화

셋째 : 구성원들의 Identity 기반으로 검토할 우선순위 수립

- 서비스 계정 확인
- 비활성 상태인 계정 검토

IAM Recommneder는 최소 권한 상태는 보안 전문가뿐만 아니라 개별 프로젝트 팀원들에게도 책임이 있기 때문에 이를 보완하기 위한 것

- IAM Recommender는 당신이 얼마만큼 액세스 권한을 부여했고 해당 권한들이 얼마나 자주 사용되는지 자동으로 측정 가능
  - 액세스 로그를 일일이 수집하고 분석할 필요없음 (수동 → 자동)
  - Back End에서 구글이 매일 데이터를 저장하고 처리됨 (추가 비용 없음)

시스템 보안 관리자와 사용자들이 GCP에 원치 않은 액세스를 발견하고 제거하는 과정에서 구글 머신러닝을 활용할 것을 권장

- 구성원은 현재 역할에 포함되어 있지만 최근 90일 동안 사용하지 않은 특정 권한이 필요할 수 있으며 이러한 권한을 식별하기 위해 ML (머신러닝)을 사용
  - **관찰된 내역의 동시발생 패턴**

    이전에 사용자가 A, B, C권한을 사용했다는 건, A, B, C가 어떤 식으로든 관련이 있을 수 있다는 힌트를 제공하며 Google Cloud 에서 작업을 수행하는 데 필요하면, 이러한 패턴을 자주 관찰하여 다른 사용자가 A와 B권한을 사용할 때 모델이 사용자에게 C 권한 또한 필요할 것이라고 제안
  - **역할 정의에 인코딩된 (encoded) 도메인 지식**

    IAM은 서비스별로 수백 가지의 사전 정의된 역할을 제공함. 사전 정의된 역할에 일련의 권한이 포함된다는 것은 이러한 권한들이 함께 부여되어야 한다는 강력한 신호임.

Uber Case (by Sonal-Senior Cloud Security Engineer Uber)

GCP에서 9만개의 역할 바인딩(binding)이있으며 Uber의 목표는 비지니스 파트너들이 클라우드를 안전하고 효율적으로 이용하여 비즈니스 업무를 진행할 수 있는 환경을 구축하는 것입니다.

✔ Problem

- **Uber의 딜레마** | 파트너팀 입장
  - 클라우드에서 리소스를 쉽게 할당
  - 편리한 유지보수 체계
  - ownership 소유권 권장
- **Uber의 딜레마** | 보안팀 입장
  - 클라우드를 모니터 할 의무
  - 불필요한 권한들을 삭제/제거
  - 최소 권한 상태를 유지

  → 보안팀의 목표는 해당 양측 요구사항을 평등하게 반영 필요
- **Overprovisioning에 의한 심각한 데이터 유출 사고 예방**
  예) 상위레벨 권한을 갖춘 ID가 해킹당해 PIC / PII data가 타협 또는 유출되는 사고

✔ 해결책

1. 클라우드 현황 모니터링

- 우리의 Cloud Asset은 무엇인가?
- 우리의 identity (신분)은?
- Role Binding (역할 바인딩)은 몇개?

2. 상황에 맞는 신속한 권한 조정

- 서비스 계정 (Service Accounts), 사용자 계정 (User Accounts), 구글 그룹 (Google group)의 Over Provisioning
  예) 기본 역할이 지정된 서비스 계정들이 2,500개 이상의 권한을 소유하고 있을때.
- Orphaned 계정
  예) 회사원이 이직을 했을때 그 회사원의 계정을 GCP 환경에서 삭제해야함.
- 오래되고 확인되지 않은 권한

3. 해결 조치 및 보안 강화

- 파트너 팀들을 위해서 티켓 (ticket) 생성 : 티켓이 생성된 이유 그리고 조치방안 대한 정보 제공
- Uber 보안팀이 'auto-apply' 추천 제공
- 데이터 기반으로 생성되는 권장

✔ GCP 적용이후

- 타 Cloud Service를 이용 시

  - activity log 찾기위해 직접 script 작성.
  - 액세스 패턴을 파악.
  - 데이터를 spreadsheet에 복사해서 일일이 점검.
  - 그리고 조치방안 권장.

