프로젝트 소개

2022.08.26.~2022.12.17.

강대명(주멘토), 정승기(부멘토), 이재상(PL)

배경석(PM), 박병제, 임태인, 정금종, 차유담

INDEX

1. 개요

- 프로젝트 개요

많은 기업이 클라우드로 전환함에 따라 IaC는 많은 관심을 받고 있다. 인프라를 코드로 관리하기에 재사용이 가능하여 일관성과 배포 속도 향상 등 다양한 장점을 기대할 수 있기 때문이다. 하지만 IaC의 장점인 재사용성은 안전하지 않은 구성을 쉽게 배포할 수 있기 때문에 IaC 보안은 필수이다. 그중 가장 대중적인 Terraform 보안을 연구하였다.

- 목적

IaC(Terraform)에서 발생할 수 있는 보안 위협을 연구하며 사용자에게 이해하기 쉬운 형태로 전달한다.

- 시장 현황

2022년 가트너의 기술 트랜드에서 Cloud-Native Platforms가 선택되었으며, 2022년 github에서 공개한 오픈소스 생태계 보고서에서 트랜드 1위는 IaC이다.

하지만 2020년 팔로알토 보고서에서 Terraform의 22%는 안전하지 않은 구성을 가졌으며, 클라우드 인프라 관리자 31명에게 진행한 설문조사에서는 75%의 회사는 IaC 보안 솔루션 또는 절차가 존재하지 않았고, 63%의 사용자는 배포 전 보안 설정 문제로 IaC를 수정한 경험이 있다.

- 기대 효과

1) 보안 점검을 통해 보안성 향상
2) 보안 점검 자동화를 통해 일의 효율성 증대
3) 시각화를 통해 보안 위협 파악 용이
4) 리포트를 통해 IaC 보안 관련 원활한 소통

- 산출물

1) 웹

스캔 페이지	보안 위협 점검 및 시각화
체크리스트 페이지	점검 항목 세부 사항 및 룰 custom 제공

기능

2) 체크리스트

보안 위협 점검	설정 상의 보안 위협 점검
잘못된 구성 점검	사용자의 실수로 발생 가능한 보안 위협 점검
Report 제공	보안 위협 및 Compliance(ISMS-P) 통계 자료 제공
점검 도구	CheckOV를 활용한 점검 자동화

기능

2. 결과

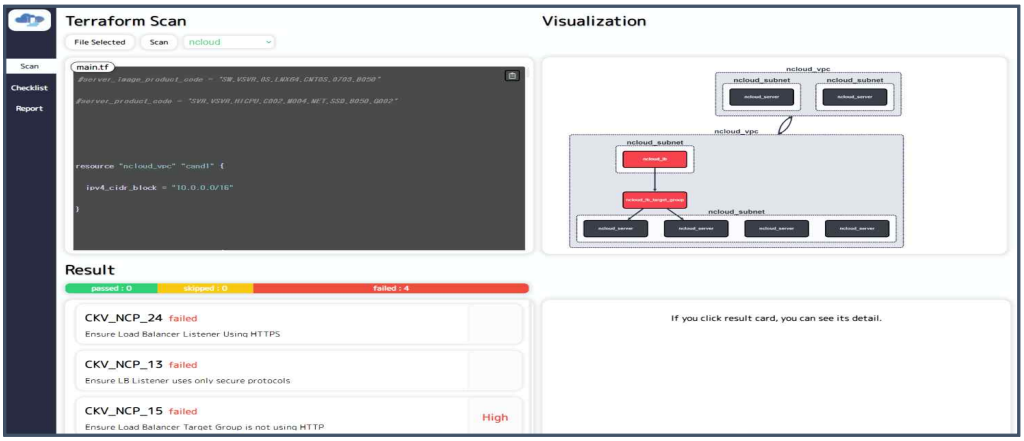
- 관리도구 ① 사용자 가이드 ② 기능 명세서 ③ https://github.com/init-cloud

