CNAPP 동작 원리와 클라우드-네이티브 보안 보고서

1) CNAPP란? (개념·구성·동작)

CNAPP(Cloud-Native Application Protection Platform)은 개발부터 운영까지 전 수명주기에 걸쳐 보안을 하나의 플랫폼에서 통합합니다. 일반적으로 **CSPM(구성 점검)**, **CWPP(워크로드 보호)**, **CIEM(권한/ID 통제)**, **IaC 스캐닝**, **취약점/이미지 스캔**, **런타임 위협 탐지** 모듈을 묶어 제공합니다.

동작 흐름(요약)

코드/템플릿 → 빌드/이미지 → 배포(K8s/서버리스) → 런타임

- **Shift-left**: IaC(Terraform/K8s manifest)와 컨테이너 이미지를 파이프라인에서 먼저 스캔.
- **Posture/권한**: 클라우드 계정 구성과 IAM 권한을 상시 분석.
- **런타임 가시성**: 에이전트/에이전트리스로 프로세스·네트워크·시스템 호출을 모니터링하고 정책 위반/공격 징후를 탐지.
- **프레임워크 정렬**: Kubernetes Top 10, NIST SP 800-190, MITRE ATT&CK for Containers 기준으로 탐지·대응을 표준화.

2) 클라우드-네이티브 애플리케이션 주요 취약점

- **잘못된 구성(Misconfig)**: 공개 S3/Bucket, 과도한 보안그룹/퍼블릭 서비스, 취약한 TLS. (CSPM 범주)
- **Kubernetes 리스크**: 부적절한 워크로드 설정, 과도한 RBAC, 중앙 정책 부재, 로깅 부족, 시크릿 관리 실패, 네트워크 분리 미흡
- **소프트웨어 공급망**: 이미지 취약점, 서드파티 라이브러리, 악성 베이스 이미지. (NIST 800-190)
- **권한 남용/ID 평균권한 초과**: 서비스 계정·롤 바인딩 오남용(클러스터 관리자 권한 남발).
- **런타임 위협**: 컨테이너 탈출 시도, 자격증명 탈취, 크립토마이닝, C2 통신 등 (ATT&CK for Containers).

3) 대응 방안 (CNAPP로 묶어 실행)

- **구성/권한 통제**: CSPM로 멀티클라우드 구성을 상시 점검, CIEM으로 계정·롤 최소권한(Least Privilege) 강제.
- **Shift-left 보안**: IaC 스캐닝(잘못된 리소스 정의 차단), 이미지 취약점·SBOM 스캔을 CI 파이프라인에 기본화. (NIST 800-190 권고)
- **Kubernetes 보안 기본기**: 네임스페이스 격리, NetworkPolicy 적용, PodSecurity/OPA/Kyverno로 중앙 정책 집행, 시크릿은 KMS/전용 보관소 사용. (K8s Top 10 권고)
- **런타임 보호**: eBPF/에이전트 기반 행위 탐지, 파일·프로세스 무결성, 동적 위협 탐지 룰을 **MITRE ATT&CK for Containers**매트릭스에 맞춰 튜닝.
- **가시성·감사**: 클라우드 감사 로그(CloudTrail 등)와 K8s 감사/컨테이너 런타임 로그를 수집·연계 분석. (CNCF 보안 백서)
- **보안 운영**: 레이트 리밋·WAF·레지스트리 서명/검증, 취약 컴포넌트 신속 패치, 런북/플레이북 기반 대응.

4) CNAPP 기반 **진단 절차(면접용 스크립트 요약)**

1. **자산 식별/가시성 확보**: 클라우드 계정·클러스터·네임스페이스·이미지 인벤토리 자

동 수집(CSPM/자산 지도).
2. **설계·구축 점검**: IaC/K8s 매니페스트 정책 검사(금칙 설정: 퍼블릭 스토리지, 0.0.0.0/0, privileged 등).
3. **공급망 보안**: 이미지/패키지 취약점·서명 검증, SBOM 생성·추적. (NIST 800-190)
4. **권한·ID 분석**: 과권한 서비스계정·롤 바인딩 탐지·차단(CIEM).
5. **런타임 탐지**: 프로세스·네트워크 이상행위를 ATT&CK 매핑으로 탐지·알림.
6. **지속 개선**: 리스크 스코어·공격 경로 리포트 기반 우선순위화 후, 파이프라인 게이트로 회귀(DevSecOps).

5) 개인 의견

- CNAPP의 가치는 "도구 통합"이 아니라 **리스크를 수명주기 전 구간에서 같은 언어로 보게 하는 것**에 있습니다. 특히 멀티클라우드/K8s 환경에선 **구성 오류와 권한 남용**이 가장 큰 실전 리스크이며, **Shift-left+런타임**의 이중 방어가 효과적입니다.
- 면접에서 저는 **OWASP K8s Top 10·NIST 800-190·ATT&CK**3축에 맞춰 진단·대응을 설명하고, 조직 상황에 따라 **에이전트리스 우선 도입→핵심 워크로드에 에이전트 보강**전략을 권합니다.

6) 참고 자료

https://www.gartner.com/reviews/market/cloud-native-application-protection-platforms
https://www.aquasec.com/cloud-native-academy/cnapp/cnapp-gartner/
https://tag-security.cncf.io/community/resources/security-whitepaper/
https://owasp.org/www-project-kubernetes-top-ten/