  → 이런 방식으로 하면, 'access denied' 같은 많은 문제들이 발생

- GCP IAM Recommender를 활용하여 업무 개선 향상

  - 기록된 활동 (activity) 로그와 머신러닝 (ML), API 기능을 갖추어 IAM 권장 체계를 자동화

  → 로그를 수집, 보관, 그리고 분석 할 필요없음

Google Cloud IAM Recommender New Features :

✔ IAM 정책 Insights

- 정책 활용 데이터를 더 쉽게 접근할 수 있음
- custom 리포트 작성 또는 권장사항을 governance 도구들에 적용.

✔ Legacy 역할들에서 migration

- Owner와 Editor 역할에 더하여 커스텀 역할까지 권장사항 지원.

✔ 그룹들 대상으로 분석 및 권장사항 확장

- Over provision 상황 인식하고 어떤 역할을 할당 할 지 지원함.

✔ 커스텀 역할 권장

- Custom Role을 사용하여 보안성을 더 강화시킬 수 있다면, 구글이 직접 커스텀 역할 생산하는데 지원.

✔ 액세스 권장을 이제 customize 할 수 있음

- 권한을 제거하거나 추가 가능하며 이러므로 커스텀 역할을 생성함.
- 해당 커스텀 역할은 활동 데이터와 Google 머신러닝(ML)을 통해 개선되며 적절한 권한을 자동으로 권장함.
- 사용자로서는 해당 커스텀 역할을 적용하면 되고 비슷한 활동 데이터를 갖춘 사용자들에게 권장함.

✔ IAM 권장을 더 쉽게 발견할 수 있게 시스템 구축

- 프로젝트 팀원들은 Cloud Console에서 권장사항들을 검토하고 권한이 있으면 적용할 수 있음.

✔ 보안팀들에게는 BigQuery를 통해 'box integration' 서비스 제공함

- 이제 모든 권장사항들을 BigQuery 테이블로 보낼 수 있으며 "white customer" 보고서 작성 가능함.

✔ **API를 통해 권장사항들을 제공**

- 권장사항 자동화 뿐만 아니라 알림과 미리알림 (alerts and reminders)를 생성할 수 있음.

✔ **Google Cloud 새로운 솔루션 'Active Assist'**

- 데이터와 머신러닝(ML)을 사용하여 클라우드의 복잡한 관리 작업을 감소하고 클라우드의 보안, 성능 및 비용을 쉽게 최적화 할 수 있는 새로운 툴임.

베스핀글로벌 인사이트

클라우드 시장이 계속 성장하며 더 많은 기업들이 다양한 클라우드 서비스를 사용하고 있다.
클라우드 제공자들은 보안 관련 된 모든 문제들을 책임져주는 것은 아니지만, GCP는 기업들이 더 쉽고 편한 보안체계를 설립할 수 있도록 노력하는 것으로 보인다. IAM Recommender의 다양한 기능과 서비스를 통해 IAM 최소 권한 제공을 보다 쉽게 구성하도록 지원해 줌으로서 보안 위협 또는 문제들을 더욱더 철저하게 방지할 수 있도록 기업들에게 독립적인 보안 강화 능력을 키워준다.

베스핀글로벌은 Google Cloud를 가장 잘 아는 전문가이며, Google Cloud의 프리미어 파트너이자,
국내 최초 Google Cloud의 MSP(Managed Service Provider)입니다.
베스핀글로벌에서는 클라우드 문의나 Google Cloud 관련 무료 컨설팅을 진행하고 있습니다.
아래 문의로 편하게 연락주시기 바랍니다.

문 의 사 항 | 베스핀글로벌 구글사업부 sales.google@bespinglobal.com 070-7931-9600

참고 웹사이트 | https://cloud.withgoogle.com/next/sf/