1) Docker Image로 배포

▶ Client의 코드 유출 방지 우려 제거

2) 스캔 페이지

▶ 보안 위협 점검 및 시각화 제공



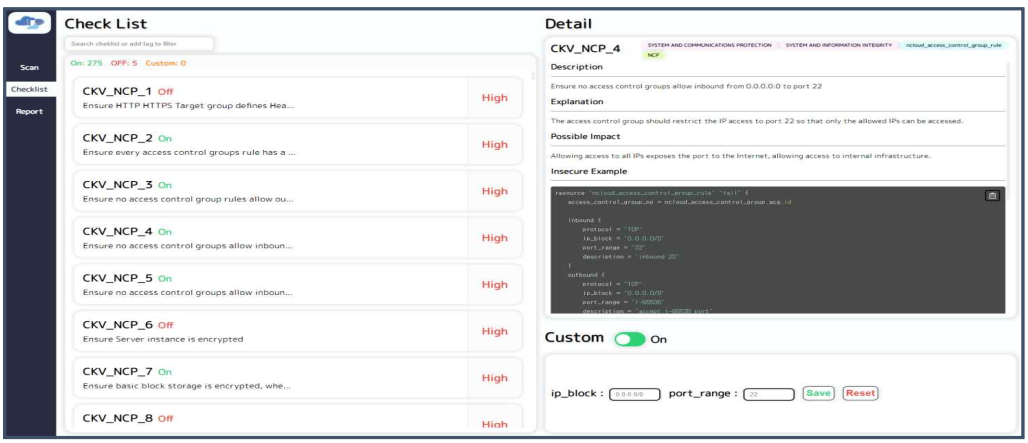
스캔 페이지

보안 위협 스캔	CheckOV 기반 보안 위협 스캔
시각화	보안 위협, 아키텍처 시각화
점검 결과 제공	점검 결과 세부사항 제공
Report 제공	보안 위협 및 Compliance(ISMS-P) 통계 자료 제공

기능

2) 체크리스트 페이지

▶ 점검 항목 세부사항 및 룰 custom 제공



체크리스트 페이지

문서 제공	룰 세부 설명 확인
커스텀	룰 세부 사항 변경

기능

- 체크리스트 ④ 체크리스트 ⑤ 룰 연구 예시 ⑥ ISMS-P 맵핑

1) 보안 위협 점검 체크리스트 ▶ 총합 : 38개

No	분류	ID	isms-p	Policy	Resource	커스텀	커스텀옵션	심각도
1	AUDIT AND ACCOUNTABILITY	CKV_NCP_1	2.9.2 2.10.2	Ensure HTTP HTTPS Target group defines Healthcheck	ncloud_lb_target_group	X		high
2	AUDIT AND ACCOUNTABILITY	CKV_NCP_2	2.10.2	Ensure every access control groups rule has a description	ncloud_access_control_group, ncloud_access_control_group_rule	X		low
3	ACCESS CONTROL, MEDIA PROTECTION	CKV_NCP_3	2.6.1	Ensure no security group rules allow outbound traffic to 0.0.0.0/0	ncloud_access_control_group_rule	O	IP 커스텀	high

보안 위협 점검 체크리스트 예시

■ NCP 보안 위협 체크리스트 제작

▶ 서버(3) ▶ 스토리지(2) ▶ 키(1) ▶ 계정관리(13)

▶ 네트워크(15) ▶ 로드밸런서(6) ▶ 오토스케일링(2) ▶ 쿠버네티스(4)

■ 심각도 계산 방법

분류	점수
High	1-3 점
Medium	4-6 점
Low	7-9 점

심각도 산정 방법

분류	내용	가중치
C	기밀성	3
I	무결성	3
A	가용성	3

심각도 점수 계산 방법

2) 구성상 오류 체크리스트 ▶ 총합 : 44개

No	분류	ID	github	Policy	Resource	Argument	심각도
1	IAM	cand1	https://github.com/cand0/InitCloud/tree/main/aws/Rule/cand1	두개의 리소스에 같은 group을 선언하면 rule이 상충되어 정상 작동이 되지 않을 수 있음.	aws_iam_group_policy_attachment	group	High
					aws_iam_policy_attachment	groups	
2	IAM	cand4	https://github.com/cand0/InitCloud/tree/main/aws/Rule/cand4	두개의 리소스에 같은 user를 선언하면 rule이 상충되어 정상 작동이 되지 않을 수 있음	aws_iam_user_policy_attachment	user	High
					aws_iam_policy_attachment	users	

구성상 오류 점검 체크리스트 예시

■ NCP 구성상 오류 체크리스트 제작 ▶ 총합 : 6개

▶ 네트워크(3) ▶ 서버(2)

■ AWS 구성상 오류 체크리스트 제작 ▶ 총합 : 38개

▶ IAM(12) ▶ EBS(4) ▶ VPC(8)

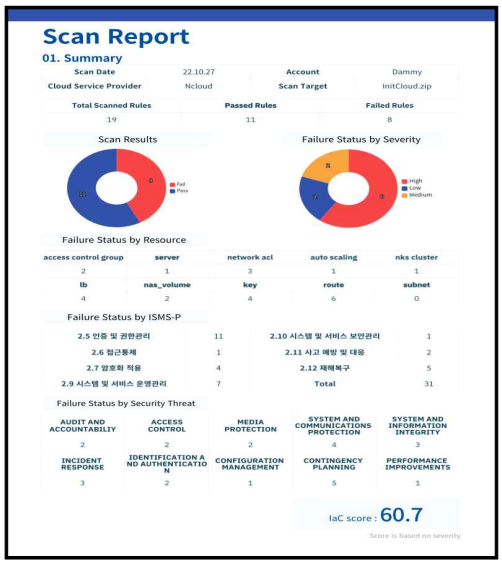
▶ EC2(4) ▶ S3(10)

■ 심각도 계산 방법

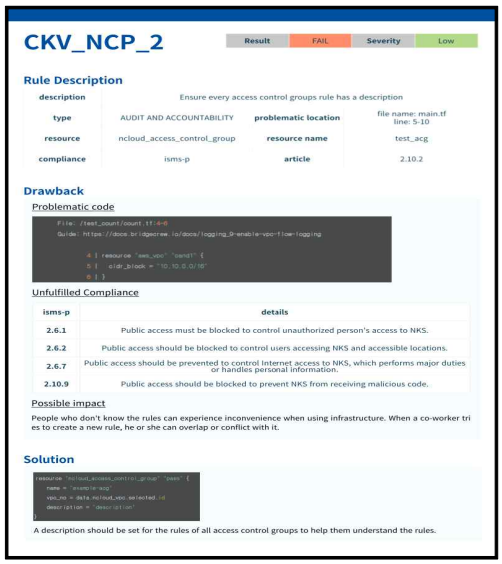
분류	내용
High	- 데이터가 훼손되는 경우 - 비인가자가 데이터에 접근할 수 있는 경우
Medium	- 복구를 위해 기존 인프라를 재구성 해야 하는 경우
Low	- 복구를 위해 기존 인프라를 재구성할 필요가 없는 경우

심각도 산정 방법

3) Report ⑦ 리포트 샘플



통계 자료

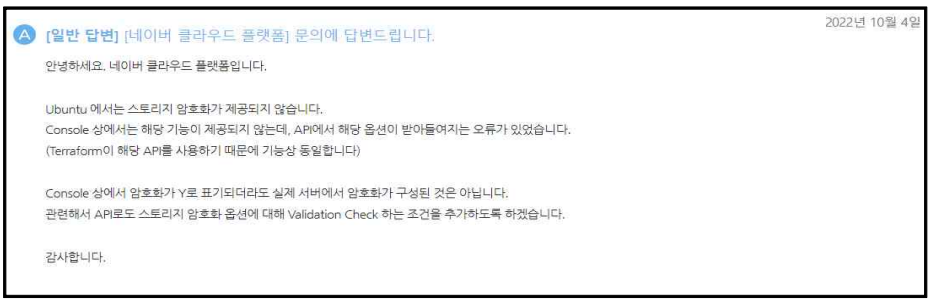


스캔 결과

3. 기타

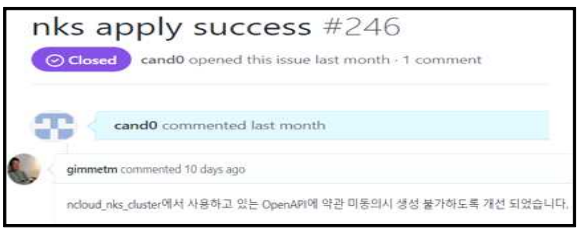
2) 버그 리포팅

- 암호화 관련 버그(NCP)



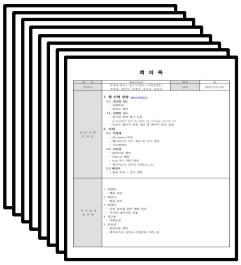
NaverCloud 고객 센터

- 약관을 동의하지 않아도 서비스 이용이 가능함(NCP)



NaverCloud github Issue

2) 회의록 ⑧ 회의록



총 25회 회의 진행

3) 인터뷰 ⑨ 인터뷰

- 클라우드 제품 판매 회사 이사
  : 클라우드 시장 발전에 따라 IaC 보안은 꼭 필요합니다.
- Tatum CEO
  : IaC 보안은 미래에 많은 니즈가 요구될 것입니다.
- Aviram 멘토님
  : 곧 모두가 IaC를 사용하게 될 것이며 IaC 시장은 작지 않습니다.
- Naver Cloud 관계자
  : 시각화와 컴플라이언스는 시장에서 필요로 하는 기능이라 생각합니다.
- 레몬트리 CTO
  : 구성상 오류는 시장에서 필요로 하며, 체크리스트는 잘 정리하였습니다. 하지만 스캔과 서비스 부분에서 사용자 친화적인 제공 방법을 고려하는 것이 좋아보입니다.
- Bridgecrew 관계자
  :

4. 첨부 파일

① 사용자 가이드
목적 : 서비스 이용을 위한 사용자 가이드
파일 : initcloud_사용자 가이드

② 기능 명세서
목적 : 대시보드 개발을 위한 기능 명세서 작성
파일 : initcloud_기능명세서

③ github
목적 : 배포를 위한 github 링크
파일 : http://github.com/init-cloud

④ 체크리스트
목적 : 룰 제작 및 공유를 위한 체크리스트
파일 : initcloud_체크리스트

⑤ 룰 연구 예시
목적 : 룰 연구의 세부 설명을 위한 문서
파일 : initcloud_룰 연구 예시

⑥ ISMS-P 맵핑
목적 : 사용자에게 ISMS-P 항목에 대한 이해를 돕기 위한 문서
파일 : initcloud_ISMSP

⑦ 리포트 샘플
목적 : 사용자에게 스캔 결과를 이해하기 쉬운 형태로 전달하기 위한 문서
파일 : initcloud_리포트 샘플

⑧ 회의록
목적 : 회의 내용 정리
파일 : initcloud_회의록

⑨ 인터뷰
목적 : 시장 현황 파악을 위한 인터뷰 및 결과지
파일 : initcloud_인터뷰